Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials

Ronald J. Hedges, Editor

August 2020

Updated from 2019 Supplement

Table of Contents

FOREWARD TO THE AUGUST 2020 SUPPLEMENT

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, a September, 2019, edition was published that updated the December, 2017, compilation.

It is now August of 2020 and the time has come to publish a supplement to the December 2017 and September 2019 editions.

This latest supplement features links to materials, as does its predecessors. The links in the supplement were last visited when it was completed in August 2020. The reader is cautioned that specific links may have 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.

RJH August 13, 2020

TAGS
#Admissibility
#CSLI
#Discovery Materials
#Encryption
#Fifth Amendment – Self-Incrimination
#Fourth Amendment – Ex Ante Conditions
#Fourth Amendment – Exigent Circumstances
#Fourth Amendment – Good Faith Exception
#Fourth Amendment – Particularity Requirement and/or Overbreadth
#Fourth Amendment – Warrant Required or Not
#International
#Miscellaneous
#Preservation and Spoliation
#Probation and Supervised Release
#Reasonable Expectation of Privacy
#Sixth Amendment – Assistance of Counsel
#Sixth Amendment – Right of Confrontation
#SCA (Stored Communications Act)
#Social Media
#Third-Party Doctrine
#Trial-Related

ABBREVIATIONS
"Cell Site Location Information" – CSLI
"Stored Communications Act" – SCA

DECISIONS – UNITED STATES SUPREME COURT

Byrd v. United States, 138 S. Ct. 1518 (2018)

The defendant was the sole occupant and operator of a rental vehicle when he was stopped for a traffic infraction. Arresting officers searched the vehicle without the defendant's consent after they learned he was not an authorized driver under the rental agreement. The officers found body armor and heroin. The defendant was convicted of various federal offenses after he moved unsuccessfully to suppress the fruits of the search. His conviction was affirmed by the Third Circuit Court of Appeals, which held that the defendant had no expectation of privacy and therefore no standing to challenge the search. The Supreme Court granted *certiorari* to address a conflict between the circuits "over whether an unauthorized driver has a reasonable expectation of privacy in a rental car." Addressing the circumstances under which a person can have a reasonable expectation of privacy, the Court held that a reasonable expectation can derive from "concepts of real or personal property law or to understandings that are recognized and permitted by society," that the former "guides resolution of [the] case," and that a remand was appropriate for factual development of whether the defendant had lawful possession of the vehicle. The Court also left open the question of whether there was probable cause to search under the automobile exception to the Warrant Requirement.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

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

The petitioner had been convicted of various offenses related to a series of robberies across several States. Evidence offered against him included CSLI collected over a 127-day period pursuant to orders issued under the SCA. The court of appeals affirmed, holding that the petitioner had no reasonable expectation of privacy in the location information because he had shared that information with his wireless carriers. The Supreme Court reversed.

At issue was the application of the Fourth Amendment to a "new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals." Writing for the majority, the Chief Justice declined to extend the third-party doctrine: "Given the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection." The Court held that information obtained was the product of a "search" and that the Government should have secured a

warrant based on probable cause. The judgment below was reversed and remanded for further proceedings. The Court declined to decide whether there was a "limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be. It is sufficient *** to hold today that accessing seven days of CSLI constitutes a *** search." The Court also left undisturbed the exceptions to the Warrant Requirement.

#Fourth Amendment – Warrant Required or Not

#Reasonable Expectation of Privacy

#Third-Party Doctrine

Kansas v. Boettger, 140 S.Ct. 1956 (2020) (Thomas, J., dissenting from denial of *certiorari*)

> In my view, the Constitution likely permits States to criminalize threats even in the absence of any intent to intimidate. *** It appears to follow that threats of violence made in reckless disregard of causing fear may be prohibited. The Kansas Supreme Court reached the opposite conclusion by overreading our decision in [*Virginia v.*] *Black* [538 U.S. 343 (2003)], which *did not answer the question presented here. Other courts looking to Black*, however, have upheld similar statutes. *** I would grant the petition for certiorari to resolve the split on this important question.

#Social Media

Mitchell v. Wisconsin, 139 S.Ct. 2525 (2019)

In this appeal from a drunk driving conviction, the Supreme Court addressed whether taking a warrantless blood sample of a suspected drunk driver who had been arrested and was unconsciousness violated the Warrant Requirement. The Court adopted a "rule for an entire category of cases—those in which a motorist believed to have driven under the influence of alcohol is unconscious and thus cannot be given a breath test," concluding that there is a compelling need for a blood draw as the evidence dissipates over time. Moreover, some other factor must be present that would take priority over a warrant application. The Court rejected the defendant's argument that advances in communication technology made warrantless searches unnecessary: "In other words, with better technology, the time required has shrunk, but it has not disappeared. In the emergency scenarios created by unconscious drivers, forcing police to put off other tasks for even a relatively

short period of time may have terrible collateral costs. That is just what it means for these situations to *be* emergencies." (emphasis in original).

#Fourth Amendment – Warrant Required or Not

United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (*per curiam*)

"The Court granted certiorari *** to decide whether, when the Government has obtained a warrant under 18 U.S.C. Sec. 2703, a U.S. provider of e-mail services must disclose to the Government electronic communications within its control even if the provider stores the communications abroad." Prior to oral argument the CLOUD Act was enacted. Moreover, a new warrant replaced the original one. The Court concluded that the case had become moot, vacated the judgment under review, and remanded with instructions.

#International

#SCA (Stored Communications Act)

CERTIORARI GRANTED – UNITED STATES SUPREME COURT

Van Buren v. United States, No. 19-783, 2020 WL 1906566 (U.S. Apr. 20, 2020)

Question presented: Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.

Decision below: *United States v. Van Buren*, 940 F.3d 1192 (11th Cir. 2019)

DECISIONS – FEDERAL

Airbnb, Inc. v. City of New York, 373 F. Supp. 3d 467(S.D.N.Y. 2019)

Two home-sharing platforms sought to preliminarily enjoin a city ordinance that would require them to turn over on a monthly basis "voluminous data regarding customers who use their platforms to advertise short-term rentals." The court held that the ordinance implicated the Fourth Amendment: "It puts in place a search and seizure regime that implicates privacy interests of the 'booking services' whose user records must be produced monthly ***." The court then looked to Fourth Amendment precedent outside the criminal context to determine whether the ordinance was reasonable. It found that two features of the ordinance mitigated its intrusion on privacy and security interests. However, because its scope was "breathtaking" and "the antithesis of a targeted administrative subpoena for business records," the court granted the relief sought, ordering discovery to proceed expeditiously.

#Miscellaneous

Andrews v. Baltimore City Police Dep't, No. 18-1953, 2020 U.S. App. LEXIS 9641 (4th Cir. Mar. 27, 2020)

In this Section 1983 action, the plaintiff contended that the defendant police department conducted a warrantless search when it used a cell site simulator known as "Hailstorm" to locate him. After his arrest, the defendant prevailed on a motion to suppress in State court and commenced this federal action. The district court found that the State court order that allowed the use of the simulator was a warrant. It then granted summary judgment. The Court of Appeals reversed and remanded for findings of fact on the "degree of intrusion onto constitutionally protected areas that occurred as a result of the Hailstorm simulator's use." The court did note that "[l]aw enforcement agencies are reluctant to disclose information about cell site simulators. *** This case is no different."

#Miscellaneous

I/M/O App. for the Subpoena 2018R00776¸947 F.3d 148 (3d Cir. 2020)

> This case requires us to determine whether the First Amendment permits a court, acting pursuant to the Stored Communications Act (SCA), to restrain a grand jury witness from disclosing its receipt of service to a third party. A grand jury issued a subpoena to ABC Corp., an electronic service provider, for the data of one of its customer's employees who was under criminal investigation. A search warrant later demanded additional data regarding the same subscriber. These requests were accompanied by nondisclosure orders (NDOs) prohibiting ABC Corp. from notifying anyone of the existence of the data requests. ABC Corp. complied with both requests but challenges the constitutionality of the NDOs, arguing that they infringe upon its freedom of speech. ABC Corp. asks to amend the NDOs to permit disclosure to an individual who, it argues, poses no risk to the grand jury investigation. We must determine whether the First Amendment tolerates such a restraint on speech.
>
> Our conclusion *** is that the governmental interest in maintaining grand jury secrecy is sufficiently strong for the NDOs to withstand strict scrutiny. Disclosure to anyone outside of the grand jury process would undermine the proper functioning of our criminal justice system. We will affirm the District Court's denial of ABC Corp.'s motion to amend the NDOs. (footnotes omitted).

Explaining its conclusion, the Court of Appeals recognized that the NDOs in issue implicated First Amendment rights. Moreover, the NDOs were content-based and constituted a presumptively unconstitutional prior restraint. The court applied strict

scrutiny and affirmed the NDOs because the NDOs (1) served a compelling government interest in protecting the secrecy of a grand jury investigation; (2) were narrowly tailored for a period of one year and permitted "abstract" discussion of the requests; and (3) were the least restrictive means to advance the compelling interest.

#Miscellaneous

#Stored Communication Act

Arizmendi v. Gabbert, 919 F.3d 891 (5th Cir. 2019)

The plaintiff filed a Section 1983 action against the defendant, the criminal investigator for the school district by which she was employed. The plaintiff alleged that the defendant knowingly or recklessly misstated material facts in an affidavit for a warrant for her arrest for allegedly communicating a false report. The district court denied summary judgment to the defendant. On appeal, the defendant argued that he was entitled to summary judgment because, even if he had made false allegations, facts stated in the affidavit established probable cause to arrest the defendant for a different offense. The Fifth Circuit reversed: "the validity of the arrest could not be saved by facts stated in the warrant sufficient to establish probable cause for a different charge from that sought in the warrant." However, the defendant was entitled to qualified immunity because "this was not clearly established at the time of his conduct."

#Fourth Amendment – Good Faith Exception

#Miscellaneous

Boudreau v. Lussier, 901 F.3d 65 (1st Cir. 2018)

This was an action brought under Section 1983 and the Electronic Communications Privacy Act. The plaintiff's employer suspected him of viewing child pornography at work. The employer "covertly installed screenshot-capturing software on Boudreau's work computer, which confirmed these suspicions. This led them to contact law enforcement." After the plaintiff's arrest and nolo plea to one count in State court he filed the action against the individuals who participated in the events that led to his arrest and followed his arrest. The district court granted summary judgment. The court of appeals affirmed, concluding that (1) the impoundment and search of the plaintiff's vehicle after his arrest was reasonable under the "community caretaking function" exception to the Warrant Requirement; (2) there was no proof of a conspiracy to entrap the plaintiff into driving on a suspended license; (3) there was no impermissible search of the plaintiff's work

computer because the business owner had apparent authority to allow law enforcement to conduct a warrantless search; (4) even assuming that the affidavits submitted in support of search warrants omitted material facts and were disregarded, probable cause existed for the issuance of the warrants; and (5) the screenshots were not intercepted contemporaneously with their transmission and thus was not a violation of EPCA. Finally, the court of appeals held expert testimony was required to defeat summary judgment on the EPCA claim, which plaintiff did not present.

#Admissibility

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Crocker v. Beatty, 886 F.3d 1132 (11th Cir. 2018) (*per curiam*)

This was an appeal by the defendant, a sheriff's deputy, from the denial of his motion for summary judgment. The plaintiff had filed a Section 1983 action against the defendant, alleging that his Fourth Amendment rights had been violated when the defendant seized a cell phone after the plaintiff had taken photos and videos of a crash scene from an "interstate grass median." After the defendant refused to return the phone the plaintiff refused to leave the scene and he was arrested for resisting an officer without violence. Addressing the exigent circumstances exception to the Warrant Requirement, the court of appeals held that, even assuming "*arguendo* [that] it was reasonable for Beatty to consider that the photographs and videos may be evidence of a crime," there were "no facts in the record [to] support the conclusion that a reasonable, experienced agent would have thought destruction of the evidence was imminent." The court of appeals also rejected the defendant's argument that he was entitled to qualified immunity:

> Beatty's argument, however, is that the *application* of this exception to the seizure of cell phones—in particular, Internet-connected smart phones like Crocker's iPhone—was not clearly established in 2012. But this argument asks far too much. The novelty of cutting-edge electronic devices cannot grant police officers *carte blanche* to seize them under the guise of qualified immunity. This is not how our analysis operates. Even in 'novel factual situations,' we must deny qualified immunity when clearly established case law sends the 'same message' to reasonable officers. *** Our case law has sent a consistent message, predating 2012, about the warrantless seizure of personal property and how exigent circumstances may arise. The technology of the iPhone simply does not change our analysis. To hold otherwise would deal a devastating blow to the Fourth Amendment in the face of sweeping technological advancement. These advancements do not create

> ambiguities in Fourth Amendment law; the principles remain as always. Because of this, Beatty is not entitled to qualified immunity. (emphasis in original).

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Good Faith Exception

Cruise-Gulyas v. Minard, 918 F.3d 494 (6th Cir. 2019)

This was an interlocutory appeal by the police officer defendant from the district court's denial of his motion to dismiss a Section 1983 action on qualified immunity grounds. The defendant had pulled over the plaintiff for speeding but gave her a ticket for a lesser traffic violation. As she drove away the plaintiff gave a defendant "an all-too-familiar gesture *** with her hand *** and without four of her fingers showing." The defendant then pulled over the plaintiff a second time and changed the ticket to a speeding offense. The court of appeals affirmed: (1) the second stop was a seizure under the Fourth Amendment and required a showing of probable cause distinct from the first; (2) "[a]ny reasonable officer would know that a citizen who raises her middle finger engages in speech protected by the First Amendment"; and (3) "[a]n officer who seizes a person for Fourth Amendment purposes without proper justification and issues her a more severe ticket clearly commits an adverse action that would deter her from repeating that conduct in the future."

#Fourth Amendment – Good Faith Exception

#Miscellaneous

Gould v. Farmers Ins. Exchange, No. 4:17 CV 2305 RWS, 2018 WL 4144773 (E.D. Mo. Aug. 30, 2018)

This is a putative class action brought under the Telephone Consumer Protection Act. The plaintiff sought to compel two non-party agents of the corporate defendants to produce documents related to text messages they purportedly sent to potential customers. The agents argued, among other things, that compelling production would violate their Fifth Amendment privilege against self-incrimination. The court granted the motion to compel: "the Agents' mere possession, production, or authentication of call logs or other documents is not the act that would tend to incriminate them. The Fifth Amendment protection *** does not protect against disclosure of the requested documents because of the 'settled proposition that a person may be required to produce specific documents even

though they contain incriminating assertions of fact or belief because the creation of those documents was not "compelled" within the meaning of the privilege.'" (quoting *United States v. Hubbell*, 530 U.S. 27 (2000)).

#Fifth Amendment – Self-Incrimination

I/M/O Grand Jury Subpoena, 749 Fed. App'x 1 (D.C. Cir. 2018) (Judgment)

This was an appeal from the denial of a motion to quash a grand jury subpoena. The corporation served with the subpoena argued that it was immune under the Foreign Sovereign Immunities Act and that the subpoena was unenforceable under *Fed. R. Crim. P.* 17(c)(2) because it would require the corporation to violate another country's domestic law. The court of appeals affirmed, concluding that, among other things, the corporation had failed to carry its burden to show that compliance would violate the other country's law. The text of the law did not support the corporation's position and the corporation's submissions that purported to explain an "atextual interpretation lack[s] critical indicia of reliability."

#Miscellaneous

Hately v. Watts, 917 F.3d 770 (4th Cir. 2019)

This is an action brought under the Stored Communications Act, a statute that one commentator has described to be "notoriously difficult to understand." Here, the court of appeals reversed the district court and held that previously opened and delivered emails stored in a web-based email service were in protected "electronic storage" under the SCA.

For an extended discussion of the SCA and the circuit split over its interpretation, see Orin Kerr's article in the "Articles" Section of this Supplement.

#SCA (Stored Communications Act)

Jernigan v. City of Montgomery, 806 Fed. App'x 915 (11th Cir. 2020) (*per curiam*)

The plaintiffs in this Section 1983 action appealed from the entry of summary judgment in favor of the defendant city and one of its officers. The officer had arrested the plaintiffs after he misinterpreted a computer database as listing outstanding warrants for their arrest instead of criminal summonses. The district court held that the officer was entitled to qualified immunity for his reasonable mistake of fact and that the city had not acted with deliberate indifference because "it was not obvious that the failure to provide additional training on the mobile computer database would result in improper arrests." The Eleventh Circuit affirmed.

#Miscellaneous

Johnson v. Duxbury, 931 F.3d 102 (1st Cir. 2019)

This was a Section 1983 action brought by a police officer against the municipality by which he was employed and the chief of police. The officer alleged that the defendants violated his Fourth Amendment rights by demanding his cell and home phone records in the course of an internal investigation into his conduct. The district court granted summary judgment in the favor of the defendants. The First Circuit affirmed, concluding that the demand did not implicate the Fourth Amendment because "an individual has no reasonable of [sic] expectation of privacy in a phone service provider's records of the phone numbers that he has dialed or from which he has received calls." In so ruling, the Court of Appeals relied on the third-party doctrine and distinguished the demand for phone numbers at issue from demands for content. It also rejected the officer's argument that, by requesting the phone records from him rather than from the service provider, the officer had a reasonable expectation of privacy because he had "physical possession of a copy."

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

Pagan-Gonzalez v. Moreno, 919 F.3d 582 (1st Cir. 2019)

“This case requires us to consider the constitutional boundaries for the use of deception by law enforcement officers seeking consent for a warrantless search. We conclude that the search at issue here violated the Fourth Amendment because the circumstances -- including a lie that conveyed the need for urgent action to address a pressing threat to person or property -- vitiated the consent given by appellants. We further hold that the defendants are not entitled to qualified immunity from civil liability for the unlawful search because any reasonable officer would have recognized that the circumstances were impermissibly coercive. However, we reject a related claim alleging malicious prosecution on the ground that, even if it had merit, the defendants would be entitled to qualified immunity.”

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Good Faith Exception

#Miscellaneous

Sandvig v. Barr, Civil Action No. 16-1368 (JDB), 2020 WL 1494065 (D.D.C. Mar. 27, 2020)

> Plaintiffs are academic researchers who intend to test whether employment websites discriminate based on race and gender. In order to do so, they plan to provide false information to target websites, in violation of these websites' terms of service. Plaintiffs bring a pre-enforcement challenge, alleging that the Computer Fraud and Abuse Act ("CFAA") *** as applied to their intended conduct of violating websites' terms of service, chills their First Amendment right to free speech. Without reaching this constitutional question, the Court concludes that the CFAA does not criminalize mere terms-of-service violations on consumer websites and, thus, that plaintiffs' proposed research plans are not criminal under the CFAA. The Court will therefore deny the parties' cross-motions for summary judgment and dismiss the case as moot.

#Miscellaneous

I/M/O Search of a Residence in Aptos, California, Case No. 17-mj-70656-JSC-1, 2018 WL 1400401 (N.D. Cal. Mar. 20, 2018)

This matter arose out of the Government's application pursuant to the SCA to compel the real party in interest (Spencer) to provide access to three electronic storage devices seized during the search of his home. The court granted the application. It found that "the record demonstrates that Mr. Spencer's knowledge of the encryption passwords is a foregone conclusion and—in addition—that the authenticity, possession, and existence of the sought-after files are a foregone conclusion. In either event, the testimony inhering to the act of decryption is a foregone conclusion that 'adds little or nothing to the sum total of the Government's information.' (*quoting Fisher v. United States*, 425 U.S. 391 (1976)).

#Encryption

#Fifth Amendment – Self-Incrimination

I/M/O Search of a Residence in Oakland, California, 354 F. Supp. 3d 1010 (N.D. Cal. 2019)

Here, the court denied an application to compel anyone present at the time of a search of a premises to "press a finger (including a thumb) or utilize other biometric features, such as facial or iris recognition, for the purposes of unlocking the digital devices found in order to permit a search of the contents as authorized by the search warrant." In denying the application, the court found: (1) the

application was overbroad as there was no probable cause to compel any person who might be in the premises at the time of the search to provide a biometric feature to "unlock any unspecified digital device that may be seized during the otherwise lawful search"; (2) the warrant was overbroad insofar as it sought to permit the search of a device "on a non-suspect's person simply because they are present" at the time of the search; (3) the proposed use of biometric features to unlock a device would be testimonial in nature and raise the issue and, even if there was probable cause to seize devices, that probable cause "does not permit the Government to compel a suspect to waive" the Fifth Amendment privilege; and (4) the foregone conclusion did not apply because, citing *Riley v. California* and noting the volumes of information on a device, "the Government inherently lacks the requisite prior knowledge of the information and documents that could be obtained via a search of these unknown digital devices ***." The court then permitted the Government to make a new application consistent with its ruling.

#Encryption

#Fifth Amendment – Self-Incrimination

#Miscellaneous

I/M/O Search of: A White Google Pixel 3 XL Cellphone In a Black Incipio, 398 F. Supp. 3d 785 (D. Idaho 2019)

A magistrate judge denied the Government's application to compel a "subject's finger on a cellphone to unlock the phone to conduct a forensic search," concluding that granting the application would infringe on the suspect's Fifth Amendment privilege against self-incrimination. The district court reversed the magistrate judge and granted the application:

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

#Fifth Amendment – Self-Incrimination

*I/M/O The Search of *** Washington, District of Columbia*, 317 F. Supp. 3d 523 (D.D.C. 2018)

The Government filed an application for a warrant to search a premise and to seize, among other things, evidence found on electronic devices. The Government also sought to compel "'biometric features of an individual believed to have perpetrated the alleged offenses *** in connection with any biometric recognition sensor-enabled'" device within the scope of the warrant. The court appointed the Federal Public Defender as *amicus* to submit its views on the lawfulness of the application. The court issued the warrant. Addressing the Fourth Amendment, the court concluded that this standard should be complied with in all future applications that sought to compel the use of biometric features:

> when attempting to unlock a *** device during the execution of a search warrant that authorizes the search of the device, the government may compel the use of an individual's biometric features, if (1) the procedure is carried out with dispatch and in the immediate vicinity of the premises to be searched, and if, at time of the compulsion, the government has (2) reasonable suspicion that the suspect has committed a criminal act that is the subject matter of the warrant, and (3) reasonable suspicion that the individual's biometric features will unlock the device, that is, for example, because there is a reasonable suspicion to believe that the individual is a user of the device. (footnote omitted).

The court also held that the compelled use of a biometric feature would not implicate Fifth Amendment privilege against self-incrimination because the individual would not communicate anything of a testimonial nature.

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

I/M/O Search Warrant App. for the Cellular Telephone in United States v. Barrera, 415 F. Supp. 3d 832 (N.D. Ill. 2019)

The Government sought to compel a defendant's fingers and thumbs to be pressed on an iPhone home button in an attempt to unlock the device. The defendant opposed the application, contending that the compulsion would violate his Fourth and Fifth Amendment rights. The court held that the supporting affidavit established the existence of probable cause to believe that evidence of the crime charged existed on the device and that the device belonged to the defendant. As to the Fifth Amendment objection, the court noted that federal and State courts had reached different results. Nevertheless, the court found the Fifth Amendment

inapplicable because (1) the "biometric unlock procedure is more akin to a key than a passcode combination," (2) the unlock "is first and foremost a physical act," and (3) any "implicit inference from the biometric unlock procedure . . . is not sufficient to convert the act to testimonial."

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

In re: Search Warrant Issued June 13, 2019, 942 F.3d 159 (4th Cir. 2019)

> The appellant in these proceedings is a Baltimore law firm (the "Law Firm") that challenges the government's use of a so-called 'Filter Team' — created *ex parte* by a magistrate judge in the District of Maryland and comprised of federal agents and prosecutors — to inspect privileged attorney-client materials. Those materials were seized from the Law Firm in June 2019 during the execution of a search warrant issued by the magistrate judge. The Law Firm requested that the district court enjoin the Filter Team's review of the seized materials, invoking the attorney-client privilege and the work-product doctrine. When the court denied its request, the Law Firm pursued this appeal. As explained below, we are satisfied that use of the Filter Team is improper for several reasons, including that, inter alia, the Team's creation inappropriately assigned judicial functions to the executive branch, the Team was approved in *ex parte* proceedings prior to the search and seizures, and the use of the Team contravenes foundational principles that protect attorney-client relationships. We therefore reverse and remand.

#Discovery Materials

In re Search Warrant No. 5165, No. 5:20-MJ-5165, 2020 WL 3581608 (E.D. Ky. July 2, 2020)

This was an application by the Government for a search warrant that requested, among other things, "to compel any individuals present during *** execution to provide biometrics in order to access seized electronic devices." Addressing Fourth Amendment concerns raised by an *amicus curiae*, the court concluded that the warrant was overbroad:

> [T]he United States may only compel individuals present *** to provide biometric markers to unlock electronic devices where the United States has reasonable suspicion that such an individual has committed a criminal act that is the subject matter of the warrant, and reasonable suspicion that the individual's biometrics will unlock the device. (footnote omitted).

Turning to a Fifth Amendment analysis, the court concluded that the privilege against self-incrimination did not apply to the compulsion in issue because the use of biometrics would not be testimonial. In so concluding, the court rejected case law that reached the opposite conclusion.

#Encryption

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Warrant Required or Not

Taylor v. Saginaw, 922 F.3d 328 (6th Cir. 2019) (Amended Opinion)

The plaintiff, a "frequent recipient of parking tickets," filed this Section 1983 action against the defendant city and one of its employees. The plaintiff alleged that the city's practice of "chalking" – using chalk to mark the tires of parked vehicles to track how long they have been parked, abridged her Fourth Amendment right to be free from unreasonable searches. The district court dismissed the complaint, finding that, although chalking might be a search, it was reasonable. The Sixth Circuit reversed. It concluded: (1) chalking constituted a common law trespass upon a constitutionally-protected area and therefore was a search under the Fourth Amendment pursuant to *United States v. Jones*, 565 U.S. 400 (2012); (2) the search was intended to secure information used by the city to issue parking citations; and (3) the warrantless search in issue did not fall within the community caretaking or automobile exceptions to the Warrant Requirement. The court remanded with this observation: "When the record *** moves beyond the pleadings stage, the City is, of course, free to argue anew that one or both of those exceptions do apply, or that some other exception to the warrant requirement might apply."

#Fourth Amendment – Warrant Required or Not

United States v. Ackell, 907 F.3d 67 (1st Cir. 2018)

The defendant was convicted of stalking under 18 U.S.C. Section 2261A. On appeal, among other things, he challenged the statute under which he was charged on First Amendment grounds. The First Circuit affirmed the conviction. The matter arose out of a series of online communications between the defendant and a third person. When the latter wanted to end their online relationship, the defendant threatened to expose her. The First Circuit held that the statute in issue penalized conduct rather than speech and that, "while acknowledging that *** [the statute] could have an unconstitutional application, and remaining cognizant of the chilling-effect-related concerns inherent in declining to invalidate a statute that can

be applied to violate the First Amendment – we are unconvinced that we must administer the 'strong medicine' of holding the statute facially overbroad." The appellate court observed that "as-applied challenges will properly safeguard the rights that the First Amendment enshrines."

#Social Media

United States v. Aigbekaen, 949 F.3d 713 (4th Cir. 2019)

Acting on a tip from a minor, the government seized three electronic devices from the defendant on his return to the United States from abroad and conducted warrantless forensic searches of the data on the devices. Thereafter, the defendant was charged with and convicted of sex trafficking and related crimes. On appeal, he challenged the denial of his motion to suppress evidence derived from the searches. The district court held that the "border search" exception applied. The Fourth Circuit disagreed:

> Because Aigbekaen does not challenge any *routine* border searches, we need not decide whether or how the interests that underpin the border search exception constrain, in practice, the Government's broad and historic authority to conduct suspicionless searches of individuals and their effects at the border. *** Similarly, we need not determine what quantum of individualized suspicion, if any, beyond the familiar reasonable-suspicion standard is needed to justify a warrantless forensic search of a device at the border. (emphasis in original).
>
> *** where a search at the border is so intrusive as to require some level of individualized suspicion, the object of that suspicion must bear some nexus to the purposes of the border search exception in order for the exception to apply. Because no such nexus existed here, the warrantless, nonroutine forensic searches violated the Fourth Amendment. (citations omitted).

However, the court applied the good faith exception to the Warrant Requirement and affirmed the conviction.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Anzalone, 923 F.3d 1 (1st Cir. 2019)

Playpen was an online forum hosted on the Tor Network that allowed users to upload, download, and distribute child pornography. The FBI had taken control of Playpen and maintained the website live for two weeks to identify and arrest users. The defendant was identified as a Playpen user and indicted for possession and

receipt of child pornography. He moved to suppress evidence obtained pursuant to a Network Investigative Technique ("NIT") and to dismiss the indictment for outrageous government conduct. The district court denied both motions. The First Circuit affirmed. The appellate court held that the defendant's challenge to the NIT warrant under *Fed. R. Crim. P.* 41 and to the inapplicability of the *Leon* exception had been foreclosed by its earlier decision of *United States v. Levin*. The court also held that the totality of the circumstances set forth in the NIT warrant established the existence of probable cause. The First Circuit then rejected the defendant's argument that the Government's conduct in running the website was so outrageous as to require the dismissal of the indictment, although the court observed that "the strategy that the government employed *** falls close to the line. In an ideal world, there would be effective ways to intercept individuals who trade and distribute child pornography online other than running a child pornography website for two weeks. But we live in a less than ideal world. Ultimately, we agree with the district court that the FBI's Playpen sting does not clear the high bar we have set for the outrageous government conduct defense to succeed."

#Miscellaneous

United States v. Asgari, 918 F.3d 509 (6th Cir. 2019)

The Government suspected that the defendant, born in Iran, lied on his visa application and transmitted scientific information to Iran in violation of U.S. law. A magistrate judge issued a warrant in 2013 to search the defendant's email account for evidence of these crimes. Based on information uncovered from that search the Government secured a second warrant in 2015 to search subsequent emails. The district court granted the defendant's motion to suppress evidence secured through the warrants, finding that the application for the first warrant did not demonstrate the existence of probable cause and the good faith exception to the Warrant Requirement did not apply. The Sixth Circuit reversed. As to probable cause, the appellate court held that, "it doesn't matter because the *Leon* good-faith rule applies." First, the supporting affidavit for the 2013 warrant alleged facts sufficient that "investigators operating in good faith reasonably could have thought the warrant was valid." Second, although there were omissions from and "technically inaccurate" statements in the affidavit, none led to a deliberate or reckless falsehood.

#Fourth Amendment – Good Faith Exception

United States v. Babcock, 924 F.3d 1180 (11th Cir. 2019)

> In this case, police officers investigating a domestic disturbance confiscated a suspect's cell phone and held it for two days before eventually obtaining a warrant to search it. The appeal before us presents two Fourth Amendment questions. First, was the seizure justified on the ground that the officers had reasonable suspicion to believe that the phone's owner was engaged in criminal wrongdoing—was it, in effect, a permissible 'Terry stop' of the phone? We hold that it was not. Second, in the particular circumstances of this case, did the officers have probable cause to believe not only that the phone's owner had committed a crime and that the phone contained evidence of that crime, but also that the suspect would likely destroy that evidence before they could procure a warrant? We hold that they did. Accordingly, and on that ground, we affirm the district court's order denying the motion to suppress.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

United States v. Bell, 925 F.3d 362 (7th Cir. 2019)

An individual who stole firearms brokered a deal with the defendant to sell the weapons. The individual was arrested for another offense, agreed to cooperate, and implicated the defendant. The cooperation included the individual showing an FBI agent a photo of a weapon that the defendant supposedly texted to the individual. When the defendant was arrested an officer seized the defendant's flip phone. The officer opened the phone. Its home screen showed a weapon that might have been a stolen weapon. Thereafter, the FBI secured two warrants to search the defendant's phone. One warrant application referred to the warrantless search. The other did not. The defendant moved to quash his arrest warrant and suppress evidence obtained from the phone, arguing that, without the information from the warrantless first search, probable cause was lacking for both. The district court denied the motion, concluding that: (1) the warrantless search violated the Fourth Amendment; and (2) even striking the information secured through the warrantless search, probable cause exited for issuance of the two warrants. On appeal, the court of appeals accepted that the warrantless search was illegal. However, there was an independent source for the photo. Moreover, even after the exclusion of the "tainted information," probable cause existed for both warrants and law enforcement would have sought the warrants even if it was unaware of the fruits of the warrantless search. The court of appeals also declined to remand for a *Franks* hearing.

#Fourth Amendment – Warrant Required or Not

United States v. Brewer, 915 F.3d 408 (7th Cir. 2019)

The defendant and his girlfriend "traveled the country robbing banks, a la Bonnie and Clyde." The Government secured a warrant from an Indiana state judge for real-time GPS vehicle monitoring and tracked the defendant's car to California where he and his girlfriend committed a robbery. He was arrested and convicted of bank robbery and argued on appeal, among other things, that the Government violated the Fourth Amendment by tracking him to California when the warrant only permitted monitoring in Indiana. The Seventh Circuit rejected the argument, concluding that there was no remedy under the Fourth Amendment for "noncompliance with a state-based, ancillary restriction in the warrant." (footnote omitted).

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Carpenter, 926 F.3d 313 (6th Cir. 2019)

"This case returns on remand from the Supreme Court." The Sixth Circuit affirmed the defendant's conviction, concluding that the FBI agents who collected the defendant's CSLI pursuant to the SCA did so in good faith.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Diggs, 385 F. Supp. 3d 648 (N.D. Ill. 2019)

The defendant and others were charged under the Hobbs Act for robbing a jewelry store. While investigating the robbery a detective obtained without a search warrant from a third party more than a month's worth of GPS location data for a vehicle associated with the defendant. The data was secured from a business that extended credit to the defendant's wife to buy the car. The wife's contract included this provision: "If your vehicle has an electronic tracking device, you agree that we may use this device to find the vehicle." Defendant moved to suppress the evidence derived from the warrantless search. The district court granted the motion. First, the court found that the GPS data "fits squarely within the scope of the reasonable expectation of privacy identified by the *Jones* concurrences and reaffirmed in *Carpenter*." The court rejected the Government's argument that the third-party doctrine applied, concluding that the detailed record of the defendant's movements made the application of that doctrine inconsistent with *Carpenter*. The court then held that, consistent with *Byrd v. United States,* the defendant had standing to challenge the search. The court rejected application of the good faith

exception because there was no binding Seventh Circuit precedent on point at the time of the search on which a reasonable officer could have relied. Finally, the court held that the contract language did not give the company permission to continuously track the vehicle for any purpose.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

United States v. Donahue, 726 Fed. App'x 3 (2d Cir. 2018) (Summary Order)

The defendant pled guilty to receipt of child pornography. He was sentenced to a term of imprisonment followed by 20 years' supervised release. A special condition was imposed that prohibited the defendant from having direct or indirect contact with a minor "through another person or through a device" unless he were supervised. After his release from prison the probation office filed a revocation petition because, among other things, the defendant used his employer's computer to search for child pornography. The defendant admitted to the violations and was sentenced to another term of imprisonment and 20 years' supervised release. The district court re-imposed a special condition that the defendant not have unsupervised contact with minors. The court delegated to the probation office the defendant's contact with his nine-year-old son who lived in Virginia. The defendant challenged this prohibition and delegation. The Second Circuit reversed and remanded because the district court had not explicitly identified the sentencing goal of the condition, had not clarified whether the goal was to protect the defendant's son, and had not made clear whether the father-son relationship was sufficiently established to merit constitutional protection. The appellate court held that the delegation to probation might be impermissible.

#Probation and Supervised Release

United States v. Elbaz, 396 F. Supp. 3d 583 (D. Md. 2019)

The defendant was charged with one count of conspiracy to commit wire fraud and three counts of wire fraud. In connection with its investigation the Government collected millions of documents. Knowing that some might be protected under the attorney-client or some other privilege, the Government established a "filter team" to identify and separate privileged and nonprivileged materials before turning the latter over to the prosecution team. Any privileged documents for which the defendant held the privilege or was a recipient of the communication were provided to the defendant and her attorneys. Other privileged documents not

related to the defendant were identified on a privilege log which was provided to them. Once discovery began the Government produced the nonprivileged documents to the defendant after applying search terms to ensure that only relevant documents were produced. However, the prosecution team did not conduct a manual review because, "according to the Government, the volume was too large for it to both review each document and produce the files to Elbaz in accordance with the discovery schedule." **To make a long story short,** unfiltered materials were uploaded to a Relativity database and the prosecution team "accessed or are presumed to have accessed 137 potentially privileged communications, 103 of which represent unique communications or conversations, once duplicates or near-duplicates are excluded." The defendant moved to dismiss the indictment or disqualify the prosecution team. The district court found no violation of the Sixth Amendment right to counsel. It rejected the defendant's argument that the Government's possession of attorney-client confidential information was a *per se* violation and found that the defendant had failed to establish either intentional misconduct or prejudice. Thus, neither dismissal of the indictment nor disqualification was warranted, "particularly where the Government's voluntary decision [to] replace the prior members of the trial team with three new trial attorneys with no earlier involvement in this case has eliminated any argument of prejudice to Elbaz." However, the court ordered that certain privileged email and related communications be excluded from evidence at trial. The court did extend a note of caution to the Government:

> the Prosecution Team's request to have some of the contents of two hard drives containing thousands of unfiltered documents uploaded to the Relativity database was a significant error in judgment not justified by a perceived need to meet discovery deadlines. And concern about meeting deadlines should have been addressed through a motion to extend the deadline rather than engaging in shortcuts without considering the potential consequences. The Court trusts that the Government will take all necessary steps to avoid similar errors in the future and will hold the Government fully accountable for any additional lapses.

#Discovery Materials

#Miscellaneous

#Sixth Amendment – Assistance of Counsel

United States v. Elmore, 917 F.3d 1068 (9th Cir. 2019)

Following a drive-by murder in 2012, the police obtained a State warrant that authorized the seizure of the defendant's historical CSLI. The application for the warrant incorporated facts learned by the police in the investigation of the murder

and stated that those facts appeared to demonstrate the existence of probable cause to believe that the CSLI could lead to the identification of the murderer. However, the defendant was barely mentioned in the affidavit and the affidavit did not point to the defendant. After the CSLI data was secured, the defendant was indicted by a federal grand jury on four counts related to the murder and moved to suppress the CSLI data. The district court granted the motion, finding that probable cause had not been shown to link the defendant to the murder or that the defendant was in the area of the murder at the time it was committed. The district judge also rejected application of the *Leon* exception to the Warrant Requirement. The Ninth Circuit reversed. The court held that, "[t]he affidavit's scant and innocuous references to Gilton do not establish a 'fair probability' that evidence of the crime would be found in Gilton's location data." The Ninth Circuit also rejected the Government's argument that two inferences could support the finding of probable cause. However, the court held that the *Leon* exception applied:

> In light of the prevailing belief in 2012 that CSLI data was not protected by the Fourth Amendment, we conclude that there was no 'willful' or 'grossly negligent' error here where the officers nevertheless took the precautionary step of seeking a warrant and provided ample factual background by which the magistrate could reach his own determination of the existence of probable cause. Although we conclude that the magistrate's determination was erroneous, we hold that the police here were not required to second-guess the determination of a neutral and detached magistrate. As such, we conclude that application of the exclusionary rule to Gilton's CSLI data would have no 'appreciable deterrent' effect and is thus unwarranted. (footnote omitted).

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Fall, 955 F.3d 363 (4th Cir. 2020)

The defendant had been living with his parents when his niece came to stay with him. The niece's boyfriend opened the defendant's laptop and found at least one image of child pornography. Then the niece found images on that laptop and another. That led to a trip by the niece to the police, the discovery of more images, more devices, and more images. The police secured a warrant and then seized various devices. The defendant moved to suppress everything. That was denied and he was convicted of receipt, possession, and transportation of child pornography. The Fourth Circuit affirmed. It began with consideration of the private search doctrine and noted that, "[w]hile we have not addressed the private search doctrine in the context of electronic devices, our sister circuits have utilized varying

approaches when confronted with this issue." However, the court did not address "the outer boundaries of the private search doctrine in the context of electronic searches for this Circuit." Instead, the court held that the good faith exception to the Warrant Requirement applied. The warrant was not facially deficient even though the supporting affidavit contained "potentially problematic observations."

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Garay, 938 F.3d 1108 (9th Cir. 2019)

Police attempted to stop a vehicle driven by the defendant for a traffic violation. He led them on a high speed chase, crashed the vehicle, and attempted to flee on foot. He was arrested and a search of his person revealed a substantial amount of cash and illegal drugs. Then, as they arranged to have the wrecked vehicle towed, the police searched the vehicle and found weapons, ammunition, and cell phones, one of which was claimed by a passenger in the vehicle. The police filled out an inventory sheet, although they did not list all the property seized. Police then secured a warrant to search the contents of both cell phones based on an officer's affidavit that described the events that led up to the discovery of the phones and the officer's knowledge that "individuals who possess firearms take pictures of them and communicate via text messages to further their criminal activity." A second warrant was issued after the case had been referred to federal prosecution. That warrant was issued based on similar information and the "'collective experiences' of law enforcement agents that felons prohibited from possessing guns use mobile phones to coordinate buying and selling guns." The defendant was convicted of being a felon in possession of a firearm and, on appeal, challenged the warrantless seizure of his phone and the adequacy of the affidavits. The Court of Appeals affirmed the conviction. First, it held that the police conducted a reasonable inventory search even though the inventory sheet contained errors:

> we find no reason to conclude that the inventory search was used to rummage for evidence. Given the circumstances leading up to the search, the officers no doubt expected to find evidence of criminal activity inside the vehicle. But that expectation would not invalidate an otherwise reasonable inventory search.

Next, the court held that the affidavits were adequate:

> We have long held that affiants seeking a warrant may state conclusions based on training and experience without having to detail that experience. *** We have also held that magistrate judges may "rely on

> the conclusions of experienced law enforcement officers regarding where evidence of a crime is likely to be found." ***
>
> Further, there was a sufficient factual basis for both magistrate judges to conclude, independently of the affiants' beliefs, that evidence might be found on Garay's cell phone. Garay relies on authorities in which the warrant applications had contained no factual basis from which to connect the place to be searched with the evidence sought. *** But here, the affidavits explained all of the circumstances leading up to the search of the car that had been wrecked, and explained that Garay was then arrested for having drugs and cash on his person. These facts, coupled with the affiants' experience and beliefs, provide a reasonable basis to infer that evidence tying Garay to the criminal activity of which he was suspected might be found on the cell phone. Magistrate judges may, as they likely did here, draw their own reasonable inferences about where evidence might be kept based on the nature of the suspected offense and the nature of the evidence sought. ***
>
> We owe "great deference" to magistrate judges' probable-cause findings. *** The district court correctly determined that the affidavits supporting both warrants in this case gave rise to at least a fair probability that evidence of a crime would be found on Garay's cell phone.

#Fourth Amendment – Warrant Required or Not

United States v. Gatto, 313 F. Supp. 3d 551 (S.D.N.Y. 2018)

The defendants were charged with conspiracy to commit wire fraud, wire fraud, and money laundering. The charges arose from an alleged scheme to bribe high school basketball players in exchange for commitments to attend certain universities and retain the defendants' services. Law enforcement seized the defendants' cell phones incident to their arrests and applied for search warrants. A magistrate judge issued the warrants, which specified the categories of evidence responsive to the warrants. Each warrant listed targeted search techniques that utilized the Cellebrite program to search but stated that, depending on the circumstances, "a complete review of the seized ESI may require examination of all of the seized data to evaluate its contents and determine whether the data is responsive to the warrant" (footnote omitted). The defendants moved to suppress evidence derived from the searches. The district court denied the motion because: (1) probable cause existed to believe that the defendants' phones were used for relevant communications based on information derived from wiretaps; (2) the magistrate judge had a "sufficiently substantial basis" to conclude that probable cause existed as to one defendant's second phone based an agent's statement that

the defendant was on his way to a meeting and had used numerous cell phones to commit the offenses; and (3) the warrants satisfied the Particularity Requirement because the warrants "listed the criminal offenses with which defendants had been charged ***. Each warrant described also the places—*i.e.*, the specific cell phones – to be searched. And each specified exactly the types of content that fell within the scope of the warrant" (footnote omitted). The court also rejected the defendants' argument that the authorization to search all content rendered the warrants overbroad: "'Such an invasion of a criminal defendant's privacy is inevitable, however, in almost any warranted search because in "searches for papers," it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized.'" (citation omitted). Finally, the court concluded that, even if the warrants were defective, the *Leon* exception to the Warrant Requirement would be applicable.

#Discovery Materials

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

United States v. Goldstein, 914 F.3d 200 (3d Cir. 2019)

> We granted Appellant Jay Goldstein's petition for rehearing to address the effect of the Supreme Court's recent decision in *Carpenter v. United States* on our prior panel decision, *United States v. Stimler*. In *Stimler*, we held that the District Court properly denied Goldstein's motion to suppress his cell site location information (CSLI) because Goldstein had no reasonable expectation of privacy in his CSLI, and, therefore, the government did not need probable cause to collect this data. *Carpenter* sets forth a new rule that defendants do in fact have a privacy interest in their CSLI, and the government must generally obtain a search warrant supported by probable cause to obtain this information. However, we still affirm the District Court's decision under the good faith exception to the exclusionary rule because the government had an objectively reasonable good faith belief that its conduct was legal when it acquired Goldstein's CSLI.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Gratkowski, 964 F.3d 307 (5th Cir. 2020)

The defendant entered a conditional guilty plea after his motion to suppress had been denied to receipt of child pornography and accessing websites with intent to view child pornography. He paid to download the child pornography with Bitcoin and the Government discovered the defendant's identity by analyzing a blockchain transaction after having served a grand jury subpoena on a virtual currency exchange. That led to a warrant to search the defendant's home, where evidence of his crimes was found. On appeal, the defendant, relying on the limitation of the third-party doctrine in *Carpenter v. United States*, argued that he had a reasonable expectation of privacy in the records of his Bitcoin transactions on the blockchain and the exchange such that the evidence derived from those sources should have been suppressed. The Fifth Circuit affirmed, concluding that the information on the blockchain was "far more analogous to the bank records in *Miller* and the telephone call logs in *Smith* than the CSLI in *Carpenter*." The court also concluded that the defendant lacked a privacy interest in his information because it was publicly available on the blockchain. Moreover, even if the Fifth Circuit were to apply *Carpenter*, in would have upheld the conviction based on the good faith exception to the Warrant Requirement.

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Good Faith Exception

#Third-Party Doctrine

United States v. Guerrero-Torres, 762 Fed. App'x 873 (11th Cir. 2019) (*per curiam*)

The defendant was a suspect in an ongoing missing child investigation. Law enforcement arranged to meet with him. When they eventually met, and after the police rang his cell phone a number of times with no answer, the defendant stated that the phone had been damaged by rainwater and would not turn on. He also stated that, because he believed the phone did not work properly, he threw it away in a public area. However, the defendant said it was his intent to keep the content secret and that he believed the password would keep others from accessing content. A landscaper found the phone and the police retrieved it. Thereafter, the defendant was arrested. After the defendant had been questioned a digital forensic specialist extracted data from the phone. Images of child pornography were found. In subsequent interrogations the defendant admitted that he knew the phone had been found by the landscaper but did not ask it be returned. He also volunteered what he apparently thought was the complete password to the police (it was not). He also

told the police that he was not surprised to learn that the images were found because "you find everything on phones." The district court denied the defendant's motion to suppress, finding that the defendant had abandoned the phone. He was found guilty of possession and production of child pornography. The Eleventh Circuit affirmed the convictions. The court held that the defendant failed to establish a subjective expectation of privacy in the content such that he lacked standing to contest the search. The court did not address "whether the contents of a password-protected cellphone can be abandoned" or whether any exceptions to the Warrant Requirement justified the warrantless search.

#Fourth Amendment – Warrant Required or Not

United States v. Harris, 881 F.3d 945 (6th Cir. 2018)

The defendant was convicted of securities and wire fraud. He argued on appeal, among other things, that the trial court had erred in failing to investigate potential extraneous influence on a juror. The defendant presented evidence that someone had viewed his LinkedIn profile during the trial and that that person was the live-in girlfriend of a juror. This and other facts led the defendant to conclude that the juror had discussed the trial with his girlfriend. The trial court denied the defendant's motion to conduct a hearing pursuant to *Remmer v. United States*, 347 U.S. 227 (1954). The Sixth Circuit reversed and remanded: "Although Harris did not establish that Juror 12 was exposed to unauthorized communication, Harris did present a colorable claim to extraneous influence, which necessitated investigation." The district court had abused its discretion by neither holding a hearing nor allowing the defendant to conduct an investigation.

#Social Media

#Trial-Related

United States v. Hasbajrami, 945 F.3d 641 (2nd Cir. 2019)

The defendant was arrested at an airport and pled guilty to attempting to provide material support to a terrorist organization. "After he pleaded guilty, the government disclosed, for the first time, that certain evidence *** had been derived from information obtained by the government without a warrant pursuant to its warrantless surveillance program under Section 702 of the FISA Amendments Act of 2008." The defendant withdrew his plea and moved to suppress. That motion was denied and he again pled guilty. He challenged the denial of his motion on appeal on Fourth Amendment grounds. The Court of Appeals held:

> the collection of the communications of United States persons incidental to the lawful surveillance of non-United States persons located abroad

> does not violate the Fourth Amendment and that, to the extent that the government's inadvertent targeting of a United States person led to collection of Hasbajrami's communications, he was not harmed by that collection. *** Because there is insufficient information in either the classified or the public record in this case to permit us to determine whether any such querying was reasonable, and therefore permissible under the Fourth Amendment, we REMAND the case to the district court for further proceedings consistent with this opinion.

#Fourth Amendment – Warrant Required or Not

United States v. Highbull, 894 F.3d 988 (8th Cir. 2018)

The defendant pled guilty to one count of sexual exploitation of a child but reserved the right to challenge the denial of his motion to suppress evidence recovered from a cell phone that his girlfriend gave law enforcement. The district court denied the motion, finding that the girlfriend acted as a private actor and not as a government agent. The girlfriend retrieved the phone from the defendant's vehicle after her son had called the police to report that the defendant was harassing his mother, the girlfriend. She told the police on their arrival that there were images of her infant daughter on the phone but she could not find these. The police took the phone, uncovered the images, and charged the defendant. The Court of Appeals affirmed the defendant's conviction. It concluded that, although the police knew of and acquiesced in the girlfriend's search of the vehicle, they did not request it be done and that her purpose in doing so was for a compelling personal motive (the protection of her daughter).
#Fourth Amendment – Warrant Required or Not

United States v. Holena, 906 F.3d 288 (3d Cir. 2018)

The defendant repeatedly visited an online chatroom to entice a fourteen-year old boy to have sex. The "boy" was an FBI agent. The defendant pled guilty to attempting to entice a minor to engage in sexual acts and was sentenced to ten years' imprisonment and lifetime supervised release. As a special condition, he was forbidden to use the Internet without the approval of his probation officer, had to submit to regular searches of his computer and home, and had to permit the installation of monitoring and filtering software on his computer. The defendant violated the terms of his supervised release twice, once by going online to update social media profiles and answer email and then by logging into Facebook without approval and lying about doing so. After each violation the court sentenced the defendant to incarceration and re-imposed the special conditions. At the latest hearing the judge imposed another lifetime ban, forbidding the defendant to

possess or use any computer, electronic communications device, or electronic device. The defendant appealed. The Court of Appeals reversed and remanded: (1) the conditions were contradictory; (2) the bans were "draconian" and made without adequate findings. Specifically, the court of appeals questioned the length and scope of the bans; and (3) the bans raised First Amendment concerns as these "limit an array of First Amendment activity. And none of that activity is related to his [the defendant's] crime. Thus, many of the restrictions on his speech are not making the public safer."

#Probation and Supervised Release

United States v. Howard, 947 F.3d 936 (6th Cir. 2020)

> In our digitized age, enigmatic shorthand flourishes with new forms of written communication—from texts, to Instant Messaging, to Tweets, to Snapchats, to Instagram stories—in which the deciphering of acronyms, initialisms, and emojis can be difficult. But, we still have 'old school' forms of communication, like phone calls and voicemails—in which one's voice is used and words are not so easily lost in abbreviation or pictorialization. Usually unambiguous speech is fortunate, but sometimes, it can be quite disturbing. The latter is the case here, where the intent and purpose of a voicemail message came across as chillingly clear.
>
> Atrel Howard Jr. appeals his conviction of transmitting a threat in interstate commerce to murder former U.S. Attorney General Eric Holder in violation of 18 U.S.C. § 875(c). The issues before us are (1) whether the government violated Howard's Fifth and Sixth Amendment rights and deprived the district court of jurisdiction by omitting the essential *mens rea* element as required by *Elonis v. United States* [*q.v.*] ***; (2) whether the district court erred in instructing the jury as to what type of communication would constitute a 'true threat' ***; and (3) whether the government presented sufficient evidence to support Howard's conviction. For the reasons explained below, none of these arguments have merit. We therefore AFFIRM the judgment of conviction. (footnote omitted).

#Social Media

United States v. Khan, 937 F.3d 1042 (7th Cir. 2019)

"Over a seven-week span, Mohammed Khan used Facebook and his job as an Uber driver to threaten and prepare for mass murder." He was indicted and convicted for making interstate threats to injure others. On appeal, he argued that the indictment was insufficient. The court of appeals rejected that argument. The court also

rejected the defendant's argument that the instructions failed to charge that a "true threat" was required to convict.

#Miscellaneous

#Social Media

United States v. Kolsuz, 890 F.3 133 (4th Cir. 2018)

> Hamza Kolsuz was detained at Washington Dulles International Airport while attempting to board a flight to Turkey because federal customs agents found firearms parts in his luggage. After arresting Kolsuz, the agents took possession of his smartphone and subjected it to a month-long, off-site forensic analysis, yielding a nearly 900-page report cataloguing the phone's data. The district court denied Kolsuz's motion to suppress, applying the Fourth Amendment's border search exception and holding that the forensic examination was a nonroutine border search justified by reasonable suspicion. Kolsuz ultimately was convicted of attempting to smuggle firearms out of the country and an associated conspiracy charge.
>
> Kolsuz now challenges the denial of his suppression motion. First, he argues that the forensic analysis of his phone should not have been treated as a border search at all. According to Kolsuz, once both he and his phone were in government custody, the government interest in preventing contraband from crossing the border was no longer implicated, so the border exception should no longer apply. Second, relying chiefly on *Riley v. California*, [] 134 S. Ct. 2473 [] (2014) (holding that search incident to arrest exception does not apply to searches of cell phones), Kolsuz urges that the privacy interest in smartphone data is so weighty that even under the border exception, a forensic search of a phone requires more than reasonable suspicion, and instead may be conducted only with a warrant based on probable cause.
>
> We agree with the district court that the forensic analysis of Kolsuz's phone is properly categorized as a border search. Despite the temporal and spatial distance between the off-site analysis of the phone and Kolsuz's attempted departure at the airport, the justification for the border exception is broad enough to reach the search in this case. We also agree with the district court that under *Riley*, the forensic examination of Kolsuz's phone must be considered a nonroutine border search, requiring some measure of individualized suspicion. What precisely that standard should be – whether reasonable suspicion is enough, as the district court concluded, or whether there must be a warrant based on probable cause, as Kolsuz suggests – is a question we need not resolve: Because the agents who conducted the search reasonably relied on precedent holding that no warrant was required,

> suppression of the report would be inappropriate even if we disagreed. Accordingly, we affirm the judgment of the district court.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

United States v. Lickers, 928 F.3d 609 (7th Cir. 2019)

The defendant was observed by undercover officers sitting alone in a parked car while looking at his phone and watching a family with young children in a nearby playground. When they approached the vehicle, they observed a towel in the defendant's lap and the defendant's demeanor and behavior changed. The officers directed the defendant to remove the towel and, doing so, exposed his genitals. The defendant admitted that he had been pleasuring himself while looking at Craigslist. The officers directed the defendant to exit the vehicle, at which time the officers smelled marijuana. A dog search was conducted, marijuana found in the vehicle, prompting an inventory search resulting in the officers recovering a cell phone, laptop, and digital camera. A State judge issued a warrant to search the devices and the search revealed sexually explicit images of young children. The defendant was indicted on State drug and child pornography charges. A State judge suppressed all the evidence, finding that there was no basis to remove the defendant from his vehicle and no basis to detain him pending the arrival of the dog. All State charges were then dismissed. Federal authorities then entered the picture and sought a warrant for the phone and laptop. The application included a copy of the State warrant application and disclosed that the earlier search uncovered child pornography. A federal judge issued a warrant. The resulting search uncovered pornographic images and videos of young children, and the defendant was indicted for possessing and transporting child pornography. He moved to suppress the evidence. That was denied by the district judge, who found that the defendant's suspicious behavior created reasonable suspicion necessary to seize the defendant when he was ordered out of the car. The district judge also rejected the defendant's challenge to the federal warrant. The defendant was convicted of possession of child pornography and sentenced to a term of imprisonment and lifetime supervised release. The Seventh Circuit affirmed: (1) the officers had reasonable suspicion to believe that the defendant had committed a crime and to detain him for a brief time under *Terry v. Ohio*, 392 U.S. 1 (1968); (2) the dog's alert to marijuana and other circumstances furnished probable cause for the search of the vehicle; and (3) once marijuana was found, probable cause existed for the inventory search and seizure of the devices. Turning to the State and federal warrants, the Seventh Circuit concluded that both lacked probable cause. However,

the FBI agent who obtained and executed the federal warrant acted in good faith and the *Leon* good faith exception to the Warrant Requirement was applicable. Finally, the appellate court held that the district court had not abused its discretion in imposing the lifetime supervised release.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Probation and Supervised Release

United States v. Loera, 923 F.3d 907 (10th Cir. 2019)

While executing a warrant to search the defendant's home for evidence of computer fraud, FBI agents discovered child pornography on four of the defendant's CDs. The agents continued their search for evidence of computer fraud while one agent continued to search the CDs and another searched for evidence on other devices. The agents seized devices that appeared to contain evidence of computer fraud as well as the four CDs. One week later, an agent reopened the CDs without a warrant so that he could describe the images in an application for a second warrant to search all seized devices for child pornography. A magistrate judge issued the second warrant and the agents thereafter found more evidence of child pornography. The district court denied the defendant's motion to suppress. The defendant pled guilty to receipt of child pornography but reserved his right to appeal. The Tenth Circuit affirmed the denial of the motion to suppress: (1) there were no pretextual motivations on the part of the FBI in obtaining the first warrant; (2) the search by the two agents was reasonable as they continued looking for evidence of computer fraud; (3) the warrantless search one week later was unlawful because it exceeded the scope of the first warrant and no exception to the Warrant Requirement applied; (4) excising descriptions of child pornography obtained during the unlawful search, the application for the second warrant did not demonstrate the existence of probable cause; the *Leon* "exception does not apply *** because the illegality at issue stems from unlawful police conduct, rather than magistrate error, and therefore the deterrence purposes of the Fourth Amendment are best served by applying the exclusionary rule"; and (5) "the district court's supportable findings demonstrate by a preponderance of the evidence that the FBI would have inevitably discovered the child pornography evidence on Loera's electronic devices through lawful means independent from *** [the] unlawful second search."

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. May-Shaw, 955 F.3d 563 (6th Cir. 2020)

The defendant entered a conditional guilty plea to conspiracy to distribute cocaine. On appeal, he challenged, among other things, the denial of his motion to suppress evidence derived from the warrantless surveillance of his car in a parking lot near his apartment building and a covered carport over a 23-day period from a camera affixed to a telephone pole on a public street and from cameras in a surveillance van parked in the lot. The court of appeals affirmed:

> Because the officers' use of the pole camera did not involve any sort of physical intrusion into a constitutionally protected area, May-Shaw must show that he had a reasonable expectation of privacy in the carport. Cobbling together dicta from several Fourth Amendment cases, he argues that, although police may permissibly observe the curtilage of a home for a short period of time, for example with an aerial flyover ***, long-term video surveillance of a home's curtilage is problematic under the Fourth Amendment ***. There is at least some support for that proposition, as this court and five Justices of the Supreme Court have noted concerns about the problems with long-term warrantless surveillance. ***
>
> Although this argument may be compelling in theory, as applied here, it is foreclosed by this circuit's case law, which has consistently held that this type of warrantless surveillance does not violate the Fourth Amendment. For example, in *United States v. Houston*, we held that affixing a video camera to the top of a utility pole to record the defendant's front porch over a ten-week period did not violate the defendant's Fourth Amendment rights because "agents only observed what [the defendant] made public to any person traveling on the roads" surrounding his home. 813 F.3d 282, 288 (6th Cir. 2016). We rejected the defendant's claim that the length of the period of monitoring made the surveillance constitutionally unreasonable, reasoning that it is the possibility—not the practicability—that the police could have themselves sat atop the utility pole and observed the same view for every waking moment of a ten-week period that is critical. *Id.* at 289–90. That reasoning was applied in *United States v. Powell*, in which we held that the warrantless surveillance of three buildings through the installation of video cameras on three public utility poles, for periods of up to 90 days each, did not violate the defendants' Fourth Amendment rights. 847 F.3d 760, 773 (6th Cir. 2017). And, even assuming that May-Shaw is correct that the carport constitutes the curtilage of his apartment *** that is of no consequence to the constitutional analysis of the video surveillance. We held in *Houston* that warrantless video surveillance of the defendant's front porch, which is unquestionably within the curtilage of his home,

> did not violate his reasonable expectation of privacy because the camera "captured only views that were plainly visible to any member of the public who drove down the roads bordering" his home. *Houston*, 813 F.3d at 288.
>
> May-Shaw contends that the pole camera did not provide the same vantage point that was readily accessible from the street. The district court, however, held that the area surveilled by the pole camera was readily accessible from a public vantage point. This is a factual finding that is reviewed for clear error. Officer Mesman testified that the vantage point from the pole camera was the same as the vantage point from the street, and nothing in the record contradicts that assertion. Therefore, the district court's factual finding that the pole camera recorded the same view enjoyed by an individual standing on Norman Avenue was not clearly erroneous.
>
> Furthermore, the surveillance footage and photos here did not 'generate[] a precise, comprehensive record of [May-Shaw's] public movements that reflects a wealth of detail about [his] familial, political, professional, religious, and sexual associations' ***.
>
> May-Shaw has not demonstrated that when the government surveilled the carport for twenty-three days, it violated his reasonable expectation of privacy and thus conducted an unconstitutional search. We find no error in the district court's judgment that the pole-camera surveillance did not violate May-Shaw's Fourth Amendment rights. (citations omitted in part).

#Fourth Amendment – Warrant Required or Not

United States v. Mecham, 950 F.3d 257 (5th Cir. 2020)

This appeal arises out of a child pornography conviction involving a very disturbing set of facts:

> The defendant superimposed the faces of actual children on pornographic photos of adults to make it appear that the minors were engaged in sexual activity. Unlike virtual pornography, this 'morphed' child pornography uses an image of a real child. Like virtual pornography, however, no child actually engaged in sexually explicit conduct.

The defendant challenged his conviction, arguing that the morphed child pornography was protected speech under the First Amendment. The Fifth Circuit, although noting a disagreement among the circuit court of appeals, affirmed the conviction:

> Those [prior Supreme Court] decisions have consistently cited the interest in preventing reputational and emotional harm to children as a justification for the categorical exclusion of child pornography from the First Amendment. *Free Speech Coalition* and every circuit to consider the question have recognized that morphed child pornography raises this threat to a child's psychological well-being. We conclude that because morphed child pornography depicts an identifiable child, it falls outside the First Amendment. Mecham's conviction is affirmed.

What is particularly disturbing is that the superimposed images were of the defendant's grandchildren: "After Mecham spent many years interacting with his grandchildren, his daughter prevented him from having any contact with her children. By creating the images, he hoped to get back at his family for cutting him off."

#Miscellaneous

United States v. Moore-Bush, 963 F.3d 29 (1st Cir. 2020)

In mid-2017, law enforcement affixed, without any judicial authorization, a pole camera on a public utility pole across from a home that was the site of suspected criminal activity and used it to observe the exterior of the home over an eight-month period. The defendants lived at the home "off and on" during the surveillance. After the defendants were indicted on drug-related offenses the district court granted their motions to suppress evidence from the pole camera and the fruits of that evidence, concluding that *Carpenter v. United States* (*q.v.*) allowed it to reevaluate preexisting First Circuit case law that held that pole camera surveillance did not require a warrant. The Court of Appeals reversed on the basis of *stare decisis*:

> This appeal by the prosecution raises the question of whether the Supreme Court's opinion in Carpenter v. United States, ***, a cell phone location automatic tracking technology case, provides a basis for departing from otherwise binding and factually indistinguishable First Circuit precedent in United States v. Bucci, 582 F.3d 108 (1st Cir. 2009), and Supreme Court precedent, including Katz v. United States, 389 U.S. 347 [] (1967), on which Bucci is based. In departing from that precedent and suppressing evidence obtained from a pole camera, the district court erred by violating the doctrine of stare decisis.
>
> Under the doctrine of stare decisis, all lower federal courts must follow the commands of the Supreme Court, and only the Supreme Court may reverse its prior precedent. The Court in Carpenter was concerned with the extent of the third-party exception to the Fourth Amendment

law of reasonable expectation of privacy and not with the in-public-view doctrine spelled out in Katz and involved in this case.

Carpenter was explicit: (1) its opinion was a 'narrow' one, (2) it does not 'call into question conventional surveillance techniques and tools,' and (3) such conventional technologies include 'security cameras.' *** Pole cameras are a conventional surveillance technique and are easily thought to be a species of surveillance security cameras. Thus, Carpenter, by its explicit terms, cannot be used to overrule Bucci.

The district court erred for other separate reasons as well. The Bucci decision firmly rooted its analysis in language from previous Supreme Court decisions ***The Court in Carpenter was clear that its decision does not call into question the principles Bucci relied on from those cases. ***

The district court also transgressed a fundamental Fourth Amendment doctrine not revoked by Carpenter, that what one knowingly exposes to public view does not invoke reasonable expectations of privacy protected by the Fourth Amendment. This understanding, as explained by Justice Scalia in Kyllo, was part of the original understanding of the Fourth Amendment at the time of its enactment. ***

Affirming the district court's order would mean violating the law of the circuit doctrine, that 'newly constituted panels in a multi-panel circuit court are bound by prior panel decisions that are closely on point.' *** Although there are two exceptions to the doctrine, 'their incidence is hen's-teeth-rare.' *** And neither exception is applicable here.

The argument made in support of the district court's suppression order is that the logic of the opinion in Carpenter should be extended to other technologies and other Fourth Amendment doctrines, and this extension provides a basis to overturn this circuit's earlier precedent in Bucci. Nothing in Carpenter's stated 'narrow' analysis triggers the rare second exception to the law of the circuit doctrine. ***

The defendants thus ask us to violate the vertical rule of stare decisis, that all lower federal courts must follow the commands of the Supreme Court and that only the Supreme Court may reverse its prior precedent, and the law of the circuit, binding courts to follow circuit precedent. *** Affirming the district court would also violate the original understanding of the Fourth Amendment.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Reddick, 900 F.3d 636 (5th Cir. 2018)

> Private businesses and police investigators rely regularly on 'hash values' to fight the online distribution of child pornography. Hash values are short, distinctive identifiers that enable computer users to quickly compare the contents of one file to another. They allow investigators to identify suspect material from enormous masses of online data, through the use of specialized software programs—and to do so rapidly and automatically, without the need for human searchers.
>
> Hash values have thus become a powerful tool for combating the online distribution of unlawful aberrant content. The question in this appeal is whether and when the use of hash values by law enforcement is consistent with the Fourth Amendment.
>
> For the Fourth Amendment concerns not efficiency, but the liberty of the people 'to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.' There is no precedent in our circuit concerning the validity of these investigative tools under the Fourth Amendment, and to our knowledge no other circuit has confronted the precise question before us. This case therefore presents an opportunity to apply established Fourth Amendment principles in this new context.
>
> One touchstone of our Fourth Amendment jurisprudence is that the Constitution secures the right of the people against unreasonable searches and seizures conducted by the government—not searches and seizures conducted by private parties. Under the private search doctrine, the Fourth Amendment is not implicated where the government does not conduct the search itself, but only receives and utilizes information uncovered by a search conducted by a private party.
>
> The private search doctrine decides this case. A private company determined that the hash values of files uploaded by Mr. Reddick corresponded to the hash values of known child pornography images. The company then passed this information on to law enforcement. This qualifies as a 'private search' for Fourth Amendment purposes. And the government's subsequent law enforcement actions in reviewing the images did not effect an intrusion on Mr. Reddick's privacy that he did not already experience as a result of the private search. Accordingly, we affirm the judgment of the district court.

#Fourth Amendment – Warrant Required or Not

United States v. Rickmon, 952 F.3d 876 (7th Cir. 2020)

The defendant entered a conditional guilty plea after the district court denied his motion to suppress evidence derived from a *Terry* stop of the vehicle in which he

was a passenger. The stop was based on a ShotSpotter report of gunshots. He challenged the denial of his motion on appeal. As framed by the Court of Appeals:

> One hundred police departments use a surveillance network of GPS-enabled acoustic sensors called ShotSpotter to identify gunfire, quickly triangulate its location, and then direct officers to it. As a matter of first impression, this case requires us to consider whether law enforcement may constitutionally stop a vehicle because, among other articulable facts, it was emerging from the source of a ShotSpotter alert.

The appellate court held that,

> [T]he circumstances here—the reliability of the police reports, the dangerousness of the crime, the stop's temporal and physical proximity to the shots, the light traffic late at night, and the officer's experience with gun violence in that area—provided reasonable suspicion to stop Rickmon's vehicle.

The court did not address the reliability of ShotSpotter:

> At certain points in this case, Rickmon has somewhat taken issue with ShotSpotter's reliability. A police department witness testified that, in general, ShotSpotter validates whether a sound is a gunshot within seconds; however, in these specific circumstances, the witness was unable to say how long that process took. The district court also received evidence that ShotSpotter is not always accurate and that officers may not solely rely on it to locate gunfire. As Rickmon points out, the record here does not demonstrate how often the Peoria Police Department received incorrect ShotSpotter reports or anything else attesting to the reliability of the system. Still, the witness was subject to cross-examination about ShotSpotter's reliability. *** Rickmon, for his part, declined to further challenge ShotSpotter's adequacy. *** We therefore take his argument as based on reasonable suspicion and need not reach the reliability of ShotSpotter. In some future decision, we may have to determine ShotSpotter's reliability where a single alert turns out to be the only articulable fact in the totality of the circumstances. *** But, in any event, this is not that case, given that 911 calls corroborated the ShotSpotter reports here and Rickmon himself was in the system's coverage zone. We express no further opinion on the matter.

#Admissibility

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Sam, Case No. CR19-0115-JCC, 2020 WL 2705415 (W.D. Wash. May 18, 2020)

The defendant had been indicted for various crimes. At the time of his arrest a cell phone was seized and an officer activated its display screen, which revealed the name "STREEZY." Thereafter, the FBI powered up the phone and took a photograph of the lock screen, which also showed the name. No warrant was secured for either examination. The defendant moved to suppress the evidence derived from both. The court found that the first examination might constitute either a search incident to arrest or an inventory search and directed supplemental briefing on the circumstances surrounding the examination as well as the relevant legal standard. The court granted the motion to suppress as to the second, concluding that the Government had gained evidence by physically intruding on a constitutionally protected area (the defendant's personal effects) "when the FBI powered on his phone to take a picture of the phone's lock screen." The court held that it need not address whether the defendant had a reasonable expectation of privacy because of the physical intrusion.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

United States v. Sawyer, 929 F.3d 497 (7th Cir. 2019)

The defendant entered a conditional guilty plea to possession of a firearm as a felon. On appeal, he challenged the denial of his motion to suppress evidence found during a search of his backpack, which he "left inside a home that he had entered unlawfully." The district court denied the motion, concluding that the defendant had no "legitimate expectation of privacy in the house and therefore none in the unattended backpack." The court of appeals affirmed: "Although the district court mischaracterized Sawyer's argument as an issue of 'standing,' it properly concluded, nonetheless, that Sawyer, as a trespasser, had no reasonable expectation of privacy ***." Moreover, the backpack search did not violate the Fourth Amendment because the owner of the home consented to a search of the home, which included the backpack: "An otherwise unreasonable search is permissible when a third party with common control over the searched premises consents, or when someone with apparent authority to consent does so."

#Fourth Amendment – Warrant Required or Not

United States v. Sesay, 937 F.3d 1146 (8th Cir. 2019)

The defendants were convicted of aggravated identity theft and conspiracy to commit bank fraud. On appeal, one argued, among other things, that the trial court had erred in denying his motion to suppress evidence derived from the warrantless examination by law enforcement of the guest registry of the motel where he had stayed. The appellate court rejected that argument on the basis of the third-party doctrine:

> While this doctrine does not extend to the novel phenomenon of cell phone location records ***, it encompasses checks and deposit slips retained by a bank, income tax returns provided to an accountant, and electricity-usage statistics tracked by a utility company. *** We conclude that Samaan likewise had no legitimate expectation of privacy in the identification card that he provided when registering at the motel. *Patel*'s ruling [*City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015) (*q.v.*)] in favor of hotel owners does not support Samaan's contention. The Court did not hold that *motel guests* have a privacy interest in registration records; to the contrary, the decision acknowledged that "hotel operators remain free to consent to searches of their registries." (citations omitted; emphasis in original).

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

United States v. Shipp, 392 F. Supp. 3d 300 (E.D.N.Y. 2019)

After an individual was shot, surveillance video of the incident was used to identify the defendant and he was arrested. Thereafter, a magistrate judge issued a warrant that authorized disclosure of a "substantial amount of information" from a Facebook account associated with the defendant. The defendant moved to suppress, arguing that the warrant was overbroad. The district court tended to agree: "In sum, the court is concerned that Facebook warrants of the kind at issue here unnecessarily 'authorize precisely the type of "exploratory rummaging" the Fourth Amendment protects against.'" (citation omitted). However, reliance on the warrant was not objectively unreasonable and, applying the good faith exception to the Warrant Requirement, the district judge denied the motion.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Social Media

United States v. Smith, 759 Fed. App'x 62 (2d Cir. 2019) (Summary Order)

A New York State trooper came across the defendant, who was passed out inside his vehicle parked on the side of a road. The defendant was visibly intoxicated. The defendant was put in the care of two forest rangers. The trooper searched the vehicle for the defendant's identification or a vehicle registration. While doing so the trooper came across an image on a tablet that the trooper thought was child pornography. The trooper seized the tablet. Just over a month later the trooper applied for a warrant. The warrant was issued and videos and images of child pornography were found on the tablet. The defendant was indicted for possession of child pornography, his motion to suppress denied, and he pled guilty to six counts. He reserved his right to appeal the denial of the motion to suppress. The Second Circuit declined to second-guess the district court when it determined that the trooper was credible in his testimony that the image he observed was in plain view. The defendant also argued that the failure of the police to "preserve the tablet's settings at the time of the seizure required the district court to infer that the factory settings had not been changed." The Second Circuit rejected this argument because there was no evidence that the police acted in bad faith. However, the Second Circuit reversed and remanded for a "fuller explanation and further findings" on whether the month-long delay in securing a warrant was reasonable.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Preservation and Spoliation

United States v. Taylor, 935 F.3d 1279 (11th Cir. 2019)

Both the majority and the dissenting opinions here use interesting language at times. That aside, here is how the majority summarized its ruling:

> James Taylor and Steven Smith are the latest in a long line of child-pornography consumers to argue that the evidence of their crimes should be suppressed because the warrant that led to its discovery—issued by a magistrate judge in the Eastern District of Virginia but purporting to authorize a nationwide, remote-access computer search—violated the Fourth Amendment. By our count, we become today the eleventh (!) court of appeals to assess the constitutionality of the so-called 'NIT warrant.' Although the ten others haven't all employed the same analysis, they've all reached the same conclusion—namely, that evidence discovered under the NIT warrant need not be suppressed. We find no good reason to diverge from that consensus here, but the case nonetheless calls for careful consideration, as it implicates several important issues.

> As an initial matter, did the NIT warrant violate Federal Rule of Criminal Procedure 41(b), which specifies where and in what circumstances a magistrate judge may issue a warrant—and relatedly, if the warrant did violate Rule 41(b), was that violation of constitutional magnitude? *We hold that because the magistrate judge's actions exceeded not only Rule 41(b) but also her statutorily prescribed authority under the Federal Magistrates Act, 28 U.S.C. § 636(a)—which circumscribes the scope of a magistrate judge's jurisdiction—the warrant was void ab initio, rendering any search purporting to rely on it warrantless and thus presumptively unlawful under the Fourth Amendment.*
>
> That leads us to the question of remedy, which we take in two parts: First, is exclusion required—without regard to the reasonableness of the officers' reliance—where, as here, the warrant was void from the outset, as Taylor and Smith urge? Or, as the government contends, should a void warrant be treated no differently from other defective warrants, such that the good-faith exception to the exclusionary rule can still apply? *We hold that, because the exclusionary rule is concerned solely with deterring culpable police misconduct—and not at all with regulating magistrate judges' actions—void and voidable warrants should be treated no differently; accordingly, an officer's reasonable reliance on the former, like the latter, can provide the basis for applying the good-faith exception.*
>
> Second, even if the good-faith exception can apply when an officer relies on a void warrant, should the exception apply in the particular circumstances of this case? *We hold that the officers' warrant application here adequately disclosed the nature of the technology at issue and the scope of the intended search, that the officers reasonably relied on the magistrate judge's determination that the search was permissible, and, accordingly, that the good-faith exception applies in this case.* (emphasis added).

#Fourth Amendment – Good Faith Exception

#Miscellaneous

United States v. Touset, 890 F.3d 1227 (11th Cir. 2018)

> This appeal presents the question whether the Fourth Amendment requires reasonable suspicion for a forensic search of an electronic device at the border. U.S. Const. amend. IV. Karl Touset appeals the denial of his motions to suppress the child pornography found on electronic devices that he carried with him when he entered the country and the fruit of later searches. We recently held that the Fourth Amendment does not require a warrant or probable cause for a forensic

> search of a cell phone at the border. *United States v. Vergara*, 884 F.3d 1309 (11th Cir. 2018). Touset argues that, in the light of the decision of the Supreme Court in *Riley v. California*, [] 134 S. Ct. 2473 [] (2014), reasonable suspicion was required for the forensic searches of his electronic devices. But our precedents about border searches of property make clear that no suspicion is necessary to search electronic devices at the border. Alternatively, the border agents had reasonable suspicion to search Touset's electronic devices. We affirm.

#Fourth Amendment – Warrant Required or Not

United States v. Vergara, 884 F.3d 1309 (11th Cir. 2018)

> This appeal presents the issue whether warrantless forensic searches of two cell phones at the border violated the Fourth Amendment. U.S. Const. amend IV. Hernando Javier Vergara appeals the denial of his motion to suppress evidence found on two cell phones that he carried on a cruise from Cozumel, Mexico to Tampa, Florida. He argues that the recent decision of the Supreme Court in *Riley v. California*, [] 134 S. Ct. 2473 [] (2014)—that the search-incident-to-arrest exception to the warrant requirement does not apply to searches of cell phones—should govern this appeal. But we disagree. The forensic searches of Vergara's cell phones occurred at the border, not as searches incident to arrest, and border searches never require a warrant or probable cause. At most, border searches require reasonable suspicion, but Vergara has not argued that the agents lacked reasonable suspicion to conduct a forensic search of his phones. We affirm.

#Fourth Amendment – Warrant Required or Not

United States v. Yang, 958 F.3d 851 (9th Cir. 2020)

The defendant entered a conditional guilty plea to receipt of stolen mail and being a prohibited person in possession of a firearm. He moved to suppress the evidence seized in the search of his residence. Law enforcement had located the defendant through a search of a license plate location database populated through Automatic License Plate Recognition ("ALPR") technology. The district court denied the motion. The court of appeals affirmed. The majority held that the defendant did not have a reasonable expectation of privacy in the historical location data of the rental vehicle he had used after failing to return it by the contract due date. In a concurring opinion, one judge rejected the majority's reliance on the lack of a property right in the vehicle but concluded that the limited information secured from the database did not implicate the constitutional concerns of *Carpenter*.

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

Walker v. Coffey, No. 956 F.3d 163 (3d Cir. 2020)

This was a Section 1983 action brought against a prosecutor and special agent from the Pennsylvania Office of the Attorney General, alleging that they violated the Stored Communications Act (SCA) by inducing the plaintiff's employer, Penn State, to disclose her work email with a facially invalid subpoena. The defendants conceded that the subpoena was "incomplete and therefore unenforceable." On a prior appeal a Third Circuit panel affirmed the dismissal of the complaint on qualified immunity grounds but remanded to allow the plaintiff to assert the SCA claim. The district court dismissed that claim, holding that the defendants had not violated the SCA and that, in any event, they were entitled to qualified immunity. Another Third Circuit panel affirmed: "The SCA is inapplicable because Penn State does not provide electronic communication services to the public, and the University acted within its rights as Walker's employer in voluntarily disclosing her work emails."

#Stored Communications Act (SCA)

DECISIONS – STATE

In re D.B., 24 Cal.App.5th 252 (2018)

The defendant minor was adjudicated a ward of the State for bringing a knife onto school grounds. Thereafter, he was arrested and charged for smoking marijuana in violation of his conditions of release and for drug-related use. The minor was then charged with another drug-related offense. The juvenile court imposed an electronic search condition pursuant to which probation could monitor the minor's cell phone to keep him "on track" while he was in drug treatment. The condition required the minor to surrender all devices to probation on demand. The Court of Appeal modified the condition, concluding that there was "slight justification" for the condition and that it was "constitutionally overbroad because it is not narrowly tailored to achieve its ostensible purpose or meet Minor's needs."

#Probation and Supervised Release

Carver Fed. Savings Bank v. Shaker Gardens, Inc., 90 N.Y.S.3d 653 (N.Y. 3d Dep't App. Div. Dec. 27, 2018)

This was an appeal from orders denying the plaintiff's motions to hold two defendants in contempt. The plaintiff had secured a judgment against the defendants and served subpoenas on them for the production of documents and

their appearance at depositions. Neither complied. Eventually, both appeared for depositions but refused to answer questions or produce documents, instead invoking the Fifth Amendment. The appellate court found that a finding of civil contempt was amply justified as to one defendant and stated the question on appeal to be "whether defendant's invocation of the Fifth Amendment *** in response to each of the questions presented, and his assertion of the privilege as a basis for withholding disclosure of the documents demanded in the subpoena, served to purge himself of the contempt." The appellate court held that tax information sought by the subpoenas fell within the "required records exception" to the privilege and had to be produced. As to the remaining information sought, one defendant did not assert that he was subject to any criminal investigation or proceeding and failed to show that his fear of prosecution was other than "imaginary." His claim was remanded for particularized objections and an *in camera* inquiry. The other defendant's claim (as well as her invocation of the spousal privilege) was also remanded.

#Fifth Amendment – Self-Incrimination

#Miscellaneous

C.C. v. J.A.H., Docket No. A-4425-18T3, 2020 WL 2108186 (N.J. Sup. Ct. App. Div. May 4, 2020)

> In this case of first impression, we examine the meaning of a 'dating relationship' under the [New Jersey] Prevention of Domestic Violence Act *** where the parties never experienced a traditional, in-person 'date.' Instead, their relationship was demonstrated by the intensity and content of their communications, including the exchange of nearly 1300 highly personal text messages. We conclude the proliferate and exceedingly intimate communications between the parties constituted a dating relationship within the meaning of the Act and supported entry of the final restraining order (FRO).

The parties had met at a fitness center where the plaintiff was the general manager. The defendant, against whom the FRO was entered below, was a new member. The Appellate Division, in agreeing with the trial judge that "the parties' dating relationship was 'peculiar" because they never experienced an in-person date," noted the "prevalence of virtual communications in the ever-changing world."

#Social Media

Commonwealth v. Jerome Almonor, 120 N.E.2d 1183 (Mass. 2019)

> The police quickly identified the defendant as the person suspected of murdering the victim with a sawed-off shotgun. In an attempt to pinpoint the location of the fleeing suspect, the police caused the defendant's cell phone to be 'pinged.' They did so without a warrant. The legality of that ping in these circumstances is the central legal issue in this murder case. ***
>
> This appeal raises an issue of first impression in Massachusetts: whether police action causing an individual's cell phone to reveal its real-time location constitutes a search in the constitutional sense under either the Fourth Amendment or art. 14. For the reasons set forth below, we conclude that, under art. 14 [of the Massachusetts Declaration of Rights], it does. We also conclude, however, that in the circumstances of this case, the warrantless search was supported by probable cause and was reasonable under the exigent circumstances exception to the search warrant requirement. We therefore reverse the motion judge's allowance of the defendant's motion to suppress. (footnotes omitted).

#Fourth Amendment – Exigent Circumstances

Commonwealth v. Arthur, 120 N.E.2d 1183, (Mass. App. Ct. 2018)

> This case presents the question whether the police unreasonably delayed obtaining a warrant to search the contents of cellular telephones (second warrant), where those cell phones had already been properly seized pursuant to a lawful first warrant and were being held as evidence pending trial. A Superior Court judge held that the delay in seeking the second warrant was unreasonable *** and suppressed the fruits of the search conducted pursuant to the second warrant. We reverse, concluding that the delay in seeking the second warrant was not unreasonable, where the cell phones were already lawfully in police custody and were reasonably expected to remain so until trial. (footnote omitted).

#Fourth Amendment – Warrant Required or Not

Commonwealth v. Bell, 211 A.3d 761 (Pa. 2019)

The defendant was arrested for DUI. He refused to submit to a blood test and was charged with drunk driving and a traffic offense. The defendant moved unsuccessfully to suppress evidence of his refusal to submit to the warrantless test. A police officer testified about the defendant's refusal and he was found guilty of all charges. The defendant moved for reconsideration in light of *Birchfield v. North Dakota*. The trial court granted a new trial because the court has relied on the

defendant's refusal as a basis for the conviction. An intermediate appellate court reversed, relying on Pennsylvania's implied consent law. The Pennsylvania Supreme Court agreed: "we conclude the 'evidentiary consequence' provided by Section 1547(e) for refusing to submit to a warrantless blood test – the admission of that refusal at a subsequent trial for DUI – remains constitutionally permissible post-*Birchfield*."

#Miscellaneous

#Trial-Related

Commonwealth v. Brennan, 112 N.E.3d 1180(Mass. 2018)

The defendant was charged with two counts of criminal harassment. The charges arose out of allegations that he had concealed GPS devices on the vehicles of a married couple and had used the devices to track their movements. The trial court dismissed the charges, finding that the Commonwealth had not alleged sufficient "qualifying acts" under the statute in issue. The Supreme Judicial Court reversed, concluding that concealing a GPS device on a vehicle qualified as an "act," a sufficient number of acts had been alleged, there was evidence that the couple suffered substantial emotional distress, and the defendant's conduct was willful and malicious. The court also made this observation:

> As technology has advanced, the tools that people can use to harass victims have increased. *** The law has not fully caught up to the new technology, and given the speed with which technology evolves, it may sometimes leave victims without recourse. See *id.* at 48-49. The Legislature may wish to explore whether the conduct of a private person electronically monitoring the movements of another private person should be criminalized, regardless of whether it would constitute criminal harassment. In these circumstances, the defendant's behavior satisfied the three acts necessary for the criminal harassment statute, but there may be occasions where the facts might not be sufficient for the statute to encompass a defendant's conduct. (footnote omitted).

#Miscellaneous

#Social Media

Commonwealth v. Carter, 52 N.E.3d 1054 (Mass. 2019), *cert.* denied, 140 S. Ct. 910 (2020)

The defendant was indicted for and convicted of involuntary manslaughter arising out of her exchange of text messages with an individual who she encouraged to commit and her voice contact with him while he did so. The Massachusetts

Supreme Judicial Court held the evidence was sufficient to establish the defendant's guilt beyond a reasonable doubt. The court also rejected the defendant's argument that the statute under which she was charged was unconstitutionally vague and that her conviction violated her right to free speech.

#Miscellaneous

#Social Media

Commonwealth v. D'Adderio, No. 833 MDA 2018, 2019 WL 2500421 (Pa. Super. Ct. June 17, 2018)

The defendant was convicted of harassment under Pennsylvania law after she directed multiple Facebook posts to an individual that were "vulgar and inflammatory." She argued on appeal that her posts were protected by the First Amendment and that the harassment statute was unconstitutionally overbroad. The appellate court affirmed the conviction. It held that her posts "did not express social or political beliefs or constitute legitimate conduct" and were not protected by the First Amendment. The court also held that the statute in issue does not punish constitutionally protected speech and, thus, was not overbroad.

#Miscellaneous

#Social Media

Commonwealth v. Davis, 220 A.3d 534 (Pa. 2019)

The defendant was charged with child pornography-related offenses. An encrypted computer was found at the time of his arrest. A trial judge granted the Commonwealth's motion to compel the defendant to decrypt the computer, relying on the foregone conclusion doctrine and rejecting his self-incrimination argument. On an interlocutory appeal, the Pennsylvania Supreme Court reversed:

> *** we conclude that compelling the disclosure of a password to a computer, that is, the act of production, is testimonial. Distilled to its essence, the revealing of a computer password is a verbal communication, not merely a physical act that would be nontestimonial in nature. There is no physical manifestation of a password, unlike a handwriting sample, blood draw, or a voice exemplar. As a passcode is necessarily memorized, one cannot reveal a passcode without revealing the contents of one's mind. Indeed, a password to a computer is, by its nature, intentionally personalized and so unique as to accomplish its intended purpose — keeping information contained therein confidential and insulated from discovery. Here, under United States Supreme Court precedent, we find that the Commonwealth is seeking the electronic equivalent to a combination to a wall safe — the passcode to unlock

> Appellant's computer. The Commonwealth is seeking the password, not as an end, but as a pathway to the files being withheld. As such, the compelled production of the computer's password demands the recall of the contents of Appellant's mind, and the act of production carries with it the implied factual assertions that will be used to incriminate him. Thus, we hold that compelling Appellant to reveal a password to a computer is testimonial in nature.

The dissenting justice would have held that the foregone conclusion doctrine applied because the defendant "voluntarily informed them [the government agents] that he was the sole user of the computer, that he used hardwired Internet services that were password protected, that only he knew the password to decrypt his computer files, and that he would never disclose the password, as it would incriminate him."

#Encryption

#Fifth Amendment – Self-Incrimination

Commonwealth v. Feliz, 119 N.E.3d 700 (Mass. 2019)

The defendant pled guilty to possession and distribution of child pornography. At sentencing, the court imposed GPS monitoring as a condition of probation as required by a Massachusetts statute. The trial court rejected the defendant's argument that the condition was an unreasonable search, found the statute in issue constitutional, and rejected an as-applied challenge. On appeal, the Supreme Judicial Court reversed:

> The defendant argues that, as applied to him, the condition of mandatory GPS monitoring, pursuant to G. L. c. 265, § 47, constitutes an unreasonable search under the Fourth Amendment and art. 14. We consider this argument in light of the United States Supreme Court's holding that GPS monitoring is a search. See *Grady* v. *North Carolina* ***, is overinclusive in that GPS monitoring will not necessarily constitute a reasonable search for all individuals convicted of a qualifying sex offense.
>
> Article 14 requires an individualized determination of reasonableness in order to conduct more than minimally invasive searches, and GPS monitoring is not a minimally invasive search. To comport with art. 14, prior to imposing GPS monitoring on a given defendant, a judge is required to conduct a balancing test that weighs the Commonwealth's need to impose GPS monitoring against the privacy invasion occasioned by such monitoring.

> We conclude that, in the circumstances of this case, the Commonwealth's particularized reasons for imposing GPS monitoring on this defendant do not outweigh the privacy invasion that GPS monitoring entails. Accordingly, as applied to this defendant, GPS monitoring is an unconstitutional search under art. 14. (footnote omitted).

#Probation and Supervised Release

Commonwealth v. Fredericq, 121 N.E.3d 166 (Mass. 2019)

The defendant was indicted for trafficking cocaine. He moved to suppress the cocaine and cash seized from a warrantless search of his residence. That motion was granted by a judge who concluded that the evidence seized were the fruits of the "unlawful police tracking of a cellular telephone through which the police obtained *** [CSLI] without a search warrant based on probable cause." The Supreme Judicial Court affirmed the suppression order:

> We conclude that the defendant has standing to challenge the Commonwealth's warrantless CSLI search because, by monitoring the telephone's CSLI, the police effectively monitored the movement of a vehicle in which he was a passenger. We further conclude that, under the circumstances here, the seizure of the cocaine and cash was the direct result of information obtained from the illegal CSLI search; that, under the fruit of the poisonous tree doctrine of the exclusionary rule, it is irrelevant whether the defendant had a reasonable expectation of privacy in the crawl space where the cocaine was found; and that the Commonwealth has failed to meet its burden of proving that the seizure was sufficiently attenuated from the illegal search such that it should not be deemed a forbidden fruit of the poisonous tree. Specifically, we conclude that the defendant's consent to a search of his residence did not purge the seizure from the taint of the illegal CSLI search, where the consent was obtained through the use of information obtained from that search. For these reasons and as discussed more fully infra, we affirm the order granting the defendant's motion to suppress. (footnote omitted).

#Fourth Amendment – Warrant Required or Not

#Fourth Amendment – Good Faith Exception

#SCA (Stored Communications Act)

Commonwealth v. Johnson, 119 N.E.3d 669 (Mass. 2019)

The defendant was convicted of breaking and entering and related offenses. Evidence offered against him at trial included GPS location data recorded from a GPS monitoring device that had been attached to the defendant as a condition of

probation. He had moved to suppress the evidence, arguing that the Commonwealth's accessing and reviewing the GPS data was an unreasonable search. The motion was denied. The defendant argued on appeal, among other things, that accessing the data was an unconstitutional warrantless search. The Supreme Judicial Court affirmed the denial of the motion to suppress, concluding that,

> although the original imposition of GPS monitoring as a condition of the defendant's probation was a search, it was reasonable in light of the defendant's extensive criminal history and willingness to recidivate while on probation. We also conclude that once the GPS device was attached to the defendant, he did not possess a reasonable expectation of privacy in data targeted by police to determine his whereabouts at the times and locations of suspected criminal activity that occurred during the probationary period. Accordingly, no subsequent search in the constitutional sense under either art. 14 or the Fourth Amendment occurred.

#Fourth Amendment – Warrant Required or Not

#Probation and Supervised Release

Commonwealth v. Jones, 117 N.E.3d 702 (Mass. 2019)

The defendant was indicted for prostitution-related offenses. A cell phone was seized at the time of his arrest. Because the Commonwealth believed that the contents of the phone included material and inculpatory evidence it secured a warrant to search the phone. It could not do so, however, because the phone was encrypted and the defendant, asserting the Fifth Amendment privilege, refused to provide the password. A trial judge denied a motion to compel, finding that the Commonwealth had not shown that the defendant's knowledge of the password was a foregone conclusion. The court also denied a renewed motion. On appeal, the Supreme Judicial Court reversed and remanded. First, the court held that Article 12 of the Massachusetts Declaration of Rights requires the Commonwealth to prove beyond a reasonable doubt that the defendant knows the password for the foregone conclusion doctrine to apply. Then, the court held that there were sufficient facts to meet that burden as the phone was in the defendant's possession at the time of his arrest and statements made by a witness tended to show the defendant's regular use of the phone. Finally, the court held that, "a judge acting on a renewed Gelfgatt motion may consider additional information without first finding that it was not known or not reasonably available at the time of the first filing."

The court also rejected the trial judge's imposition of an additional requirement on the Commonwealth, distinguishing between knowledge of a password and content:

> The motion judge required the Commonwealth to prove the defendant's knowledge of the password, and the existence of information relevant to the charges against the defendant within the LG phone, with 'reasonable particularity.' This standard has been used to define the level of particularity required in the identification of subpoenaed documents. *** Here, neither documents nor the contents of the LG phone are sought. *** [T]he Commonwealth therefore need not prove any facts with respect to the contents of the LG phone. The only consideration is whether the defendant knows the password to the encrypted device. The reasonable particularity standard, which considers the level of specificity with which the Commonwealth must describe sought after evidence, is therefore inapt in the context of compelled decryption. Indeed, as other courts have noted, the defendant either knows the password or does not. His knowledge therefore must be proved to a level of certainty, not described with a level of specificity. *** We need not address how the reasonable particularity standard combines with the proof beyond a reasonable doubt requirement in document production cases, as no such content has been sought in this case.

#Fifth Amendment – Self-Incrimination

Commonwealth v. Knox, 190 A.3d 1146 (Pa. 2018)

At issue here was "whether the First Amendment *** permits the imposition of criminal liability based on the publication of a rap-music video containing threatening lyrics directed to named law enforcement officers." The defendant had been arrested after a traffic stop, during which the police found a stolen weapon and drugs. The defendant was charged with a number of offenses and, while the charges were pending, he wrote and recorded a rap song, titled "F—k the Police," which was put on video along with photos showing the defendant motioning as if he was firing a weapon. The arresting officers were identified by name and the video was uploaded onto social media sites. The defendant was charged with making terroristic threats and witness intimidation under Pennsylvania law. He was found guilty of the charges and the conviction affirmed by the intermediate appellate court. The Pennsylvania Supreme Court affirmed. After canvassing precedent, the court concluded, "[f]irst, the Constitution allows states to criminalize threatening speech which is specifically intended to terrorize or intimidate. Second, in evaluating whether the speaker acted with an intent to terrorize or intimidate, evidentiary weight should be given to contextual circumstances ***." (footnote omitted). The court held that there was sufficient

evidence to support the finding that the defendant acted with the subjective intent to commit the crimes and that the video constituted a "true threat."

#Social Media

Commonwealth v. McCarthy, 142 N.E.3d 1000 (Mass. 2020)

The defendant was under investigation for drug distribution. Law enforcement used automated license plate readers ("ALPRs") at two fixed locations on two bridges to track his historical movements over a three-month period and also received real-time alerts. The defendant challenged the denial of motions to suppress, arguing that the warrantless surveillance violated the Fourth Amendment and its Massachusetts counterpart. The Supreme Judicial Court rejected the applicability of the "mosaic" theory recognized by the United States Supreme Court in *Carpenter v. United States* (*q.v.*) and by it in *Commonwealth v. Augustine* (*q.v.*) because the ALPRs in issue did not "implicate expressive and associative rights" of the defendant and thus did not interfere with a reasonable expectation of privacy: "This limited surveillance does not allow the Commonwealth to monitor the whole of the defendant's public movements, or even his progress on a single journey." The court declined to "establish a bright-line rule for when the use of ALPRs constitutes a search," although it did recognize that this "may bring some interim confusion."

#Fourth Amendment – Warrant Required or Not

Commonwealth v. Norman, 142 N.E.3d 1 (Mass. 2020)

The defendant was charged with possession with intent to distribute. He was given pre-trial release and ordered to stay outside Boston. He was also ordered to wear a GPS monitoring device. Thereafter, a home invasion and armed robbery occurred. In an attempt to solve the crime law enforcement contacted the probation service's electronic monitoring program and, without a search warrant, inquired whether anyone under GPS supervision had been present at the time and location of the crime. The data produced identified the defendant. Law enforcement then secured a warrant for a location that the data revealed the defendant had been before and after the crime. That search revealed inculpatory information and the defendant was arrested and indicted. He moved to suppress on Fourth Amendment and equivalent Massachusetts constitutional grounds. The motion court granted the motion, finding that,

> the defendant had consented to the imposition of the GPS device and use of the GPS location data only for the purposes of enforcing conditions of release, and for general law enforcement purposes. The judge therefore

> determined that the police were not permitted to obtain the GPS location data without probable cause. Because nothing linked the defendant to the crimes before police obtained the GPS location data, the judge concluded that the search was not supported by probable cause and granted the motion to dismiss.

The Supreme Judicial Court affirmed.

#Fourth Amendment – Warrant Required or Not

#Probation and Supervised Release

Commonwealth v. Pacheco, 227 A.3d 358(Pa. Super. Ct. 2020)

In 2015, in the course of a narcotics investigation, prosecutors secured orders under the Pennsylvania Wiretap Act that authorized a cell service provider to "ping" the defendant's cell phone and send real-time CSLI to them. Defendant moved to suppress evidence derived from the CSLI, which the trial court denied. He was convicted on multiple counts of drug-related offenses and appealed from, other things, the denial of the suppression motion. The appellate court rejected the defendant's contention that the CSLI orders were unconstitutional under *Carpenter v. United States* (*q.v.*) because the prosecutors failed to secure a search warrant. First, the court rejected a distinction between historical and real-time CSLI:

> We find no meaningful distinction between the privacy issues related to historical and real-time CSLI. In our view, the High Court's rationale in ***Carpenter*** extends to real-time CSLI tracking. Applying that Court's analogy, obtaining real-time CSLI is the equivalent of attaching an ankle monitor to the cell phone's user; it allows the government to track the user's every move as it is happening. ***See Carpenter*** ***. Therefore, we hold that an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through real-time CSLI. As such, when prosecutors sought and obtained real-time information about Pacheco's location by pinging his cell phone, they conducted a 'search' under the federal and state constitutions.

The court then held that the orders in issue were the functional equivalents of traditional search warrants and affirmed the denial of the suppression motion.

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

Commonwealth v. Raspberry, 107 N.E.3d 1195 (Mass. App. Ct. 2018)

The defendant appealed from the denial of her motion to suppress evidence obtained by police through warrantless real-time tracking of her location using

CSLI and through a search of her vehicle. The trial court denied the motion and the Appeals Court affirmed. Law enforcement was lawfully monitoring a telephone conversation during which the defendant said she would kill someone. An officer then made an "exigent request" to AT&T, which agreed to cooperate and made a number of "emergency pings" to the defendant's cell phone number, enabling law enforcement to locate the vehicle the defendant was in. The appellate court held that the "emergency aid" exception to the warrant and probable cause requirements of the Fourth Amendment and Article 12 applied because law enforcement had objectively reasonable grounds to believe that an emergency existed and law enforcement conduct had been reasonable. The appellate court also held that, since the police had probable cause to believe that the defendant possessed a loaded weapon, the automobile exception justified the warrantless search of the vehicle.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Edwards v. State, 274 So. 3d 1222 (Fla. 3d Dist. Ct. App. 2019)

The defendant, a former police officer, appealed her conviction and sentence for official misconduct. "Her primary contention *** is that the trial court erred in denying her motion to suppress evidence obtained from a personal flash drive plugged into her work computer." Evidence offered against the defendant came from the flash drive, which, she contended, was personal property that had been illegally seized when her work computer had been legally seized. The District Court of Appeal affirmed: The flash drive was plugged into a work computer, the computer was in an office shared with another officer who had full access to the defendant's computer, the computer was connected to a network which anyone with appropriate credentials could access, and a login banner warned, among other things, that users of the network had no expectation of privacy.

#Fourth Amendment – Warrant Required or Not

Edwards v. State, 294 So. 3d 671 (Miss. Ct. App. 2020)

The defendant was convicted under a Mississippi statute for posting Facebook Live videos in which he accused a local pastor of sexual misconduct. The statute criminalized the posting of messages "for the purpose of causing injury" whether the information was "truthful or untruthful." The Court of Appeals reversed on First Amendment grounds:

> While the statute could have some valid applications, there is nothing in its language that would serve to limit its reach to unprotected speech. As shown above, speech does not lose its constitutional protection simply because its purpose or intent is to cause injury. We conclude that the statute's potential valid applications pale in comparison to its overbreadth. That is, the statute's 'overbreadth [is] *substantial*, not only in an absolute sense, but also relative to [its] legitimate sweep.' *** Therefore, the statute is facially invalid and unconstitutional, and Edwards's conviction must be reversed and rendered. (emphasis added).

#Social Media

I/M/O Eldridge, 836 S.E.2d 859 (N.C. Ct. App. 2019)

The defendant was held in criminal contempt under the following facts:

> On 29 November 2018, defendant Davin Eldridge, a frequent publisher for a Facebook page called 'Trappalachia,' entered the Macon County Courthouse. The officer working the metal detector saw defendant had a small tape recorder and 'advised [defendant that] he [could] not record inside the courtroom. Defendant acknowledged the officer's instruction and entered a courtroom. As he did so, defendant bypassed signs posted on the entranceways stating:
>
> > BY ORDER OF THE SENIOR RESIDENT SUPERIOR COURT JUDGE: DO NOT use or open cell phones, cameras, or any other recording devices inside the courtrooms. Violations of this order will be contempt of court, subjecting you to jail and/or a fine. Your phone may be subject to seizure and search.
>
> While in the courtroom, defendant was observed sitting on the second row with a cell phone, holding it 'shoulder-chest level' towards the front of the courtroom. The officer went over to defendant and instructed him to put his phone away. Defendant replied, 'I'm not doing anything.' The Honorable William H. Coward, Superior Court Judge of Macon County, was presiding over a criminal matter at that time. Judge Coward was informed that a live posting of the hearing in session was streaming from a Facebook page. Based on that information, Judge Coward interrupted the hearing to issue a reminder that recordings of courtroom proceedings were prohibited by law. At the conclusion of the hearing, Judge Coward viewed the Facebook postings by defendant, which included footage of the inside of the courtroom and the prosecutor presenting his closing argument. The trial court ordered defendant to return to the courtroom later that day. Defendant failed to return as ordered.

Among other things, he challenged this sentence on appeal:

> Here, the trial court sentenced defendant to be confined in the Macon County Detention Center for thirty days. Defendant's sentence was suspended for twelve months, upon six specific conditions for him to meet during his probationary sentence: (1) serve an active sentence of 96 hours; (2) pay the costs of the action; (3) pay a fine of $500.00; (4) draft a 2,000-3,000 word essay on the following subject: 'Respect for the Court System is Essential to the Fair Administration of Justice,' forward the essay to Judge Coward for approval, and following approval, post the essay on all social media or internet accounts that defendant owns or controls or acquires hereafter during his period of probation and attributed to defendant, without negative comment or other negative criticism by defendant or others, during said period of probation; (5) not violate any order of Court or otherwise engage in further contemptuous behavior; and (6) not attend 'any court session in Judicial District 30A unless and until his essay has been approved and posted as required herein and he has fully complied with all other provisions of this order.'

The Court of Appeals affirmed:

> Given defendant's questionable and intentional conduct, his frequent visits to the courtroom, and his direct willingness to disobey courtroom policies, we discern no abuse of discretion in the trial court's decision to impose conditions on defendant's probationary sentence. Such conditions are reasonably related to the necessity of preventing further disruptions of the court by defendant's conduct, and the need to provide accountability without unduly infringing on his rights. Thus, because there is sufficient evidence that the trial court properly exercised its authority, we overrule defendant's argument.

#Miscellaneous

#Social Media

Everett v. State of Delaware, 186 A.3d 1224 (Del. 2018)

A detective monitored the defendant's Facebook page using a fake profile for approximately two years. At some point the detective used the fake profile to send the defendant a "friend request," which the defendant accepted. Thereafter, the detective saw a photo on the defendant's Facebook page which showed, among other things, a firearm. This led the detective to apply for a search warrant of the defendant's home. The warrant was issued and, among other things, a weapon was found. The defendant was indicted and convicted of possession of a firearm by a "person prohibited." The defendant learned of the deceptive Facebook activity on the first day of the trial. His motion for a mistrial or a hearing was denied. On appeal, the defendant argued that the monitoring of his Facebook page was an

unlawful warrantless search and that any evidence seized pursuant to the search should be suppressed. He did this by arguing that the trial court had erred in denying his motion for a "reverse-*Franks*" hearing. The Delaware Supreme Court affirmed: The defendant did not have a reasonable expectation under either the Fourth Amendment or the Delaware Constitution that the Facebook posts he had voluntarily shared with the detective and others would not be disclosed. The court declined to extend its discussion to the sharing of information with third parties such as an internet service provider.

#Fourth Amendment – Warrant Required or Not

#Social Media

#Third-Party Doctrine

Facebook, Inc. v. Pepe, No. 19-SS-1024, 2020 WL 1870591 (D.C. Ct. App. Jan. 14, 2020)

This matter arises from an expedited appeal by Facebook from an order holding it in civil contempt for refusing to comply with an *ex parte* subpoena served by the appellee and from a related order directing Facebook not to disclose the existence of the subpoena. The DC Court of Appeals affirmed the contempt but vacated the nondisclosure order. The appellee had sought evidence from Facebook in defense of then-pending criminal charges arising out of a shooting. The evidence was a "disappearing Instagram." In explaining its rulings, the court held that the Stored Communications Act did not render the subpoena unenforceable, rejecting Facebook's argument that the appellee was not "an addressee or intended recipient" of the "expired" Instagram and that the Act did not preempt "laws that require disclosures the SCA expressly *permits*." (emphasis in original) (footnote omitted). As to the nondisclosure order, the court held that it imposed a burden on Facebook's First Amendment rights and that, regardless of whether the order was subject to strict scrutiny or to a lesser standard, the appellee did not meet it. The appellee "did not establish a substantial risk that Facebook's disclosure of the existence of his subpoena to the government would *** result in revealing any additional details of his self-defense strategy" or that there was an "appreciable risk of spoliation."

#Discovery Materials

#Social Media

#SCA (Stored Communications Act)

Facebook, Inc. v. Superior Court, Case no. S256686 (Cal. July 17, 2019) (*en banc*)

The trial judge in an ongoing gang-related murder trial ordered production of private social media postings. The California Supreme Court denied relief to the service providers because the trial had begun and the trial judge had found a "strong justification for access to the sought information."

NOTE: This order is not available electronically.

#SCA (Stored Communications Act)

#Trial-Related

Facebook, Inc. v. Superior Court, 4 Cal. 5th 1245(2018)

> Real parties in interest Derrick D. Hunter and Lee Sullivan (defendants) were indicted by a grand jury and await trial on murder, weapons, and gang-related charges arising out of a driveby shooting in San Francisco. Each defendant served a subpoena duces tecum on one or more petitioners, social media service providers Facebook, Inc. (Facebook), Instagram, LLC (Instagram), and Twitter, Inc. (Twitter) (collectively, social media providers, or simply providers). The subpoenas broadly seek public and private communications, including any deleted posts or messages, from the social media accounts of the homicide victim and a prosecution witness.
>
> As explained below, the federal Stored Communications Act (18 U.S.C. § 2701 et seq.; hereafter SCA or Act) regulates the conduct of covered service providers, declaring that as a general matter they may not disclose stored electronic communications except under specified circumstances (including with the consent of the social media user who posted the communication) or as compelled by law enforcement entities employing procedures such as search warrants or prosecutorial subpoenas. Providers moved to quash defendants' subpoenas, asserting the Act bars providers from disclosing the communications sought by defendants. They focused on section 2702(a) of the Act, which states that specified providers 'shall not knowingly divulge to any person or entity the contents of' any 'communication' that is stored or maintained by that provider. They asserted that section 2702 prohibits disclosure by social media providers of *any* communication, whether it was configured to be public (that is, with regard to the communications before us, one as to which the social media user placed no restriction regarding who might access it) or private or restricted (that is, configured to be accessible to only authorized recipients). Moreover, they maintained, none of various exceptions to the prohibition on disclosure listed in section 2702(b) applies here. And in any event, providers argued, they would face

substantial technical difficulties and burdens if forced to attempt to retrieve deleted communications and should not be required to do so.

Defendants implicitly accepted providers' reading of the Act and their conclusion that it bars providers from complying with the subpoenas. Nevertheless, defendants asserted that they need all of the requested communications (including any that may have been deleted) in order to properly prepare for trial and defend against the pending murder charges. They argued that the SCA violates their constitutional rights under the Fifth and Sixth Amendments to the United States Constitution to the extent it precludes compliance with the pretrial subpoenas in this case.

The trial court, implicitly accepting the parties' understanding of the SCA, agreed with defendants' constitutional contentions, denied providers' motions to quash, and ordered them to produce the requested communications for the court's review in camera. Providers sought, and the Court of Appeal issued, a stay of the production order. After briefing and argument, the appellate court disagreed with the trial court's constitutional conclusion and issued a writ of mandate, directing the trial court to quash the subpoenas. We granted review.

Our initial examination of the Act, its history, and cases construing it, raised doubts that section 2702 of the Act draws no distinction between public and restricted communications, and that no statutory exception to the prohibition on disclosure could plausibly apply here. In particular, we questioned whether the exception set out in section 2702(b)(3), under which a provider may divulge a communication with the ‘lawful consent’ of the originator, might reasonably be interpreted to permit a provider to disclose posted communications that had been configured by the user to be public.

Accordingly, we solicited supplemental briefing concerning the proper interpretation of section 2702. In that briefing, all parties now concede that communications configured by the social media user to be public fall within section 2702(b)(3)'s lawful consent exception to section 2702's prohibition, and, as a result, may be disclosed by a provider. As we will explain, this concession is well taken in light of the relevant statutory language and legislative history.

The parties differ, however, concerning the scope of the statutory lawful consent exception as applied in this setting. Defendants emphasize that even those social media communications configured by the user to be restricted to certain recipients can easily be shared widely by those recipients and become public. Accordingly, they argue that when any restricted communication is sent to a ‘large group’ of friends or followers the communication should be *deemed* to be public and hence disclosable by the provider under the Act's lawful consent exception. On

> this point we reject defendants' broad view and instead agree with providers that restricted communications sent to numerous recipients cannot be deemed to be public—and do not fall within the lawful consent exception. Yet we disagree with providers' assertion that the Act affords them 'discretion' to defy an otherwise proper criminal subpoena seeking public communications.
>
> In light of these determinations we conclude that the Court of Appeal was correct to the extent it found the subpoenas unenforceable under the Act with respect to communications addressed to specific persons, and other communications that were and have remained configured by the registered user to be restricted. But we conclude the court's determination was erroneous to the extent it held section 2702 also bars disclosure by providers of communications that were configured by the registered user to be public, and that remained so configured at the time the subpoenas were issued. As we construe section 2702(b)(3)'s lawful consent exception, a provider must disclose any such communication pursuant to a subpoena that is authorized under state law.
>
> Ultimately, whether any given communication sought by the subpoenas in this case falls within the lawful consent exception of section 2702(b)(3), and must be disclosed by a provider pursuant to a subpoena, cannot be resolved on this record. Because the parties have not until recently focused on the need to consider the configuration of communications or accounts, along with related issues concerning the reconfiguration or deletion history of the communications at issue, the record before us is incomplete in these respects. Accordingly, resolution of whether any communication sought by the defense subpoenas falls within the statute's lawful consent exception must await development of an adequate record on remand.
>
> We will direct the Court of Appeal to remand the matter to the trial court to permit the parties to appropriately further develop the record so that the trial court may reassess the propriety of the subpoenas under the Act in light of this court's legal conclusions.

#Social Media

#SCA (Stored Communications Act)

Facebook, Inc. v. Wint, 199 A.3d 625 (D.C. 2019)

This was an emergency appeal from an order holding Facebook in civil contempt for refusing to comply with subpoenas served by the defendant in a murder trial. The subpoenas, which had been authorized by the trial judge, sought production of records from various social media accounts, including the content of communications. Facebook argued on appeal that the SCA barred it from complying. The Colorado Supreme Court reversed. It concluded that the SCA

prohibited compliance and that there were no statutory exceptions that would allow Facebook to comply. The court also rejected the defendant's argument that criminal defendants have a "constitutional right to obtain evidence for trial and that this court therefore should reject a reading of the SCA that would preclude providers from complying with criminal defendants' subpoenas."

#Miscellaneous

#Social Media

#Trial-Related

D.J. v. C.C., Case no. A151996, 2019 WL 117619 (Cal. Ct. App. Jan. 7, 2019)

D.J. sought a restraining order against his former wife. He alleged that she had harassed and abused him by posting humiliating details about him on the Internet. The trial judge found that the ex-wife's conduct constituted abuse under the controlling statute and issued a restraining order using a pre-printed California Judicial Council form. Before that order had been issued, another court had declined to issue a similar order, finding that the relief sought would constitute a prior restraint and that an order could not issue absent a finding that the ex-wife's speech was unlawful. The Court of Appeal affirmed. There was substantial evidence to support the finding of abuse. Moreover, the Court of Appeal rejected the ex-wife's argument that the order was an unconstitutional prior restraint: the order, "which prevents C.C. from harassing D.J., was not aimed at C.C.'s speech: it was aimed at her abusive and harassing conduct, as found by the court after a hearing, and only incidentally affected her speech. *** As the trial court explained, C.C. had no right to use her free speech rights in an abusive fashion, which the court found she had done." (footnote omitted).

#Social Media

Ex Parte: Jordan Bartlett Jones, No. 12-17-00346-CR, *see* 2018 WL 2228888 (Tex. Ct. App. May 16, 2018)

The petitioner was charged with unlawful disclosure of intimate visual material in violation of the Texas "revenge pornography" statute, which, among other things, prohibits the disclosure of certain visual material in various formats. The trial court denied his request for *habeas* relief, rejecting the petitioner's argument that the statute violated the First Amendment. On appeal, and addressing a facial challenge to the statute, the court found that, "[b]ecause the photographs and visual recordings are inherently expressive and the First Amendment applies to the distribution of such expressive media in the same way it applies to their creation,

*** the right to freedom of speech is implicated *** .” (footnote omitted). The appellate court then held that the statute’s regulation of speech was content-based and subject to strict scrutiny. The appellate court rejected the argument of the respondent State of Texas that any visual material within the scope of the statute was contextually obscene. The court concluded that the statute did not use the least restrictive means to achieve the “compelling government interest of preventing the intolerable invasion of a substantial privacy interest” and therefore violated the First Amendment. The appellate court also held that the statute was overbroad “in the sense that it violates rights of too many third parties by restricting more speech than the Constitution permits.”

#Miscellaneous

#Social Media

G.A.Q.L. v. State, 257 So. 3d 1058 (Fla. 4th Dist. Ct. App. 2018)

> Two passcodes stand in the way of the state accessing the contents of a phone alleged to belong to a minor. The state sought, and the trial court agreed, to compel the minor to provide two passcodes, finding that ‘the act of producing the passcodes is not testimonial because the existence, custody, and authenticity of the passcodes are a foregone conclusion.’ We disagree. The minor is being compelled to ‘disclose the contents of his own mind’ by producing a passcode for a phone and a password for an iTunes account. Further, because the state did not show, with any particularity, knowledge of the evidence within the phone, the trial court could not find that the contents of the phone were already known to the state and thus within the ‘foregone conclusion’ exception. We grant the minor’s petition for writ of certiorari and quash the trial court’s order compelling the disclosure of the two passcodes.

#Fifth Amendment – Self-Incrimination

LMP Services, Inc. v. City of Chicago, 2019 IL 123123, 2019 WL 2218923 (Ill. May 23, 2019), *cert.* denied, 140 S. Ct. 468 (Nov. 4, 2019)

The operator of a food truck challenged a municipal code requirement that it refrain from parking within 200 feet of the entrance of a ground-floor restaurant and permanently install a GPS device that transmitted location information. A trial court granted summary judgment in favor of the defendant city and the Illinois Supreme Court affirmed on an interlocutory appeal. As to the 200-foot rule, the court rejected a substantive due process argument and held that the rule was reasonable because “it is a part of a regulatory scheme that seeks to balance the interests of food trucks with the City’s need to advance the stability and long-term

economic growth of its neighborhoods." Turning to the GPS requirement, the court rejected the argument that it constituted a warrantless search in violation of the Illinois Constitution. It held that the operator's analogy to *United States v. Jones* (*q.v.*) *and Katz v. United States* was misplaced because "any expectation of privacy a food truck might have in their location is greatly diminished, if it exists at all." Moreover, if the GPS requirement was a search, it was reasonable and therefore constitutional because, among other things, it "is the best and most accurate means of reliably locating a food truck, which is particularly important and necessary in the event of a serious health issue."

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

Lynch v. State, 260 So. 3d 1166 (Fla. 1st Dist. Ct. App. 2018) (*per curiam*)

On appeal from a conviction for selling crack cocaine the defendant challenged on *Brady* grounds, among other things, the failure of the trial court to allow him access to photos that a facial-recognition system returned as possible matches but that were deemed "nonmatches" by an analyst. The appellate court rejected the challenge:

> First, because he cannot show that the other photos the database returned resembled him, he cannot show that they would have supported his argument that someone in one of those photos was the culprit. Second, his attorney stated on the record that she did not want to call the analyst who evaluated the photos because the analyst's testimony that Lynch was the man in the officers' photos would only corroborate the officers' testimony. And third, the jury convicted only after comparing the photo the officers took to Lynch himself and to confirmed photos of Lynch. Under these circumstances, we cannot conclude that Lynch met his burden to demonstrate prejudice under *Brady*.

#Discovery Materials

#Miscellaneous

Mobley v. State, 839 S.E.2d 199 (Ga. 2020)

A driver appealed from his conviction of various offenses arising out of a fatal automobile collision. He had moved unsuccessfully to suppress evidence derived from the "airbag control module" of his vehicle, which showed that he had been driving nearly 100 mph moments before the collision. After law enforcement conducted a warrantless search of the module at the scene, the module was removed and searched a second time pursuant to a warrant. That search did not

result in the retrieval of any additional data. The Court of Appeals affirmed. The Georgia Supreme Court reversed. It concluded: (1) citing U*nited States v. Jones* (*q.v.*), the physical intrusion into the vehicle for law enforcement purposes was a search within the meaning of the Fourth Amendment; (2) the warrantless search was unreasonable because there was no applicable exception to the Warrant Requirement; (3) Georgia law does not compel the exclusion of evidence derived from a warrantless search; and (4) the inevitable discovery exception to the Warrant Requirement was inapplicable because there was no evidence that a warrant would have been applied for absent the initial warrantless search.

#Fourth Amendment – Warrant Required or Not

Park v. State, 825 S.E.2d 147 (Ga. 2019)

The defendant was convicted of child molestation and related offenses. After he was released from prison he was classified as a "sexually dangerous predator" under Georgia law. That classification required that the defendant wear and pay for an ankle monitor for the rest of his life (even after he had completed his probation). After the monitor was fitted, he was arrested and indicted for tampering with it. He argued that he could not be prosecuted because the statute was unconstitutional. A trial court rejected the argument and the Georgia Supreme Court allowed an interlocutory appeal. Relying on *Grady v. North Carolina*, the court held that the statute in issue authorized a search that implicated the Fourth Amendment. The court then held the lifetime monitoring to be unreasonable because (1) the permanent application of the monitor and collection of data constituted a "significant intrusion" on the defendant's privacy, and (2) the monitoring did not constitute a reasonable "special needs" search. Thus, the court held the statute unconstitutional on its face. The court also noted that the provision could be problematic if, for example, an individual were unable to pay.

#Fourth Amendment – Warrant Required or Not

#Probation and Supervised Release

People in Interest of R.D., 464 P.3d 717 (Colo. 2020) (en banc)

R.D., a juvenile, was adjudicated a delinquent under Colorado law based on tweets directed to another student. The adjudication was reversed by an intermediate appellate court, which concluded that his tweets were not "true threats." The Colorado Supreme Court reversed and remanded for the juvenile court to apply the Supreme Court's new guidance for determining whether a statement was a true threat or protected by the First Amendment:

> We hold that a true threat is a statement that, considered in context and under the totality of the circumstances, an intended or foreseeable recipient would reasonably perceive as a serious expression of intent to commit an act of unlawful violence. In determining whether a statement is a true threat, a reviewing court must examine the words used, but it must also consider the context in which the statement was made. Particularly where the alleged threat is communicated online, the contextual factors courts should consider include, but are not limited to (1) the statement's role in a broader exchange, if any, including surrounding events; (2) the medium or platform through which the statement was communicated, including any distinctive conventions or architectural features; (3) the manner in which the statement was conveyed (e.g., anonymously or not, privately or publicly); (4) the relationship between the speaker and recipient(s); and (5) the subjective reaction of the statement's intended or foreseeable recipient(s).

#Social Media

People v. Aleyniko, 104 N.E.3d 687 (N.Y. 2018)

While employed by Goldman Sachs the defendant compressed, uploaded, and downloaded its high frequency trading source code. He was convicted under a New York statute that criminalized the making of a tangible reproduction or representation of secret scientific material. The trial court set aside the jury verdict, concluding that the defendant's conduct did not fall within the statute. An intermediate appellate court reversed. The New York Court of Appeals affirmed:

> Ideas begin in the mind. By its very nature, an idea, be it a symphony or computer source code, begins as intangible property. However, the medium upon which an idea is stored is generally physical, whether it is represented on a computer hard drive, vinyl record, or compact disc. The changes made to a hard drive or disc when information is copied onto it are physical in nature. The representation occupies space. Consequently, a statute that criminalizes the making of a tangible reproduction or representation of secret scientific material by electronically copying or recording applies to the acts of a defendant who uploads proprietary source code to a computer server.

#Miscellaneous

#Trial-Related

People v. Augustus, 163 A.D.3d 981 (NY 2d Dep't App. Div. 2018)

The defendant was convicted of murder. The Second Department of the New York Appellate Division reversed the conviction. The defendant had moved to challenge

a warrant pursuant to which a saliva sample was taken from him and to suppress evidence derived from that search. Those motions were denied. The evidence offered against the defendant included his DNA profile, obtained from the saliva sample. However, the affidavit submitted in support of the search warrant failed to establish probable cause:

> The detective stated that he believed evidence related to the victim's murder may be found in the defendant's saliva based on his interview of witnesses, information supplied to him by fellow police officers, and his review of police department records. However, the detective did not identify the witnesses or indicate what information he obtained from them, and did not specify what police department records he reviewed, or what information was contained in the records.

Reversal and remand were required because the error was not harmless.

#Fourth Amendment – Warrant Required or Not

#Trial-Related

People v. Burwell, 183 A.D.3d 173 (N.Y. 3d Dep't App. Div. 2020)

The defendant was found guilty on various charges arising out of falsely reporting that she was the victim of a racially-motivated assault on a bus. One charge was that she circulated false information through social media in violation of a New York law that made it a crime to do so "under circumstances in which it is not unlikely that public alarm or inconvenience will result." The appellate court reversed the conviction on that charge. It held that the statute in issue regulated content-based speech and was subject to strict scrutiny. Although the statute served compelling interests it was unconstitutionally overbroad as applied: "neither general concern nor the Twitter storm that ensued following defendant posting the false tweets are the type of 'public alarm or inconvenience' that permits defendant's tweets to escape protection under the First Amendment ***." (footnote omitted). There was no proof of specific harm to identifiable victims or a great likelihood of harm. Moreover, since "defendant's false tweets were largely debunked through counter speech *** criminalizing her speech *** was not actually necessary to prevent public alarm and inconvenience."

#Social Media

People v. Buza, 4 Cal. 5th 658 (2018)

California law requires California law enforcement to collect DNA samples from persons arrested for and convicted of felony offenses. The defendant was arrested for arson and related felonies. He refused to provide a DNA sample and was later

convicted of the felonies and for refusing to provide a DNA specimen. His conviction for the latter offense was reversing on appeal. That ruling was reversed and remanded by the California Supreme Court. On remand, the intermediate appellate court again reversed the conviction under the California Constitution as an unreasonable search and seizure. The California Supreme Court reversed:

> Defendant raises a number of questions about the constitutionality of the DNA Act as it applies to various classes of felony arrestees. But the question before us is a narrower one: Whether the statute's DNA collection requirement is valid as applied to an individual who, like defendant, was validly arrested on 'probable cause to hold for a serious offense'—here, the felony arson charge for which defendant was ultimately convicted—and who was required to swab his cheek as 'part of a routine booking procedure' at county jail. *** Under the circumstances before us, we conclude the requirement is valid under both the federal and state Constitutions, and we express no view on the constitutionality of the DNA Act as it applies to other classes of arrestees. We accordingly reverse the judgment of the Court of Appeal in this case.

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

People v. Davis, 438 P.3d 266 (Colo. 2019)

After the defendant's arrest, he wanted someone to contact his girlfriend and have his car retrieved. The defendant gave his cell phone to an officer to make the call and gave the officer his password. He then offered up his phone a second time. The police thereafter obtained a warrant to search the contents of the phone and used the previously disclosed password to conduct the search. A trial court suppressed evidence from the phone, holding that the defendant had given "very limited" consent for the police to use the password. The Colorado Supreme Court reversed:

> The limited scope of Davis's consent to use the passcode does not alter this analysis. In general, an individual does not retain an expectation of privacy in 'information revealed to a third party and conveyed by him to Government authorities, *even if the information is revealed on the assumption that it will be used only for a limited purpose*.' *** Here, where Davis voluntarily disclosed his passcode directly to law enforcement, this principle holds especially true. Once an individual discloses the digits of his passcode to law enforcement, we conclude that it is unreasonable to expect those digits to be private from the very party to whom he disclosed them, regardless of any limitations he might be said to have implicitly placed upon the disclosure.

#Encryption

#Fourth Amendment – Warrant Required or Not

People v. Ellis, 130 N.E.3d 887 (N.Y. 2019)

The defendant, a convicted sex offender, was indicted for failing to disclose that he had a Facebook account, although he had disclosed the identifier he used to log in to Facebook, and the name by which he went on Facebook. A trial-level court denied the defendant's motion to dismiss the appeal. An appellate court reversed and dismissed the appeal on statutory interpretation grounds. The Court of Appeals affirmed, concluding that a Facebook account is not an "internet provider" within the meaning of the statute in issue.

#Social Media

People v. Fonerin, 159 A.D.3d 717 (N.Y. 2d Dep't App. Div. 2018)

A codefendant set fire to a homeless man while the defendant recorded the incident on his cell phone. The incident was also captured on surveillance footage. The defendant appealed his conviction for assault in the first degree, arguing, among other things, that the verdict was against the weight of the evidence. The Second Department reversed the conviction:

> It is undisputed that the defendant did not assist the codefendant in dousing the victim with lighter fluid or setting fire to the victim, and did not supply any of the materials to the codefendant to commit the criminal act. The defendant's actions, in uttering, 'Do that shit, man,' as the codefendant doused the victim with lighter fluid, and in filming this incident for approximately one minute before rendering any aid to this particularly vulnerable and helpless victim, were deplorable. However, his actions did not support the jury's finding beyond a reasonable doubt that he solicited, requested, commanded, importuned, or intentionally aided the codefendant to assault the victim, and that he did so sharing the codefendant's state of mind.

A dissenting judge disagreed: "Upon viewing the surveillance video, the cell phone video played to the jury, and all the evidence proffered, I am certain, as found by the jury, that the defendant importuned the codefendant to commit this reprehensible act and fully shared the codefendant's intent."

#Trial-Related

People v. Hackett, 166 A.D.3d 1483 (N.Y. 4th Dep't App. Div. 2018)

The defendant was convicted of the rape of a minor. Relying on *Riley v. California*, he argued on appeal that the trial court erred in denying his motion to suppress text messages between the minor and himself found on his cell phone. The cell phone was seized when the defendant was arrested and, in an application for a search warrant for the cell phone, the affiant stated that an officer had "sent a text message to the phone number that had been used during earlier communications between the victim and defendant, and the officer noted that the phone recovered from defendant *** signaled the arrival of a new text message moments later." The appellate court rejected the defendant's reliance on *Riley*: "Although *Riley* prohibits warrantless searches of cell phones incident to a defendant's arrest, *Riley* does not prohibit officers from sending text messages to a defendant, making observations of a defendant's cell phone, or even manipulating the phone to some extent upon a defendant's arrest." Since no information contained in the application suggested a warrantless search the denial of the motion was affirmed. Moreover, even if the text message did constitute an unconstitutional search and was stricken, the application contained sufficient information to establish probable cause for a search.

#Fourth Amendment – Warrant Required or Not

People v. Haggray, 162 A.D.3d 1106 (N.Y. 3d Dep't App. Div. 2018)

The defendant appealed from his conviction for robbery and grand larceny. He argued that, "the People deprived him of an opportunity to develop an effective argument on appeal by failing to provide him with certain video and photographic exhibits that were introduced into evidence at trial in a format that he could readily view." (footnote omitted). The Third Department found that the argument had merit and directed the prosecution to provide the defendant's counsel with copies of the exhibits "in a format readily accessible by modern personal computer equipment, and provide defendant's counsel with the necessary instructions and program requirements to do so."

#Miscellaneous

#Trial-Related

People v. Herskovic, 165 A.D.3d 835 (N.Y. 2d Dep't App. Div. 2018)

The defendant was convicted of, among other things, gang assault. His conviction was reversed on appeal. The complainant was unable to identify any person who assaulted him. The complainant's sneaker was recovered six days after the assault

and testing of a DNA sample taken from the sneaker used to determine that DNA from the defendant and the complainant was likely to have been on the sneaker. However, the analysis was questionable. “Under the circumstances of this case, including the complainant’s inability to positively identify any of his attackers, the varying accounts regarding the incident, and the DNA evidence, which was less than convincing, we find that the evidence, when properly weighed, did not establish the defendant’s guilt beyond a reasonable doubt.”

#Trial-Related

People v. Jones, 166 A.D.3d 803 (N.Y. 2d Dep’t App. Div. 2018)

The defendant was convicted of conspiracy to commit murder and other gang-related offenses. At trial, the prosecution presented testimony from police officers about their investigation and introduced thousands of social media posts of the defendant, co-defendants, and charged and uncharged co-conspirators. The trial court declared a police officer an “expert” and permitted him to testify about gangs. The defendant’s conviction was reversed for this and other reasons:

> Georg’s testimony also ran afoul of the proscription against police experts acting as summation witnesses, straying from their proper function of aiding the jury in its fact[f]inding, and instead ‘instructing the jury on the existence of the facts needed to satisfy the elements of the charged offense’ ***. During the trial, Georg read Facebook posts verbatim to the jury, offered commentary about the time of each post in relation to key events in the case, and connected evidence of the parties exchanging their phone numbers with records confirming that a call was subsequently placed. The defendant’s counsel correctly objected to such testimony *** on the ground that Georg was no longer acting as an expert witness but was usurping the jury’s function by interpreting, summarizing, and marshaling the evidence.

#Social Media

#Trial-Related

People v. Kennedy, 917 N.W.2d 355 (Mich. 2018)

The defendant was convicted of a 1993 murder. His trial counsel had requested the appointment of a DNA expert to help understand the evidence. That evidence was derived from swabs taken from the victim’s body in 2011 that included a mixture of DNA profiles from the defendant and three others. The defendant’s profile matched the major donor’s and also matched swabs from other areas of the victim’s body. The trial court denied the request. An intermediate appellate court affirmed the conviction and the denial of the request because “defendant did not

produce enough evidence that an expert would have aided the defense, nor did defendant raise enough specific concerns with the evidence." (footnote omitted). The Michigan Supreme Court reversed. It held that, following *Ake v. Oklahoma*, 470 U.S. 68 (1985), a remand was necessary to apply a due process analysis and, "in particular, whether defendant made a sufficient showing that there exists a reasonable probability both that an expert would be of assistance to the defense and that denial of expert assistance would result in a fundamentally unfair trial."

#Trial-Related

People v. Lively, 82 N.Y.S.3d 671 (N.Y. 4th Dep't App. Div. 2018)

The defendant was convicted of murder. On appeal, he argued that his counsel had not provided effective assistance when counsel failed to make timely motions to suppress. Evidence offered against the defendant was derived from the warrantless search of a garbage tote in the curtilage of his grandmother's house. The police conducted a limited search of the premises in search of a recently missing girl and that search fell within the emergency exception to the Warrant Requirement. Evidence consisting of CSLI and text messages was also offered. Assuming *arguendo* that *Carpenter v. United States* "applies with equal force to the contents of text messages sent to or received by the phone," the warrantless search of the phone was justified by exigent circumstances. Finally, although the Fourth Department acknowledged that the defendant's counsel had failed to object to the prosecutor's mischaracterization of DNA evidence, that mischaracterization did not rise to the level of misconduct that deprived the defendant of due process. The conviction was affirmed.

#Fourth Amendment – Exigent Circumstances

#Fourth Amendment – Warrant Required or Not

#Sixth Amendment – Assistance of Counsel

#Trial-Related

In re Alonzo M., 40 Cal.App.5th 156 (2019)

The defendant minor was declared a ward of the juvenile court and placed on probation. He challenged a condition that required him to submit his cell phone and other electronic devices to probation without a warrant at any time. The Court of Appeal affirmed the imposition of the condition because it would "help to ensure that Alonzo does not again succumb to the negative influences he blames for the criminal behavior that led to this wardship." However, it remanded for the

juvenile court to narrow any search to "any medium of communication reasonably likely to reveal whether Alonzo is associating with prohibited persons."

#Probation and Supervised Release

People v. Perkins, 184 A.D.3d 776 (N.Y. 2d Dep't App. Div. 2020) (*per curiam*)

The defendant, an airline pilot, was convicted of possessing a sexual performance by a child. Evidence against him was derived from a search of his iPad when the defendant landed at JFK airport on a flight from Montreal. Acting on advice from an agent in Texas, the defendant was taken to an interview room by DHS agents and given the option of unlocking the device so agents could look at it or leaving the device with the agents so a forensic examination could be conducted. He chose the former. An agent saw images of child pornography and a subsequent forensic examination found more. On appeal, the defendant argued, among other things, that the trial court had erred in denying his motion to suppress the content of the iPad. The Second Department affirmed:

> While federal circuit courts are split as to whether reasonable suspicion or something less than that is required to justify a manual search of an electronic device for contraband at the border, no court has required a warrant or probable cause for either a manual or forensic search of an electronic device for contraband at the border ***. Even assuming reasonable suspicion was required, here, the DHS Agents possessed reasonable suspicion to search the defendant's iPad for child pornography ***. Thus, contrary to the defendant's contention, the DHS Agents' manual search did not violate the defendant's fourth amendment right against unreasonable searches and seizures.

The appellate court also rejected the defendant's argument that he was coerced into entering his password:

> The defendant, who was told that he was free to leave, was not in custody when he was asked to enter the password ***. The fact that the defendant's iPad would be detained if he did not enter the password did not mean that he was 'subjected to the coercive atmosphere of a custodial confinement' ***. Further, since the DHS Agents had reasonable suspicion that contraband could be found on the iPad, the Agents could perform a forensic search of the iPad without a warrant ***. Thus, the Agents' threat to retain the device *** was not a false statement of authority that would render the defendant's act of inputting the password involuntary ***.

The Second Department did hold that statements made by the defendant after the images were discovered violated his right to counsel. However, that error was harmless given the overwhelming evidence of his guilt.

#Encryption

#Fifth Amendment – Self-Incrimination

#Fourth Amendment – Warrant Required or Not

People v. Powell, 2018 165 A.D.3d 842 (N.Y. 2d Dep't App. Div. 2018)

The defendant was convicted of murder and criminal possession of a weapon. Testimony was offered against him by an expert who performed DNA testing on the murder weapon and DNA analysis reports that set forth certain facts that tended to establish the defendant's guilt. The defendant's conviction was reversed on appeal because of prosecutorial misconduct during summation when the prosecutor, among other things, "misrepresented and overstated the probative value of the DNA evidence by telling the jury that the defendant's DNA was on the safety of the murder weapon." The Second Department also held that the defendant had been denied effective assistance of counsel when his attorney failed to object to the prosecutor's improper comments during summation.

#Sixth Amendment – Assistance of Counsel

#Trial-Related

People v. Spicer, 125 N.E.3d 1286 (Ill . App. Ct. 2019)

After the defendant was arrested for criminal possession of a controlled substance the State moved to compel him to disclose the password for a cell phone found on him when he was arrested. The defendant admitted that the phone belonged to him but would not provide the password. The trial court denied the motion, finding that it would violate the defendant's Fifth Amendment privilege against self-incrimination. The appellate court affirmed, adopting the reasoning of *G.A.Q.L. v. State*:

> Here, the State is not seeking the passcode per se but the information it will decrypt. The cases that declare the passcode to be a nontestimonial communication operate under the framework that the passcode is the testimonial communication and that it falls under the foregone conclusion exception to the fifth amendment privilege. We consider that the proper focus is not on the passcode but on the information the passcode protects. The State claims it sustained its burden of proving with reasonable particularity that it knew the passcode existed, that Spicer knew the passcode, and that it would be authenticated by entering it into Spicer's phone. However, what the State actually needed to establish with reasonable particularity was the contents of the phone, which it did not do.

> The State does not know what information might be on Spicer's phone but surmises that cell phones are often used in unlawful drug distribution and such information would be available on Spicer's phone. The State has not provided a particularized description of that information or even evidence that any useful information exists on the phone. The State sought and was granted in the search warrant access to most of the information in Spicer's phone, including call logs, text messages, multimedia messages, instant messaging communications, voicemail, e-mail, all messaging applications, phonebook contacts, videos, photographs, Internet browsing, and mapping history and GPS data between May 24 and June 24, 2017. The State does not identify any documents or specific information it seeks with reasonable particularity. The State is engaging in a fishing expedition, and the foregone conclusion exception does not apply here. Even if we were to conclude that the foregone conclusion exception properly focuses on the passcode, the State did not and could not satisfy the requirements for the foregone conclusion exception. While the State is aware that the passcode existed and that Spicer knew it, the State could not know that the passcode was authentic until after it was used to decrypt Spicer's phone. Moreover, the production of Spicer's passcode would provide the State more information than what it already knew. Although the focus of the foregone conclusion is on the passcode, in our view, it properly should be placed on the information the State is ultimately seeking, which is not the passcode but everything on Spicer's phone. We find that requiring Spicer to provide his passcode implicates his fifth amendment right against self-incrimination and the trial court did not err in denying the State's motion to compel.

#Fifth Amendment – Self-Incrimination

People v. Tafoya, No. 17CA1243, 2019 WL 6333762 (Colo. App. 2019)

> Police, acting without a warrant, installed a video camera near the top of a utility pole *** to surveil the home of defendant ***. For more than three months, the elevated camera provided police with continuous, recorded video surveillance surrounding Tafoya's home, including an area behind his privacy fence. Based on what police observed over that lengthy period, they obtained a search warrant, physically searched Tafoya's property, and found a large amount of controlled substances.

The defendant was convicted of narcotics-related offenses and, on appeal, challenged the trial court's denial of his motion to suppress. The Court of Appeals reversed on Fourth Amendment grounds and remanded for a new trial. The court held that the placement of the camera would not be a search *per se*, drawing an analogy to a police officer climbing a pole and looking into a backyard with a camera. However, after noting a split of authority on whether continuous

surveillance could constitute a search—as well as *Carpenter v. United States* (*q.v.*) and other Supreme Court decisions—the court concluded that a "three-month long surveillance of the curtilage" constituted a search. The Court of Appeals, however, did not "identify with precision the point at which the surveillance became a search, for the line was surely crossed long before the three-month mark."

#Fourth Amendment – Warrant Required or Not

People v. Tsintzelis, 146 N.E.3d 1160 (N.Y. 2020)

The defendants in this consolidated appeal were convicted solely on evidence of the DNA profile generated from post-arrest buccal swabs. The convictions were reversed and a new trial ordered:

> In *People v John*, we held that, when confronted with testimonial DNA evidence at trial, a defendant is entitled to cross-examine 'an analyst who witnessed, performed or supervised the generation of defendant's DNA profile, or who used his or her independent analysis on the raw data' ***. In *People v Austin*, we reiterated that a testifying analyst who did not participate in the generation of a testimonial DNA profile satisfies the Confrontation Clause's requirements only if the analyst 'used his or her independent analysis on the raw data to arrive at his or her own conclusions' ***. The records before us do not establish that the testifying analyst had such a role in either case. Accordingly, because the analyst's hearsay testimony as to the DNA profiles developed from the post-arrest buccal swabs 'easily satisfies the primary purpose test for determining whether evidence is testimonial ***, we conclude that her testimony and the admission of those DNA profiles into evidence, over defendants' objections, violated defendants' confrontation rights. (footnote omitted).

A concurring judge observed that, although the court was unanimous that the testimony presented was insufficient, "clarification of what type of witnesses, testimony and evidence suffice to meet a defendant's Confrontation Clause rights is warranted in these appeals and for future guidance."

#Admissibility

#Sixth Amendment – Right of Confrontation

People v. Ulett, 129 N.E.3d 909 (N.Y. 2019) (Ct. App. June 25, 2019)

The defendant was convicted of murder for the shooting of an individual outside an apartment building in Brooklyn. Several witnesses placed the defendant at the scene and two identified him as the shooter. The defendant argued on appeal that the prosecution had committed a reversible *Brady* violation by failing to disclose

"a surveillance video that captured the scene at the time of the shooting, including images of the victim and a key prosecution witness." The Court of Appeals reversed the conviction, concluding the video "would have changed the tenor of the trial, placing the People's case in such a different light as to undermine confidence in the verdict." The missing videotape could have been used to impeach the witnesses and would have provided leads for additional admissible evidence. Moreover, "the prosecutor's statements in summation, which denied the existence of a video, 'compounded the prejudice to the defendant.'"

#Discovery Materials

#Trial-Related

People v. Wakefield, 175 A.D.3d 158 (N.Y. 3d Dep't App. Div. 2019)

The defendant was convicted of murder and robbery. He challenged on appeal, among other things, the admissibility of DNA evidence that linked him to the crimes. The evidence was derived from buccal swab data eventually sent to a private company that used a software program called TrueAllele Casework System. The trial court conducted a *Frye* hearing and found that the evidence was admissible. The appellate court affirmed the conviction, concluding that the trial court had not erred in its analysis. Moreover, the appellate court rejected the defendant's argument that the *Frye* hearing was a "farce" because he did not have the opportunity to review the source code since that claim had been waived because he proceeded with the hearing in the absence of the source code and did not object in doing so. Finally, the Third Department rejected the defendant's argument that his right to confrontation had been abridged because he did not have access to the source code:

> Despite concluding that the TrueAllele report is testimonial, we do not find, given the particular facts of this case, that the source code, even through the medium of the computer, is a declarant. This is not to say that an artificial intelligence-type system could never be a declarant, nor is there little doubt that the report and likelihood ratios at issue were derived through distributed cognition between technology and humans ***. Indeed, similar to many expert reports, the testimonial aspects of the TrueAllele report are formulated through a synergy and distributed cognition continuum between human and machine ***, but this fact alone does not tip the scale so far as to transform the source code into a declarant. As Perlin explained at the *Frye* hearing, there is human input when utilizing TrueAllele. Among other things, a human analyst tells the computer what to download and under what conditions to analyze the data, the analyst tells the computer what questions to ask when interpreting the data and the analyst downloads certain results from the

> computer, the analyst determines how many 'runs,' or cycles, of the data the system will complete and the analyst then makes comparisons to form the likelihood ratios. Also key to our analysis is that Perlin, the creator of TrueAllele and the individual who wrote the underlying source code, was present in court and testified, at length, as to genetic science, the TrueAllele program and the formulation of the TrueAllele report through the computer processors and algorithms, including the MCMC algorithm ***. Given the totality of the circumstances present here, we find that Perlin was the declarant in the epistemological, existential and legal sense rather than the sophisticated and highly automated tool powered by electronics and source code that he created. Accordingly, because Perlin testified at trial, we find that there was no Confrontation Clause violation as alleged by defendant because he had the opportunity to confront his true accuser. (footnote omitted).

#Admissibility

#Discovery Materials

People v. Williams, 147 N.E.3d 1131 (N.Y. 2020)

> The primary issue on this appeal is whether the trial court should have held a *Frye* hearing (see *Frye v United States* ***) with respect to the admissibility of low copy number (LCN) DNA evidence and the results of a statistical analysis conducted using the proprietary forensic statistical tool (FST) developed and controlled by the New York City Office of Chief Medical Examiner (OCME). Under the circumstances of this case, we conclude that the trial court abused its discretion as a matter of law in admitting that evidence without holding such a hearing. However, inasmuch as the error is harmless, and inasmuch as defendant's other contentions lack merit, we ultimately conclude that the judgment should not be disturbed.

#Admissibility

Pollard v. State, 287 So.3d 649 (Fla. 1st Dist. Ct. App. 2019), pet. for review vol. dismissed, Case No.: SC20-110 (Fla. Mar. 25, 2020)

The defendant was arrested and charged with armed robbery. Law enforcement seized his iPhone pursuant to a warrant and sought to compel him to disclose the passcode so that "broad categories" of encrypted data could be accessed. The supporting affidavit did not "state the existence or content of any specific text, picture, call or other particular information" but noted that there was "reason to believe" that the defendant had used the iPhone to communicate with a co-

defendant. The trial court granted the motion to compel. The court of appeal reversed:

> To what extent does the Fifth Amendment right against self-incrimination protect a suspect in a criminal case from the compelled disclosure of a password to an electronic communications device in the state's possession? Courts differ in their legal analysis of this question, resulting in no consensus in state and federal courts; indeed, different approaches currently exist between two Florida appellate courts on the topic. In this case, we conclude that the proper legal inquiry on the facts presented is whether the state is seeking to compel a suspect to provide a password that would allow access to information the state knows is on the suspect's cellphone and has described with reasonable particularity.

#Encryption

#Fifth Amendment – Self-Incrimination

Puy v. State, 294 So.3d 930 (Fla. 4th Dist. Ct. App. 2020)

The defendant was charged under a Florida statute that made it a crime to post a threat to "conduct a mass shooting or an act of terrorism." He posted a still photo of himself on social media with the caption, "On my way! School shooter." The trial court denied the defendant's motion to dismiss and he pled *nolo contendere*. He argued on appeal that the trial court erred in not granting the motion "because the posting was vague and subject to interpretation, and he was not a threat to the school." The appellate court affirmed since "there remained a material fact at issue, that being the interpretation of appellant's posting on social media. In this case, that interpretation should be made by the factfinder and not by a sworn motion to dismiss."

#Social Media

D.R. v. D.A., 104 N.E.3d 665 (Mass. Ct. App. 2018)

This was an action in which D.R. sought a permanent abuse prevention order against her husband. The trial court granted the order, finding that the defendant's Facebook "like" of a birthday greeting to the wife was a "true threat." On appeal, the husband argued that the trial court had abused its discretion in construing the "like" as a threat of physical harm. The appellate court affirmed, concluding that the totality of the circumstances supported the order: The wife had been suffering from repeated verbal, physical, and emotional abuse from the husband. The "like" could be construed as a threat of imminent harm because the husband had posted

how someone with the wife's birthdate would die. The circumstances demonstrated that the "like" by the husband would be a reminder to the wife of the post.

#Social Media

H.R. v. NJ State Parole Board, 199 A.3d 297 (N.J. App. Div. 2018)Two convicted sex offenders challenged the imposition of continuous satellite-based GPS monitoring, arguing that the monitoring violated their right to be free from unreasonable searches under the New Jersey Constitution. The trial court held that the monitoring was a "special needs search" and that the governmental need to monitor convicted sex offenders outweighed the reduced privacy interest of one offender, who was serving parole supervision for life. The trial court also held that the government's need did not outweigh the privacy interest of the other offender, who had completed his sentence for a lesser crime. The Appellate Division affirmed both rulings.

#Probation and Supervised Release

In re Jawan S, 121 N.E.3d 1002 (Ill. App. Ct. 2018) The defendant was adjudicated a delinquent after being found guilty of firearms offenses. He was sentenced to two years' probation and appealed the imposition of three conditions, one that he not display any illegal gang, gun, or drug activity on his social media. The appellate court affirmed: (1) "Given the concerns *** about the actual or potential role of gangs in respondent's life, and the specific evidence that he was likely involved in a gang-related shooting ***, the *** online gang restrictions were directly related to the facts of the offense and the juvenile court's specific concerns about the potential obstacles to respondent's rehabilitation" and (2) "respondent has not identified any way in which the juvenile court's *** social-media condition places an unreasonable burden on his first-amendment rights."

#Probation and Supervised Release

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

The defendant's encrypted iPhone was seized at the time of her arrest on various charges. Despite an order compelling her to do so, the defendant refused to unlock the device on Fifth Amendment grounds and was held in contempt. She pled guilty to one charge but, because the contempt citation remained open, she still faced a sanction for failing to decrypt the device. The intermediate appellate court reversed the contempt order and the Indiana Supreme Court affirmed.

Applying United States Supreme Court precedent, the Indiana Supreme Court held:

> *** the act of production doctrine links the physical act to the documents ultimately produced. *** And the foregone conclusion exception relies

> on this link by asking whether the government can show it already knows the documents exist, are in the suspect's possession, and are authentic. *** True, the documents' contents are not protected by the Fifth Amendment because the government did not compel their creation. *** But the specific documents 'ultimately produced' implicitly communicate factual assertions solely through their production. ***
>
> When extending these observations to the act of producing an unlocked smartphone, we draw two analogies. First, entering the password to unlock the device is analogous to the physical act of handing over documents. *** And second, the files on the smartphone are analogous to the documents ultimately produced. ***
>
> Thus, a suspect surrendering an unlocked smartphone implicitly communicates, at a minimum, three things: (1) the suspect knows the password; (2) the files on the device exist; and (3) the suspect possessed those files.3 And, unless the State can show it already knows this information, the communicative aspects of the production fall within the Fifth Amendment's protection. Otherwise, the suspect's compelled act will communicate to the State information it did not previously know—precisely what the privilege against self-incrimination is designed to prevent. ***
>
> This leads us to the following inquiry: has the State shown that (1) Seo knows the password for her iPhone; (2) the files on the device exist; and (3) she possessed those files? (footnote omitted).

The Indiana Supreme Court then held that the State had not met its burden of proof:

> As discussed above, compelling Seo to unlock her iPhone would implicitly communicate certain facts to the State. And for those communicative aspects to be rendered nontestimonial, the State must establish that it already knows those facts.
>
> Even if we assume the State has shown that Seo knows the password to her smartphone, the State has failed to demonstrate that any particular files on the device exist or that she possessed those files. Detective Inglis simply confirmed that he would be fishing for "incriminating evidence" from the device. He believed Seo—to carry out the alleged crimes—was using an application or internet program to disguise her phone number. Yet, the detective's own testimony confirms that he didn't know which applications or files he was searching for ***.
>
> In sum, law enforcement sought to compel Seo to unlock her iPhone so that it could then scour the device for incriminating information. And Seo's act of producing her unlocked smartphone would provide the State

> with information that it does not already know. But, as we've explained above, the Fifth Amendment's privilege against compulsory self-incrimination prohibits such a result. Indeed, to hold otherwise would sound 'the death knell for a constitutional protection against compelled self-incrimination in the digital age.' ***
>
> Though the foregone conclusion exception does not apply to these facts, this case underscores several reasons why the narrow exception may be generally unsuitable to the compelled production of any unlocked smartphone. We discuss three concerns below.
>
> ***
>
> Extending the foregone conclusion exception to the compelled production of an unlocked smartphone is concerning for three reasons: such an expansion (1) fails to account for the unique ubiquity and capacity of smartphones; (2) may prove unworkable; and (3) runs counter to U.S. Supreme Court precedent. ***

Two Justices dissented on mootness grounds, although one stated that, although the majority's decision on the merits was not unreasonable, he would "come out the other way for the reasons further explained by Professor Kerr (footnote omitted)."

***NB*: See Prof. Kerr's article cited below for his summary of this decision and his approach to the compelled decryption of a cell phone.**

#Fifth Amendment – Self-Incrimination

State v. Adame, No. S-1-SC-36839, 2020 WL 4188121 (N.M. 18, 2020)

The defendants were suspected of drug trafficking. A federal grand jury issued subpoenas for, and secured, the defendants' bank records. Thereafter, a State grand jury issued subpoenas for records from two banks for a five-year period. The defendants were indicted in State court, primarily for crimes that were financial-related. They moved to suppress the records obtained by the federal subpoenas (which were the same records obtained by the State subpoenas) under the New Mexico Constitution. A trial court denied the motion and, on an interlocutory appeal, the Court of Appeals certified questions to the New Mexico Supreme Court, one of which was whether the New Mexico Constitution afforded greater protection than the Fourth Amendment, which would not protect the bank records. *United States v. Miller*, 425 U.S. 435 (1978). The New Mexico Supreme Court declined to depart from federal precedent in interpreting the New Mexico constitution because (1) the *Miller* analysis was not flawed and (2) "distinctive state characteristics do not support a reasonable expectation of privacy *** in the Adames' bank records, which consist of five years' of financial information

voluntarily shared with their banks." In so holding, the New Mexico Supreme Court rejected the argument that the narrowing of the third-party doctrine by *Carpenter v. United States*, 138 S. Ct. 2206 (2018), rendered *Miller* "flawed."

#Fourth Amendment – Warranted Required or Not

#Miscellaneous

#Third-Party Doctrine

State v. Andrews, A-72-18, 2020 WL 4577172 (N.J. Aug. 10, 2020)

> This appeal presents an issue of first impression to our Court -- whether a court order requiring a criminal defendant to disclose the passcodes to his passcode-protected cellphones violates the Self-Incrimination Clause of the Fifth Amendment to the United States Constitution or New Jersey's common law or statutory protections against self-incrimination. We conclude that it does not and affirm the Appellate Division's judgment.

#Fifth Amendment – Self-Incrimination

State v. Armstrong, No. A-2102-17T2, 2020 WL 2844219 (N.J. Super. Ct. App. Div. June 2, 2020)

The defendant pled guilty to offenses arising out of a murder. He appealed the denial of his motion to suppress incriminating text messages he had sent to his former girlfriend's cell phone, arguing that the warrantless seizure of the messages violated his rights under the New Jersey Constitution. The Appellate Division held that he did not have standing. The girlfriend consented to the search of the phone and the defendant did not have a reasonable expectation of privacy in the messages once he sent them to his girlfriend. The court also rejected the defendant's argument that he had a sufficient "participatory interest" because "the mere fact that the text messages could be evidence used by the State to prove defendant's commission of a crime does not confer standing ***."

#Fourth Amendment – Warrant Required or Not

State v. Brown, 815 S.E.2d 761 (S.C. 2018)

A cell phone was found in a home that had been burglarized. The phone was taken to a police station, secured in an evidence locker, and thereafter opened by a detective who guessed the passcode. The content of the phone led to the defendant, who was convicted of burglary. The trial court denied the defendant's motion to suppress the evidence derived from the warrantless search, finding that the phone

had been abandoned. The intermediate appellate court affirmed the conviction, as did the South Carolina Supreme Court. That court rejected the defendant's argument that the reasoning of *Riley v. California* "fundamentally alters the abandonment analysis when the property in question is the digital information on a cell phone." Instead, the court held that, "the unique character of cell phones *** is one factor a trial court should consider when determining whether the owner has relinquished his expectation of privacy." Examining the record, the court concluded: "The idea that a burglar may leave his cell phone at the scene of his crime, do nothing to recover the phone for six days, cancel cellular service to the phone, and then expect that law enforcement officers will not attempt to access the contents of the phone to determine who committed the burglary is not an idea that society will accept as reasonable."

#Fourth Amendment – Warrant Required or Not

State v. Culver, 918 N.W.2d 103 (Wis. Ct. App. 2018)

The defendant posted nude photos of a woman. He was convicted of violating a Wisconsin statute that criminalized posting or publishing a private depiction of a person and for being a felon in possession of a firearm. On appeal, he challenged the "posting or publishing" law as overbroad. The Wisconsin Court of Appeals rejected the argument: "Given the many boundaries that hem in the area of proscribed conduct, we conclude the statute is not overbroad." In doing so, the court had this to say about the use of hypotheticals:

> Culver criticizes the statute's failure to explain what happens if an image is published with consent, but the consent is later withdrawn. Culver questions whether the publisher would become criminally liable at that point. He does not explain, however, why this hypothetical tends to make the statute overbroad. We will not venture a guess. Although it is appropriate, and often necessary, to pose hypotheticals in mounting a facial challenge, the hypotheticals must point up situations where the statute impermissibly infringes on protected speech. Culver does not connect his hypothetical to a First Amendment violation.

#Social Media

State v. Denham, No. 78704-7-I, 2020 WL 2026799 (Wash. Ct. App. Div. 1 Apr. 27, 2020)

The defendant was convicted of burglary and trafficking in stolen property. He challenged on appeal, among other things, the constitutionality of a warrant to search his cell phone records and data. The Court of Appeals held that there was an insufficient nexus between burglary and the cell phone records:

> the police sought the records from Denham's phones, specifically the CSLI, for the crime of burglary. We reject the notion that the CSLI would be necessary to prove the crime of trafficking given the evidence already known to police. Even if it were, the affidavits fail to provide any specific nexus between the CSLI and the trafficking investigation. The affidavits do not establish a sufficient nexus between the crime of burglary and the thing to be searched, Denham's cell phone records, particularly as the State did not establish identity or even a basic description of the person or persons involved in the burglary.
>
> ***
>
> There was no conclusive fingerprint or DNA evidence found at the scene of the burglary and the specific method of entry differed from those associated with Denham's past burglary convictions. There was no security footage or eyewitness to suggest an approximate physical description of the suspect to compare against Denham. Additionally, there was no evidence to suggest that there were other accomplices or co-conspirators with whom the perpetrator of the burglary would have necessarily been communicating. The application for the search warrant for Denham's cell phone records was insufficient as it failed to provide specific information demonstrating a nexus between Denham, the criminal act, the information to be seized and the item to be searched. We reverse the trial court's ruling on Denham's motion to suppress as to the warrant for his cell phone records.

For this and an error related to admissibility, the appellate court reversed and remanded for a new trial.

#CSLI

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Miscellaneous

State v. Diamond, 905 N.W.2d 870 (Minn. 2018)

> This case presents an issue of first impression: whether the Fifth Amendment privilege against self-incrimination protects a person from being ordered to provide a fingerprint to unlock a seized cellphone. Neither the Supreme Court of the United States nor any state supreme court has addressed this issue.
>
> The police lawfully seized a cellphone from appellant Matthew Diamond, a burglary suspect, and attempted to execute a valid warrant to search the cellphone. The cellphone's fingerprint-scanner security lock, however, prevented the search, and Diamond refused to unlock the cellphone with his fingerprint, asserting his Fifth Amendment privilege

> against self-incrimination. The district court found no Fifth Amendment violation and ordered Diamond to provide his fingerprint to unlock the cellphone so that the police could search its contents. After the court of appeals affirmed, we granted Diamond's petition for review. Because the compelled act here—providing a fingerprint—elicited only physical evidence from Diamond's body and did not reveal the contents of his mind, no violation of the Fifth Amendment privilege occurred. Accordingly, we affirm.

#Encryption

#Fifth Amendment – Self-Incrimination

State v. Ghigliotty, No. A-0938-19T3, 2020 WL 1908508 (N.J. App. Div. Apr. 20, 2020)

> In this appeal, we address the novel issue of whether a firearms toolmark identification expert's use of untested three-dimensional (3D) computer imaging technology *** requires a Frye hearing to be held to establish the scientific reliability of the *** [technology].

The appellate court held that the hearing was required. The Appellate Division also vacated directives by the trial court related to discovery of algorithms used in the technology and remanded for consideration of the defendant's need for the discovery against, among other things, the proprietary nature of the technology.

#Admissibility

#Discovery Materials

State v. Green, 216 A.3d 104 (N.J. Sup. Ct. 2019)

> In this case, a robbery victim identified her assailant from an extensive database of digital photos. To assess the reliability of the identification process requires an understanding of modern-day digital databases.
>
> In some respects, they are today's equivalent of a paper mugshot book. In other ways, digital systems are far superior, thanks to advances in technology. The system used here, for example, allows officers to pare down a large field of photos to match a witness's physical description of a suspect. When an eyewitness selects a photo that looks similar to the culprit, the system can further narrow the field to display only other similar images. Officers can also print copies of photos and generate a report of what a witness viewed.
>
> In this appeal, the witness was mistakenly allowed to review digital photos through a feature of the database meant to be used by law

enforcement officers, not eyewitnesses. In addition, the police saved only the photo the victim ultimately selected -- an image of defendant. Beyond that, the system contained multiple photos of defendant because of his recent prior arrests, which raises concerns about mugshot exposure and its effect on the reliability of identifications.

We consider what took place in light of known risks associated with eyewitness identification, as well as case law and a court rule that address how identification procedures should be conducted and preserved. We also propose revisions to Rule 3:11 to offer clearer guidance on which photos officials should preserve when they use an electronic database to identify a suspect. In addition, to guard against misidentification, we place on the State the obligation to show that an eyewitness was not exposed to multiple photos or viewings of the same suspect.

Under the circumstances, we find that the trial court properly suppressed the identification in this case. We therefore affirm and modify the judgment of the Appellate Division majority, which largely upheld the trial court.

#Miscellaneous

#Trial-Related

State v. Jackson, 214 A.3d 211 (N.J. App. Div. 2019), *aff'd o.b.*, No. 083286, 2020 WL 1541100 (N.J. Apr. 1, 2020) (*per curiam*).

The defendants in this consolidated appeal had been arrested and confined in a county correctional facility. The facility had a policy that permitted inmates to make telephone calls subject to monitoring and recording and the defendants were aware of the policies. They made incriminating calls and recordings of the calls were secured through grand jury subpoenas. The trial court suppressed the recordings. The Appellate Division reversed. It held that federal and State statutory wiretap proscriptions did not apply to inmate phone calls recorded in prisons and that providing the recordings in response to the subpoenas was not an "interception." The Appellate Division also held that the defendants had no reasonable expectation of privacy in their recorded calls.

#Miscellaneous

#Fourth Amendment – Warrant Required or Not

State v. R.K., Docket Nos. No. A-2022-18T2, 2020 WL 1982276 (N.J. App. Div. Apr. 27, 2020)

The defendant, a convicted sex offender, challenged a regulation which imposed a supervised release condition that banned him from using the Internet to access social media. Relying on *Packingham v. North Carolina*, 137 S. Ct. 1730 (2017), and subsequent decisions, the Appellate Division held the "blanket" ban unconstitutional on its face and as applied because the defendant's sex offender-related convictions were unrelated to his use of social media or the Internet and abridged his constitutionally protected free speech. The appellate court also held that *Packingham* should be applied retroactively. However, the court did not preclude the imposition of less restrictive Internet restrictions on remand.

#Probation and Supervised Release

#Social Media

State v. Lizotte, 197 A.3d 362 (Vt. 2018)

> This case requires us to consider whether defendant's Fourth Amendment rights were violated when his online service provider, AOL, searched his transmissions, detected suspected child pornography, and sent information to the National Center for Missing and Exploited Children (NCMEC), which opened the email and attachment and provided it to law enforcement. We conclude that AOL was not acting as an agent of law enforcement when it searched defendant's transmissions, and that NCMEC and law enforcement did not expand AOL's private search by viewing the file already identified by AOL as containing child pornography. In addition, any expansion of the search by opening the related email did not invalidate the warrant because the other information in the affidavit independently provided probable cause to search. We affirm.

#Fourth Amendment – Warrant Required or Not

State v. Manning, 222 A.3d 662 (N.J. 2020)

The defendant was convicted of murder and related crimes. On the date the crimes were discovered law enforcement secured a warrant to search the vehicle in which the body was found. On the same day an investigator identified a person of interest. Rather than secure a warrant he submitted an "exigent circumstances request form" to AT&T for that person's cell phone records. On the day after he secured the records the investigator prepared detailed affidavits for the issuance of three warrants. Thereafter, the defendant was arrested and convicted. An appellate

court reversed the conviction, holding that evidence derived from the warrantless search of the records should have been suppressed. The New Jersey Supreme Court affirmed:

> In determining whether Detective Frazer's warrantless search of defendant's cell-phone records on the evening of August 16 was an objectively reasonable response to an exigency that did not permit time to secure a court order, we do not view the events through the 'distorted prism of hindsight,' *** but we also do not put on blinders. Any consideration of objective reasonableness must take into account the totality of the circumstances. ***. The Prosecutor's Office obtained a search warrant earlier in the day on August 16 and three search warrants the next day when a clear suspect was in sight. The State bore the burden of establishing the existence of an objectively reasonable basis to believe that there was a threat to members of the public or of destruction of evidence that made the securing of a court order impracticable. *** Generalized fears do not meet that standard. A review of the totality of the evidence reveals that the Prosecutor's Office was able to comply with the dictates of the warrant requirement of our State Constitution during the murder investigation. The State failed to satisfy its burden of proving that the warrantless search of defendant's cell-phone records was objectively reasonable to meet the type of exigency recognized in our jurisprudence. (citations omitted).

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

State v. Mixton, 447 P.3d 829 (Ariz. Ct. App. Div. Two 2019)

The defendant was convicted on twenty counts of sexual exploitation of a minor. He was identified as a result of an undercover operation through an ad on an internet advertising forum. After a person-to-person message exchange with an undercover detective, federal agents participating in the investigation served a federal administrative subpoena on the messaging provider to obtain the defendant's IP address. This led to another federal subpoena to an internet service provider, which gave a street address of the user to whom the IP address was assigned. This led to a search warrant for the address. The police seized various electronic devices during execution of the warrant. Images found on these devices led to the prosecution and convictions. The defendant moved to suppress, arguing that the Fourth Amendment and the corresponding section of the Arizona Constitution required a warrant or other court order. The trial court denied the motion, finding that the defendant had no recognized privacy interest in subscriber information. The Court of Appeals reversed. It held that the defendant did not have

a "federally recognized privacy interest in his subscriber information or IP address" and, therefore, the Fourth Amendment was inapplicable. However, turning to an analysis of the Arizona Constitution, the Court of Appeals rejected the application of the third-party doctrine:

> we conclude that internet users generally have a reasonable expectation of privacy in their subscriber information. We therefore join the several other states that have declined to apply the federal third-party doctrine established in Miller and Smith under their state constitutions in circumstances analogous to those before us. In the internet era, the electronic storage capacity of third parties has in many cases replaced the personal desk drawer as the repository of sensitive personal and business information—information that would unquestionably be protected from warrantless government searches if on paper in a desk at a home or office. The third-party doctrine allows the government a peek at this information in a way that is the twenty-first-century equivalent of a trip through a home to see what books and magazines the residents read, who they correspond with or call, and who they transact with and the nature of those transactions. Cf. Riley v. California ***. We doubt the framers of our state constitution intended the government to have such power to snoop in our private affairs without obtaining a search warrant.
>
> ***
>
> We are mindful our supreme court has expressed a reluctance to depart from Fourth Amendment precedent in analyzing suppression issues under article II, § 8. *** But the federal third-party doctrine, at least as applied to obtain Mixton's identity here, is unsupportable in our view. We therefore decline to apply it on independent state law grounds. *** Because the search warrant in this case was issued based upon identifying information obtained in violation of Mixton's rights under article II, § 8, we turn to the issue of whether the evidence recovered in execution of the warrant should have been suppressed. (footnote omitted).

The Court of Appeals then held that the good faith exception to the Warrant Requirement of the Arizona Constitution applied as it was objectively reasonable for the police to have relied on a "significant body of appellate law, some of it binding," and affirmed the convictions. The Court of Appeals also rejected the defendant's argument that Arizona statutory exceptions to the exclusionary rule applied.

#Fourth Amendment – Good Faith Exception

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

State v. Morrill, No. A-1-CA-36490, 2019 WL 3765586 (N.M. Ct. App. July 24, 2019)

The defendant was convicted of sexual exploitation of children. The charges against him arose from his "use of BitTorrent, a peer-to-peer, file-sharing network, to access child pornography." On appeal, he challenged, among other things, the use of Roundup software to identify him. The Court of Appeals rejected that challenge, holding that the trial court—which had conducted a *Daubert* hearing—had not abused its discretion "when it determined that the evidence generated by Roundup was sufficiently reliable to be admitted at trial." The appellate court also rejected a hearsay challenge to the use of computer-generated evidence: "Because the software programs make the relevant assertions, without any intervention or modification by a person using the software, we conclude that the assertions are not statements by a person governed by our software rules." (footnote omitted).

#Admissibility

State v. Phillip, 452 P.3d 553 (Wash. Ct. App. Div. 1 2019)

The defendant had been convicted of murder. Evidence against him included CSLI. The Court of Appeals reversed that conviction, concluding the affidavits used to secure the CSLI were not supported by probable cause. After reversal, the State moved the trial court for issuance of a subpoena directed to the defendant's service provider. The supporting affidavit attached prior ones that included information from CSLI that had been determined to be tainted. The trial court allowed the subpoena and the defendant granted interlocutory review. The Court of Appeals suppressed the subpoena under the warrant requirement of the Washington Constitution and the Fourth Amendment, relying on the Supreme Court's decision in *Carpenter v. United States*. The Court of Appeals also held that the warrant submitted in support of the subpoena failed to establish probable cause and that the trial court had not made sufficient particularized findings that supported the existence of probable cause.

#Fourth Amendment – Warrant Required or Not

State v. Shackelford, 825 S.E.2d 689 (N.C. Ct. App. 2019)

The defendant was convicted on four counts of felony stalking based primarily on the contents of posts on his Google Plus account. He had posted about a woman with whom he had an encounter and who secured a "no contact" order against him. On appeal, the defendant asserted an as-applied challenge to the statute under which he was convicted. In reversing the conviction, the North Carolina Court of

Appeals held that defendant's posts were not "speech integral to criminal conduct" such that the First Amendment did not apply. The court then held that, as applied to the defendant, the statute was a content-based restriction that had to survive strict scrutiny. Finally, the court held that the statute did not survive strict scrutiny because there was a less restrictive means to accomplish its goal, the no-contact order.

#Social Media

State v. Solomon, 419 P.3d 436 (Wash. Ct. App. Div. 1 2018)

The State appealed from an order that dismissed the charges against the defendant, finding that the actions of a police officer constituted outrageous conduct in violation of the defendant's due process rights. Here are the relevant facts:

> a law enforcement officer anonymously published an advertisement on an online classifieds platform reserved for those over the age of 18 and indicated that she was "a young female" seeking an individual interested in a casual sexual encounter. Joshua Solomon responded to the advertisement. Thereafter, the police officer assumed the guise of a fictional 14-year-old girl and sent Solomon nearly 100 messages laden with graphic, sexualized language and innuendo and persistently solicited him to engage in a sexual encounter with the fictional minor, notwithstanding that he had rejected her solicitations seven times over the course of four days.

The Washington Court of Appeals affirmed: "Given the court's finding that law enforcement had initiated and controlled the criminal activity, persistently solicited Solomon to commit the crimes so initiated, and acted in a manner (through the use of language and otherwise) repugnant to the trial judge's view of the community's sense of justice, the trial court's determination was tenable."

#Miscellaneous

#Social Media

State v. Terrell, 831 S.E.2d 17 (N.C. 2019)

The defendant was convicted of various charges related to child pornography. On appeal, he challenged the denial of his motion to suppress evidence derived from the warrantless search of a USB drive. The defendant's girlfriend had taken the drive from the defendant's briefcase, plugged it in, and uncovered images of her infant granddaughter. She and her daughter took the drive to law enforcement and a detective plugged it in, finding the granddaughter's image as well as others that might be child pornography. He stopped the search and then law enforcement

secured a warrant to search the drive. The trial court denied the defendant's motion to suppress based on the "private search doctrine." An intermediate appellate court reversed on the ground that the detective's search exceeded the scope of the girlfriend's "search" and remanded for the trial court to consider whether, absent the suppressed evidence, probable cause existed for the issuance of the warrant. The North Carolina Supreme Court affirmed:

> After viewing several non-incriminating images, Ms. Jones ceased her search upon finding the image of Sandy. Ms. Jones did not view any of the incriminating photos that were later discovered by Detective Bailey in an entirely separate folder. Had Bailey possessed virtual certainty of the device's contents, presumably he would not have been 'scrolling through . . . a lot of photos' in different folders before, according to him, he 'finally happened upon the photograph with the granddaughter.' It is clear that Ms. Jones's limited search did not frustrate defendant's legitimate expectation of privacy in the entire contents of his thumb drive and that Detective Bailey's follow-up search to locate the image of Sandy was not permissible under *Jacobsen* because he did not possess 'a virtual certainty that nothing else of significance was in the [thumb drive] and that a manual inspection of the [thumb drive] and its contents would not tell him anything more than he already had been told' by Jones. (footnote omitted).

#Fourth Amendment – Warrant Required or Not

State v. VanBuren, 214 A.3d 791 (Vt. 2019)

The defendant was charged with disclosure of nonconsensual pornography in violation of Vermont's "revenge pornography" law. She moved to dismiss the charge against her, arguing that the statute violated the First Amendment because it restricted protected speech and could not survive strict scrutiny. She also argued that the complainant had no reasonable expectation of privacy in her images because these had been sent to a Facebook user. The defendant had accessed the user's account without permission and posted the images to "teach her a lesson." The trial court granted the motion. The Vermont Supreme Court reversed: "[t]he statute is narrowly tailored to advance the State's interests, does not penalize more speech than necessary to accomplish its aim, and does not risk chilling protected speech on matters of public concern." The court directed the parties to brief an "as applied" challenge and other statutory issues.

#Social Media

State v. Verrill, Docket No. 219-2017-CR-072 (N.H. Super. Ct. Nov. 5, 2018) (Order on Motion to Search in Lieu of Search Warrant)

The State moved to allow the search of servers and/or records maintained by Amazon for recordings made by an Echo smart speaker with Alexa voice command capacity. The court found that the State could proceed *ex parte* as the defendant had no standing to object to the motion and that there was probable cause to believe that the server and/or records may contain evidence of a murder and possible removal of a body. Accordingly, it issued an order directing Amazon to produce recordings for a two-day period.

#Miscellaneous

Weida v. State, 94 N.E.3d 682 (Ind. 2018)

The defendant had sexual intercourse with a minor. They told police that before they had sex they looked at pictures of the minor on her cell phone, viewed other explicit photos on the defendant's phone, and the minor showed the defendant a website she had found about incest. The defendant also admitted that he used his phone to google explicit photos and showing those to the minor. The defendant pled guilty to felony incest and was sentenced to imprisonment for one year and two years' probation. Two special conditions were imposed, the first prohibiting the defendant from, among other things, accessing or using certain websites, chat rooms, or IM programs frequented by children and the second broader condition barring the defendant from accessing the Internet without prior approval by his probation officer. An intermediate appellate court upheld the conditions. The Indiana Supreme Court reversed in part. The court upheld the first condition: "When a defendant commits a sex crime against a child, as happened here, it is reasonable to restrict that defendant's access to children through any medium." However, the Supreme Court found that the trial court had abused its discretion by "imposing an unreasonable probation condition that did not reasonably relate to rehabilitating Weida and protecting the public" and remanded with instructions to impose a reasonable Internet restriction.

#Probation and Supervised Release

#Social Media

I/M/O Welfare of: A. J. B., Child, 929 N.W.2d 840 (Minn. 2019)

The appellant, a minor, created an anonymous Twitter account and used it to post "cruel and egregious insults" about a fellow student. The appellant was charged under two Minnesota statutes, one directed at stalking-by-mail and the other at

mail-harassment. He moved to dismiss the charges, arguing, among other things, that the statutes were facially overbroad in violation of the First Amendment. The trial court denied the motion and the appellant was found guilty and adjudicated a delinquent. The intermediate appellate court affirmed. The Minnesota Supreme Court held the stalking-by-mail statute to be unconstitutional because of "the substantial ways in which *** [it] can prohibit and chill protected expression" and because the statute was not subject to a narrowing construction. The Supreme Court severed two words from the mail-harassment statute and, having done so, upheld it. The supreme court remanded to determine whether the appellant's adjudication under the mail-harassment statute could stand under the statute as narrowed.

#Social Media

Wright v. Morsaw, 232 So. 3d 10 (Fla. 4th Dist. Ct. App. 2017) (*per curiam)*

The petitioner, a defendant in related civil and criminal actions, sought to quash portions of a discovery order entered in the civil action that required him to provide certain records over his Fifth Amendment privilege against self-incrimination objections. The petitioner was charged with criminal offenses for a hit-and-run accident that resulted in a pedestrian's death. He was also sued in a wrongful death action brought by the decedent's estate. After the accident, the defendant allegedly fled to a friend's home, posted about the accident on social media, and hid the vehicle he had been driving. The discovery order in issue directed the petitioner to, among other things, identify and produce digital copies of his social media accounts. The District Court of Appeal denied relief: "Regarding the social media records, petitioner has not demonstrated a 'link' or shown that he is being asked to furnish or reveal anything that he did not already publically post." (footnote omitted). The court did note that "there are many potential issues surrounding the testimonial nature of social media and the production of passwords. *** This case, however, does not involve the production of social media passwords."

#Social Media

DECISIONS – FOREIGN

ACL Netherlands BV v. Lynch, [2019] EWHC 249 (Ch), Case No: HC-2015-001324 (High Court of Justice Dec. 2, 2019)

This was an application for permission to provide to the FBI copies of documents and witness statements served in preparation for a trial in England. The documents and statements had been sought pursuant to a grand jury subpoena issued out of the Northern District of California. The court denied the application because the applicants had "failed to show that the disclosure of documents and witness statement is necessary for the purpose of the US process." Moreover, the court was not persuaded that the applicants had shown "compulsion either, even accepting that the US subpoena is entirely regular."

#International

Elgizouli v. Secretary of State for the Home Dep't, [2020] UKSC 10**,** https://www.supremecourt.uk/cases/uksc-2019-0057.html

#Miscellaneous

STATUTES, REGULATIONS, ETC. – FEDERAL

Comput. Crime & Intellectual Prop. Section, Criminal Div., U.S. Dep't of Just., "*Seeking Enterprise Customer Data Held by Cloud Service Providers*" (Dec. 2017), https://www.justice.gov/criminal-ccips/file/1017511/download

#Miscellaneous

#SCA (Stored Communications Act)

Dep't of Homeland Security, "*Privacy Impact Assessment for the U.S. Border Patrol Digital Forensics Programs*" (July 30, 2020), https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp053a-digitalforensics-july2020.pdf

Federal Reserve, "*Synthetic Identity Fraud in the U.S. Payment System: A Review of Causes and Contributing Factors"* (Payments Fraud Insights July 2019), https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf

#Miscellaneous

Foreign Corrupt Practices Act of 1977 – Corporate Enforcement Policy, U.S. Department of Justice Manual, 9-47.120, March 2019 (requiring companies implement "appropriate guidance and controls on the use of personal communications and ephemeral messaging platforms") https://www.justice.gov/jm/jm-9-47000-foreign-corrupt-practices-act-1977

#Preservation and Spoliation

OECD, Directorate for Financial and Enterprise Affairs Competition Committee, Algorithms and Collusion – Note by the United States (May 26, 2017), https://one.oecd.org/document/DAF/COMP/WD(2017)41/en/pdf

#International

#Miscellaneous

Office of the Inspector General, U.S. Dep't of Just., "*Oversight and Review Div. 18-03, A Special Inquiry Regarding the Accuracy of FBI Statements Concerning the Capabilities to Exploit an iPhone Seized During the San Bernardino Terrorist Attack Investigation*" (Mar. 2018), https://oversight.gov/report/doj/special-inquiry-regarding-accuracy-fbi-statements-concerning-its-capabilities-exploit

#Encryption

Pretrial Discovery Conference; Request for Court Action, Fed. R. Crim. P. 16.1 (eff. Dec. 1, 2019), https://www.law.cornell.edu/rules/frcrmp/rule_16.1

#Discovery Materials

U.S. Customs & Border Prot., Directive No. 3340-049A, CBP Directive: *Border Search of Electronic Devices* (Jan. 4, 2018), https://www.cbp.gov/document/directives/cbp-directive-no-3340-049a-border-search-electronic-devices

#Fourth Amendment – Warrant Required or Not

U.S. Dep't of Just., *Policy Regarding Applications for Protective Orders Pursuant to 18 U.S.C. [Section] 2705(b)* (Oct. 19, 2017), https://www.documentcloud.org/documents/4116081-Policy-Regarding-Applications-for-Protective.html

#Miscellaneous

#Social Media

#SCA (Stored Communications Act)

U.S. Dep't of Just., "*Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*" (Apr. 2019), https://www.justice.gov/opa/press-release/file/1153446/download

#International

STATUTES, REGULATIONS, ETC. – STATE

"*An Act to Amend the Criminal Procedure Law and the Penal Law, in Relation to Establishing New Criminal Discovery Rules* ***," 2019 NY S.B. 1716 (NS), https://legislation.nysenate.gov/pdf/bills/2019/S1716

#Discovery Materials

Order Granting Expedited Approval of Proposed Amendments to Rule 5-110 of the California Rules of Prof. Conduct, Admin. Order 2017-11-01 (Cal. Sup. Ct. Nov. 2, 2017) (en banc), http://www.courts.ca.gov/documents/order_granting_approval_of_proposed_amendments_to_rule_5_110_of_the_california_rules_of_professional_conduct.pdf

#Discovery Materials

Press Release, Office of New York State Governor Andrew M. Cuomo, "*Governor Cuomo Signs Legislation Affirming the Right to Record Law Enforcement Activity*," (June 14, 2020), https://www.governor.ny.gov/news/governor-cuomo-signs-legislation-affirming-right-record-law-enforcement-activity

#Miscellaneous

Timing of Discovery, The New York State Senate Criminal Procedure (CPL) Sec. 245.10, *et seq.* (eff. Jan. 1, 2020), https://www.nysenate.gov/legislation/laws/CPL/245.10

#Admissibility

#Discovery Materials

#Miscellaneous

#Preservation and Spoliation

Utah Electronic Information or Privacy Act, 2019 UT H.B. 57 (NS), as amended, https://le.utah.gov/~2019/bills/static/HB0057.html

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

#Third-Party Doctrine

STATUTES, REGULATIONS, ETC. – FOREIGN

Crime (Overseas Production Orders) Act 2019 (enacted Feb. 12, 2019), https://www.legislation.gov.uk/ukpga/2019/5/section/1/enacted

#International

European Commission, "*Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Cases, {SWD(2018) 118 final} – {SWD(2018) 119 final}*" (Apr. 17, 2018), https://ec.europa.eu/info/sites/info/files/placeholder.pdf

#International

European Data Protection Board, "*European Data Protection Board, Initial Legal Assessment of the Impact of the US Cloud Act on the EU Legal Framework for the Protection of Personal Data and the Negotiations of an EU-US Agreement on Cross-Border Access to Electronic Evidence*" (July 10, 2019), https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_edps_joint_response_us_cloudact_annex.pdf

#International

#SCA (Stored Communications Act)

European Data Protection Supervisor, Opinion 2/2019, "*EDPS Opinion on the negotiating mandate of the EU-US Agreement on cross-border access to electronic evidence*" (Apr. 2, 2019), https://edps.europa.eu/sites/edp/files/publication/19-04-02_edps_opinion_on_eu_us_agreement_on_e-evidence_en.pdf

#International

Press Release, European Commission, "*Security Union: Commission Facilitates Access to Electronic Evidence*" (Apr. 17, 2018), http://europa.eu/rapid/press-release_IP-18-3343_en.htm

#International

ARTICLES

Allen & Overy, "*Growing Pressure on Technology Companies to Disclose Customer Data Quickly*" (Apr. 1, 2019), http://www.allenovery.com/publications/en-gb/Pages/Growing-pressure-on-technology-companies-to-disclose-customer-data-quickly.aspx

#International

T. Alper, "*Criminal Defense Attorney Confidentiality in the Age of Social Media*," *Criminal Justice* 4 (ABA Sec. of Crim. Justice: Fall 2016), https://works.bepress.com/ty_alper/18/download/

#Sixth Amendment – Assistance of Counsel

#Social Media

R.J. Anello & R.F. Albert, "*The International Encryption Debate: Privacy vs. Big Brother*," *N.Y.L.J.* (posted June 11, 2019), https://www.law.com/newyorklawjournal/2019/06/11/the-international-encryption-debate-privacy-versus-big-brother/

#Encryption

#International

M. Artzt & W. Delacruz, "*How to Comply with Both the GDPR and the CLOUD Act*," The Daily Advisor (posted Jan. 29, 2019), https://iapp.org/news/a/questions-to-ask-for-compliance-with-the-eu-gdpr-and-the-u-s-cloud-act/

#International

S. Barney, "*Border Phone Search Questions Continue in Federal Court*," Law360 (posted June 18, 2019), https://www.law360.com/articles/1170102/border-phone-search-questions-continue-in-federal-court

#Fourth Amendment – Warrant Required or Not

J.R. Barr, *et al.*, "*COVID-19's Effects on Crim. Procedure*," *BakerHostetler Alerts* (posted Apr. 20, 2020), https://www.bakerlaw.com/alerts/covid-19s-effects-on-criminal-procedure

#Sixth Amendment – Assistance of Counsel

#Miscellaneous

I. Boudway, "*Someday Your Self-Driving Car Will Pull Over for Police*," Bloomberg Law (posted Feb. 20, 2019), https://www.bloomberg.com/news/features/2019-02-20/someday-your-self-driving-car-will-pull-over-for-police

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

M.J. Brannon, "*Carpenter v. United States: Building a Property-Based Fourth Amendment Approach for Digital Data*," Criminal Justice 20 (ABA: Winter 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/winter/carpenter-v-united-states/

#Fourth Amendment – Warrant Required or Not

K.V. Brown, "*Law Enforcement Can Do Whatever It Likes with Consumer DNA Data,"* Bloomberg Law News (posted Feb. 26, 2019), https://news.bloomberglaw.com/pharma-and-life-sciences/law-enforcement-can-do-whatever-it-likes-with-consumer-dna-data

#Miscellaneous

J.G. Browning & L. Angelo, "*Alexa, Testify: New Sources of Evidence from the Internet of Things*," 82 Tex. B.J. 506 (The State Bar of Texas: July 2019), https://www.texasbar.com/AM/Template.cfm?Section=articles&Template=/CM/HTMLDisplay.cfm&ContentID=46469

#Admissibility

#Discovery Materials

J.P. Carlin, et al., "*CLOUD Act Compliance: Key Takeaways for U.S. Companies from the U.S.-U.K. Executive Agreement*" Client Alert (posted Oct. 9, 2019), https://www.mofo.com/resources/insights/191009-cloud-act-compliance.html

#Miscellaneous

#Stored Communications Act

D. Cave, "*Australian Gag Order Strokes Global Debate on Secrecy*," N.Y. Times A9 (Dec. 15, 2018), https://www.nytimes.com/2018/12/14/world/australia/australia-gag-order-court.html

#International

J. Cedarbaum, *et al*., "*Digital Privacy One Year After Carpenter*," Law360 (posted June 20, 2019), https://www.law360.com/articles/1170123/digital-data-privacy-one-year-after-carpenter

#Fourth Amendment – Warrant Required or Not

T. Claburn, "*To Catch a Thief, Go to Google with a Geofence Warrant – And It Will Give You All the Details*," Security Shelf (posted Jan. 18, 2020), https://securityshelf.com/2020/01/18/to-catch-a-thief-go-to-google-with-a-geofence-warrant-and-it-will-give-you-all-the-details/

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

T.T. Chung, "*Evidence Collection in Criminal Investigations: Cross-Border Issues and Corporate Employee Considerations*," Jones Day White Paper (Jan. 2020), https://www.jonesday.com/en/insights/2020/01/evidence-collection-in-criminal-investigations

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

P. Crusco, "*Impeachment by Social Media*," N.Y.L.J. (posted June 25, 2018), https://www.law.com/newyorklawjournal/2018/06/25/impeachment-by-social-media/?slreturn=20190603161012

#Admissibility

#Social Media

#Trial-Related

"*Cybercrime 2020: Revisiting the Future of Online Crime and Investigations*," Georgetown Law 12 (Spring/Summer 2019), https://www.law.georgetown.edu/magazine/

#Miscellaneous

F.T. Davis & A.R. Gressel, "Storm Clouds or Silver Linings? The Impact of the U.S. CLOUD Act," Litigation 47 (ABA: Fall 2018), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2018-19/fall/storm-clouds-or-silver-linings/

#International

#SCA (Stored Communications Act)

M.E. Diamantis, "*The Problem of Algorithmic Corporate Misconduct*," Program on Corporate Compliance and Enforcement (posted Sept. 16, 2019), https://wp.nyu.edu/compliance_enforcement/?s=algorithmic+corporate+misconduct

#Miscellaneous

M.P. Diehr, "*The Yates Memo and Its Effects on White Collar Representation and Internal Investigations—A Two-Year Look Back*," Federal Lawyer 36 (Federal Bar Association Sept. 2018), http://www.fedbar.org/Resources_1/Federal-Lawyer-Magazine/2018/September/Features/The-Yates-Memo-And-Its-Effects-On-White-Collar-Representation-And-Internal-Investigations-A-Two-Yea.aspx?FT=.pdf

#Miscellaneous

W. Diffle, "*The Encryption Wars are Back but in Disguise*," Scientific American (posted June 30, 2020), https://www.scientificamerican.com/article/the-encryption-wars-are-back-but-in-disguise/

#Encryption

"*DOJ Scales Back Yates Memo Policy for Corporate Cooperation*," Government/Regulatory Enforcement (posted Dec. 5, 2018), https://www.lit-wc.shearman.com/doj-scales-back-yates-memo-policy-for-corporate

#Miscellaneous

D. Filor, *et al.*, "*DOJ Eases Stance on Use of Disappearing Message Platforms in Corporate Enforcement Policy*," GT Alert (posted Mar. 21, 2019), https://www.gtlaw.com/en/insights/2019/3/doj-eases-stance-on-use-of-disappearing-message-platforms-in-corporate-enforcement-policy

#Preservation and Spoliation

A. Flottman, "*Seventh Circuit Invokes Carpenter v. United States to Reject Third-Party Doctrine Argument*," Data Security/Privacy (posted Feb. 14, 2019), https://www.ficlaw.com/data-security-privacy/archives/seventh-circuit-invokes-carpenter-v-united-states-to-reject-third-party-doctrine-argument/

#Fourth Amendment – Warrant Required or Not

C.C. Fonzone, *et al.*, "*Carpenter and Everything After: The Supreme Court Nudges the Fourth Amendment into the Information Age*," *58 Infrastructure 4, 3* (ABA: Summer 2019), https://www.sidley.com/-/media/publications/fonzone-et-al-inf_v058n04_summer2019.pdf

#Fourth Amendment – Warrant Required or Not

#Third-Party Doctrine

K.B. Forrest, "*AI and the Confrontation Clause*," N.Y.L.J. (posted May 3, 2019), https://www.law.com/newyorklawjournal/2019/05/03/ai-and-the-confrontation-clause/

#Sixth Amendment – Right of Confrontation

K.B. Forrest, "*AI and the Fourth Amendment: When Alexa Can Be a Witness Against You*," N.Y.L.J. (posted April 17, 2019), https://www.law.com/newyorklawjournal/2019/04/16/artificial-intelligence-and-the-fourth-amendment-when-alexa-can-be-a-witness-against-you/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

K.B. Forrest, "*When AI Speaks, Is It Protected?*" N.Y.L.J. (posted June 3, 2019), https://www.law.com/newyorklawjournal/2019/06/03/when-ai-speaks-is-it-protected/

#Miscellaneous

D.K. Gelb, "*Is the Reverse Location Search Warrant Heading in the Wrong Direction?*" 34 Criminal Justice 2, 68 (ABA: Summer 2019), https://www.americanbar.org/groups/criminal_justice/publications/criminal-justice-magazine/2019/summer/is-reverse-location-search-warrant-heading-wrong-direction/

#Fourth Amendment – Warrant Required or Not

R. Gonzalez, "*How Jamal Khashoggi's Apple Watch Could Solve His Disappearance*," WIRED (posted Oct. 10, 2018), https://www.wired.com/story/jamal-khashoggis-apple-watch-investigation/

#Miscellaneous

V. Graham, "*WhatsApp, Wickr Seen by Justice Dep't as Tools to Erase Evidence*," Bloomberg Law (posted May 16, 2018), https://biglawbusiness.com/whatsapp-wickr-seen-by-justice-dept-as-tools-to-erase-evidence

#Preservation and Spoliation

P.W. Grimm, "*Admissibility of Historical Cell Phone Location Evidence*," 44 *Litigation* 1 (ABA: Summer 2018), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2017-18/summer/admissibility-historical-cell-phone-location-evidence/

#Admissibility

P. Grosdidier, "*Can Authorities Compel a Suspect to Use Biometrics to Unlock a Digital Device?*" 82 Tex. B.J. 840 (Dec. 2019), https://lsc-pagepro.mydigitalpublication.com/publication/?i=635443&article_id=3535029&view=articleBrowser

#Fifth Amendment – Self-Incrimination

N.V. Hardin, "*Uncovering the Secrets of Stingrays: What Every Practitioner Needs to Know*," Criminal Justice 20 (ABA: Winter 2018) (available from the author)

#Discovery Materials

#Miscellaneous

R.J. Hedges, "*What Might Happen After the Demise of the Third-Party Doctrine?*" Criminal Justice 62 (Winter 2018) (available from the author)

#Fourth Amendment – Warrant Required or Not

R.J. Hedges & G.L. Gottehrer, "*The Intersection of the Fourth Amendment and Level 5 Vehicle Autonomy*," 22 TortSource 1, 3 (ABA: Fall 2019), https://www.americanbar.org/groups/tort_trial_insurance_practice/publications/tortsource/2019/fall/the-intersection-the-fourth-amendment-and-level-5-vehicle-autonomy/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

S. Hernandez, "*One of the Biggest At-Home DNA Testing Companies is Working with the FBI*," Buzz Feed News (posted Jan. 31, 2019), https://www.buzzfeednews.com/article/salvadorhernandez/family-tree-dna-fbi-investigative-genealogy-privacy

#Miscellaneous

#Fourth Amendment – Warrant Required or Not

K. Hill, "*Wrongfully Accused by an Algorithm*," N.Y. Times (posted June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html

#Miscellaneous

N.L. Hillman, "*The Use of Artificial Intelligence in Gauging the Risk of Recidivism*," 58 Judges' J. 36 (Winter 2019), https://www.americanbar.org/groups/judicial/publications/judges_journal/2019/winter/the-use-artificial-intelligence-gauging-risk-recidivism/

#Probation and Supervised Release

M. Hvistendahl, "*If You Want to Kill Someone, We Are the Right Guys*," WIRED 72 (May 2019), https://www.wired.com/story/dark-web-bitcoin-murder-cottage-grove/

#Miscellaneous

#Social Media

O. Kerr, "*Fourth Circuit Deepens the Split on Accessing Opened E-Mails*," The Volokh Conspiracy (posted Mar. 21, 2019), https://reason.com/2019/03/21/fourth-circuit-deepens-the-split-on-civi/

#SCA (Stored Communications Act)

O. Kerr, "*Indiana Supreme Court Creates a Clear Split on Compelled Decryption and the Fifth Amendment*," The Volokh Conspiracy (posted: June 24, 2020), https://reason.com/2020/06/24/indiana-supreme-court-creates-a-clear-split-on-compelled-decryption-and-the-fifth-amendment/

#Fifth Amendment – Self-Incrimination

O. Kerr, "*The Law of Compelled Decryption is a Mess: A Dialogue*," The Volokh Conspiracy (posted Aug. 10, 2020), https://reason.com/2020/08/10/the-law-of-compelled-decryption-is-a-mess-a-dialogue/

O. Kerr, "*North Carolina Court Deepens Split on Private Searches of Digital Evidence*," The Volokh Conspiracy (posted Aug. 23, 2019), https://reason.com/2019/08/23/north-carolina-court-deepens-split-on-private-searches-of-digital-evidence/

#Fourth Amendment – Warrant Required or Not

O. Kerr, "*Peffer v. Stephens, on Probable Cause and Home Computer Searches*," The Volokh Conspiracy (posted Jan. 20, 2018), https://reason.com/2018/01/20/peffer-v-stephens-on-probable-cause-and/

#Fourth Amendment – Warrant Required or Not

O. Kerr, "*Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case (Part 1),*" The Volokh Conspiracy (posted Feb. 18, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/18/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-1/?utm_term=.b1c2c93ddfbf

#Miscellaneous

#Fourth Amendment – Warrant Required or Not

O. Kerr, "*Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 2, the All Writs Act,*" The Volokh Conspiracy (posted Feb. 19, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/19/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-2-the-all-writs-act/?utm_term=.d9b17e390dab

#Miscellaneous

O. Kerr, "*Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case: Part 3, the Policy Question*," The Volokh Conspiracy (posted Feb. 24, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/02/24/preliminary-thoughts-on-the-apple-iphone-order-in-the-san-bernardino-case-part-3-the-policy-question/?noredirect=on&utm_term=.1e512de09f72

#International

#Miscellaneous

O. Kerr, "*The Weak Main Argument in Judge Orenstein's Apple Opinion*," The Volokh Conspiracy (posted Mar. 2, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/03/02/the-weak-main-argument-in-judge-orensteins-apple-opinion/?noredirect=on&utm_term=.2e106e329fbc

#Miscellaneous

O. Kerr, "*When Does a Carpenter Search Start – and When Does it Stop?*" Lawfare (posted July 6, 2018), https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop

#Fourth Amendment – Warrant Required or Not

J.R. Kiefer, "*Identifying and Preparing for COVID-19 Compliance Risks*," Dentons (posted May 1, 2020), https://www.dentons.com/en/insights/alerts/2020/may/1/identifying-and-preparing-for-covid-19-compliance-risks

#Miscellaneous

A. Kofman, "*Suspicious Minds: Artificial Intelligence and the Expanding Reach of the Police*," Harper's Magazine 64 (June 2018), https://harpers.org/archive/2018/06/suspicious-minds/

#Miscellaneous

M. Mahtani, "*Police See Social Media Fuel Crime*," Wall St. J. A3 (Nov. 25-26, 2017), https://www.wsj.com/articles/social-media-emerges-as-new-frontier-in-fight-against-violent-crime-1511528400

#Social Media

E.J. McAndrew, "*Welcome Back to America! Now Gimme Your Phone*," 44 Litigation 9 (ABA: Spring 2018), https://www.americanbar.org/groups/litigation/publications/litigation_journal/2017-18/spring/welcome-back-america-now-gimme-your-phone/

#Fourth Amendment – Warrant Required or Not

"*National Lab Keeps Officers One Digital Step Ahead*," Judiciary News (posted June 27, 2018), https://www.uscourts.gov/news/2018/06/27/national-lab-keeps-officers-one-digital-step-ahead

#Discovery Materials

#Preservation and Spoliation

#Miscellaneous

K.M. Nawaday & M.S. Blume, "*The Search of Michael Cohen's Law Offices: Attorney-Client Privilege v. Law Enforcement's Prerogative to Conduct Its Investigation*," Bloomberg Law (posted May 9, 2018), https://news.bloomberglaw.com/white-collar-and-criminal-law/the-search-of-michael-cohens-law-offices-attorney-client-privilege-v-law-enforcements-prerogative-to-conduct-its-investigation-1

#Miscellaneous

P. Ohm, "*The Many Revolutions of Carpenter*," 32 Harvard J. Law & Tech. 357 (Spring 2019), https://jolt.law.harvard.edu/assets/articlePDFs/v32/32HarvJLTech357.pdf

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

J.K. Park, *et al*., "*DOJ Issues Guidance on Cooperation in False Claims Act Investigations*," Compliance and Enforcement (posted May 20, 2019), https://wp.nyu.edu/compliance_enforcement/2019/05/20/doj-issues-guidance-on-cooperation-in-false-claims-act-investigations/

#Miscellaneous

S.K. Pfaffenroth, "*Pricing Algorithms: The Antitrust Implications*" (posted Apr. 17, 2018), https://www.arnoldporter.com/en/perspectives/publications/2018/04/pricing-algorithms-the-antitrust-implications

#Discovery

#Miscellaneous

Press Release, "*Some Aspects of UK Surveillance Regimes Violate Convention*," Registrar of the Court (European Court of Human Rights Press Service: Sept. 13, 2018), https://hudoc.echr.coe.int/app/conversion/pdf?library=ECHR&id=003-6187848-8026299&filename=Big%20%Brother%20Watch%20and%20Others%20v.%20the%20United%20Kingdom%20%20-%20complaints%20about%20surveillance%20regimes.pdf

#International

E. Proudlock, "*Will U.K. Overseas Production Orders Ease Electronic Data Disclosure in International Investigations?* Bloomberg Law (posted Apr. 17, 2019), https://news.bloomberglaw.com/white-collar-and-criminal-law/insight-will-u-k-overseas-production-orders-ease-electronic-data-disclosure-in-international-investigations

#International

M. Puente, "*LAPD Pulls Plug on Another Data-Driven Crime Program*," Government Technology (posted Apr. 15, 2019), https://www.govtech.com/public-safety/LAPD-Pulls-Plug-on-Another-Data-Driven-Crime-Program.html

#Miscellaneous

"*Q&A on the judgment Big Brother Watch and Others v. United Kingdom: Is this the First Time the European Court of Human Rights has Dealt with Provisions on Secret surveillance?*" Press Service (European Court of Human Rights Press Service: Sept. 13, 2018), https://www.echr.coe.int/Documents/Press_Q_A_Brother_Watch_ENG.pdf

#International

R. Ray, *"5 Questions Policymakers Should Ask About Facial Recognition, Law Enforcement, and Algorithmic Bias,"* Brookings (Feb. 20, 2020), https://www.brookings.edu/research/5-questions-policymakers-should-ask-about-facial-recognition-law-enforcement-and-algorithmic-bias/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

W. Ridgway, "*Understanding the CLOUD Act's Expansive Reach*," Skadden (posted Dec. 10, 2018), https://www.skadden.com/insights/publications/2018/12/understanding-the-cloud-acts-expansive-reach

#International

D.G. Robinson, *et al.*, "*Pretrial Risk Assessments: A Practical Guide for Judges*," Judges' J. (posted Aug. 1, 2018), https://www.americanbar.org/groups/judicial/publications/judges_journal/2018/summer/pretrial-risk-assessments-practical-guide-judges/

#Probation and Supervised Release

N. Rodriguez, "*Loomis Look-Back Previews AI Sentencing Fights to Come*," Law360 (posted Dec. 8, 2018), https://www.law360.com/articles/1108727/loomis-look-back-previews-ai-sentencing-fights-to-come

#Probation and Supervised Release

J.A. Sherer, *et al*., "*The CLOUD Act and the Warrant Canaries That (Sometimes) Live There*," (posted Nov. 26, 2018), https://www.discoveryadvocate.com/2018/11/26/the-cloud-act-and-the-warrant-canaries-that-sometimes-live-there/

#International

#Fourth Amendment – Warrant Required or Not

J. Simpson, "*Amazon Echo Data at Center of Another Legal Battle*," (Cozen O'Connor Cyber Law Monitor: Dec. 10, 2018), http://cyberlawmonitor.com/2018/12/10/amazon-echo-data-at-center-of-another-legal-battle/

#Miscellaneous

P.S. Spivack, "*In Fraud and Corruption Investigations, Artificial Intelligence and Data Analytics Save Time and Reduce Client Costs*" (posted June 27, 2018), https://hoganlovells.com/en/publications/in-fraud-and-corruption-investigations-ai-and-data-analytics-save-time-and-reduce-client-costs

#Miscellaneous

N. Suggs, "*DOJ's Newly Released Recommended Practices Are a Win for Cloud and Enterprise Customers*," Microsoft on the Issues (posted Dec. 14, 2017), https://blogs.microsoft.com/on-the-issues/2017/12/14/new-doj-guidelines-win-cloud-enterprise-customers/

#Miscellaneous

#SCA (Stored Communications Act)

J. Tashea, "*Defense Lawyers Want to Peek Behind the Curtain of Probabilistic Genotyping*," ABA J. 18 (Dec. 2017), http://www.abajournal.com/magazine/article/code_of_science_defense_lawyers_want_to_peek_behind_the_curtain_of_probabil/P1

#Admissibility

#Discovery Materials

J. Valentino-DeVries, "*Google's Sensorvault is a Boon for Law Enforcement. This is How It Works*," N.Y. Times A19 (Apr. 14, 2019), https://www.nytimes.com/2019/04/13/technology/google-sensorvault-location-tracking.html

#Miscellaneous

#Fourth Amendment – Warrant Required or Not

J. Valentino-DeVries, "*Hundreds of Apps Can Empower Stalkers to Track Their Victims*," N.Y. Times A1 (May 19, 2018), https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html

#Miscellaneous

J. Valentino-Devries, "*Tracking Phones, Google is a Dragnet for the Police*," N.Y. Times (Apr. 13, 2019) (paywall), https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html?mtrref=www.bing.com&gwh=125E22BE161FA6B8149E42AEEF26FBB9&gwt=pay

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

K. Van Quathem & N. Shepherd, "*European Data Protection Board Issues Opinion on U.S. Cloud Act*," Inside Privacy (Covington: July 23, 2019), https://www.insideprivacy.com/data-privacy/european-data-protection-board-issues-opinion-on-u-s-cloud-act/

#International

#SCA (Stored Communications Act)

J. Vincent, "*FBI Used Instagram, an Etsy Review, and LinkedIn to Identify a Protester Accused of Arson*," The Verge (posted June 18, 2020), https://www.theverge.com/2020/6/18/21295301/philadelphia-protester-arson-identified-social-media-etsy-instagram-linkedin

#Miscellaneous

R.J. Vogt, "*When Algorithms Control Justice, Who Can Check the Math?*" Law360 (posted Apr. 21, 2019), https://www.law360.com/articles/1151573

#Miscellaneous

#Probation and Supervised Release

E. Volokh, "*Criminal Defendant Must Write and Post Essay on Respect for Judiciary, and Delete Negative Comments Posted on that Essay*," The Volokh Conspiracy REASON (Volokh Conspiracy: Dec. 4, 2019), https://reason.com/2019/12/04/criminal-defendant-must-write-and-post-essay-on-respect-for-judiciary-and-delete-any-negative-comments-posted-on-that-essay/

#Miscellaneous

#Social Media

T. Webster, "*How Did the Police Know You Were Near a Crime Scene? Google Told Them*," MPRNEW (posted Feb. 7, 2019), https://www.mprnews.org/story/2019/02/07/google-location-police-search-warrants

#Miscellaneous

#Fourth Amendment – Warrant Required or Not

W. Weinberg, "*Prosecutors Are Required to Give the Defense All Evidence, Including Evidence That May Be Favorable to the Defendant*," California Criminal Defense Lawyer Blog (posted Nov. 16, 2017), https://www.californiacriminaldefenselawyerblog.com/prosecutors-required-give-defense-evidence-including-evidence-may-favorable-defendant/

#Discovery Materials

D.C. Weiss, "*Compelled-Password Decision is 'Death Knell' for Fifth Amendment, State Justice Argues*," ABA J. (posted Mar. 11, 2019), http://www.abajournal.com/news/article/compelled-password-decision-is-death-knell-for-fifth-amendment-massachusetts-justice-argues

#Fifth Amendment – Self-Incrimination

C. Zimmer, "*One Twin Committed the Crime – But Which One? A New DNA Test Can Finger the Culprit*," N.Y. Times (posted Mar. 1, 2019), https://www.nytimes.com/2019/03/01/science/twins-dna-crime-paternity.html

#Miscellaneous

OTHER PUBLICATIONS

"*Algorithms in the Criminal Justice System*," Law Society of England & Wales (Law Society Comm'n on Use of Algorithms in the Justice System: June 2019), https://www.lawsociety.org.uk/support-services/research-trends/algorithm-use-in-the-criminal-justice-system-report/

#International

#Miscellaneous

"*Agreement Between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crimes*" (Oct. 3, 2019), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf

#Miscellaneous

R.J. Conrad, *et al*., "*The Vanishing Criminal Jury Trial: From Trial Judges to Sentencing Judges*," 86 George Washington L. R. 99 (2018), https://www.gwlr.org/wp-content/uploads/2018/04/86-Geo.-Wash.-L.-Rev.-99.pdf

#Trial-Related

"*Criminal Justice: Joint Statement on the Launch of EU-U.S. Negotiations to Facilitate Access to Electronic Evidence*," Press Corner (European Comm'n Sept. 26. 2019), https://ec.europa.eu/commission/presscorner/detail/en/statement_19_5890

#Miscellaneous

"*Dark Side: Secret Origins of Evidence in US Criminal Cases*" (Human Rights Watch: Jan. 9, 2018), https://www.hrw.org/report/2018/01/09/dark-side/secret-origins-evidence-us-criminal-cases

#Fourth Amendment – Warrant Required or Not

#International

#SCA (Stored Communications Act)

#Miscellaneous

L. De Muyter & J. Hladjk, "*Draft EU CLOUD Act—Enabling Law Enforcement Access to Overseas Data*," (posted Apr. 24,2018), https://www.jonesday.com/Draft-EU-CLOUD-Proposal-Enabling-Law-Enforcement-Access-to-Overseas-Data-04-24-2018/

#International

S.L. Dickey, "*The Anomaly of Passenger 'Standing' to Suppress All Evidence Derived from Illegal Vehicle Seizures Under the Exclusionary Rule: Why the Conventional Wisdom of the Lower Courts is Wrong*," 82 Miss. L.J. 183 (2013)

#Fourth Amendment – Warrant Required or Not

C. Doyle, "*Domestic Terrorism: Some Considerations*" (Cong. Research Service: Aug. 12, 2019), https://fas.org/sgp/crs/terror/LSB10340.pdf

#Miscellaneous

C. Doyle, "*False Statements and Perjury: An Overview of Federal Criminal Law*" (Cong. Research Service: May 11, 2018), https://fas.org/sgp/crs/misc/98-808.pdf

#Miscellaneous

A. Dressel & H. Farid, "*The Accuracy, Fairness, and Limits of Predicting Recividism*," 4 *Sci. Adv. 2018 1, eaao5580* (corrected Mar. 30, 2018), https://advances.sciencemag.org/content/4/1/eaao5580.full

#Discovery Materials

#Probation and Supervised Release

A.G. Ferguson, "*Big Data and Predictive Reasonable Suspicion*," 163 U. of Pennsylvania L. R. 327 (2015), https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=9464&context=penn_law_review

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

A.G. Ferguson, "*The Internet of Things and the Fourth Amendment of Effects*," 104 California L. R. 805 (2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2577944

#Fourth Amendment – Warrant Required or Not

K. Finklea, *et al.*, "*Court-Ordered Access to Smart Phones*" (Cong. Research Service: Feb. 26, 2016), https://fas.org/sgp/crs/misc/R44396.pdf

#Miscellaneous

#Fifth Amendment – Self-Incrimination

U. Gasser, *et al.*, "*Don't Panic: Making Progress on the 'Going Dark' Debate*," Berkman Center (Harvard University: Feb. 1, 2016), https://dash.harvard.edu/handle/1/28552576

#Encryption

A.M. Gershowitz, "*The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*," 69 Vanderbilt L. R. 585 (2016), https://scholarship.law.vanderbilt.edu/vlr/vol69/iss3/1/

#Fourth Amendment – Particularity Requirement and/or Overbreadth

#Fourth Amendment – Warrant Required or Not

K.M. Growley, *et al.*, "*Seventh Circuit Wades into Big Data Case Law*," Data Law Insights (posted Mar. 28, 2019), https://www.crowelldatalaw.com/2019/03/seventh-circuit-wades-into-big-data-case-law/

#Fourth Amendment – Warrant Required or Not

#Miscellaneous

K. Hamann, *Police Body-Worn Cameras: What Prosecutors Need to Know* (Prosecutors Center for Excellence: Mar. 1, 2018), https://pceinc.org/police-body-worn-cameras/

#Miscellaneous

#Preservation and Spoliation

K. Hamann & R.R. Brown, "*Secure in Our Convictions: Using New Evidence to Strengthen Prosecution*," (Prosecutors Center for Excellence: Jan. 2015), https://pceinc.org/wp-content/uploads/2016/01/20160123-New-Evidence-in-Prosecutions.pdf

#Admissibility

#Discovery Materials

#Miscellaneous

#Trial-Related

J.C. Hanna, "*Supreme Court Drives Home Its Concern for Privacy in Collins v. Virginia*" (Cong. Research Service Legal Sidebar: June 26, 2018), https://fas.org/sgp/crs/misc/LSB10156.pdf

#Fourth Amendment – Warrant Required or Not

O.S. Kerr, "*Compelled Decryption and the Privilege Against Self-Incrimination*," 97 Tex. L. R. 767 (2019), https://texaslawreview.org/compelled-decryption-and-the-privilege-against-self-incrimination/

#Fifth Amendment – Self-Incrimination

A. Kuehn & B. McConnell, "*Encryption Policy in Democratic Regimes: Finding Convergent Paths and Balanced Solutions*" (EastWest Institute: Feb. 15, 2018), eastwest.ngo/encryption

#Encryption

#International

J. Laperruque (principal drafter), "*Facing the Future of Surveillance*" (The Constitution Project at POGO: Mar. 4, 2019), https://www.pogo.org/report/2019/03/facing-the-future-of-surveillance/

#Fourth Amendment – Warrant Required or Not

#International

#Social Media

W. Maxwell, *et al*., "*Demystifying the U.S. CLOUD Act*" (Hogan Lovells: Jan. 16, 2019), https://www.hlmediacomms.com/2019/01/16/demystifying-the-u-s-cloud-act-assessing-the-laws-compatibility-with-international-norms-and-the-gdpr/

#International

S.P. Mulligan, "*Cross-Border Data Sharing Under the CLOUD Act*" (Cong. Research Service: Apr. 23, 2018), https://fas.org/sgp/crs/misc/R45173.pdf

#International

#SCA (Stored Communications Act)

F. Patel, *et al*., "*Social Media Monitoring: How the Department of Homeland Security Uses Digital Data in the Name of National Security*" (Brennan Center for Justice: May 22, 2019), https://www.brennancenter.org/press-release/government-expands-social-media-surveillance-little-evidence-effectiveness-0

#Fourth Amendment – Warrant Required or Not

#Social Media

Pennsylvania Comm'n on Sentencing, "*Sentence Risk Assessment Instrument*" (eff. July 1, 2020), http://pcs.la.psu.edu/news/guidelines/sentence-risk-assessment-instrument

#Miscellaneous

#Probation and Supervised Release

R. Pfefferkorn, "*The Risks of 'Responsible Encryption'*" (Center for Internet and Society: Feb. 5, 2018), https://cyberlaw.stanford.edu/publications/risks-responsible-encryption

#Encryption

#Fifth Amendment – Self-Incrimination

Pretrial Justice Institute, "*Updated Position on Pretrial Risk Assessment Tools*" (Feb. 7, 2020), https://university.pretrial.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=b417a859-9fe9-2a6c-5e12-3f472d0dc997&forceDialog=0

#Miscellaneous

#Probation and Supervised Release

Probation & Pretrial Services, "*Using Evidence-Based Strategies to Protect Communities*" (posted Aug. 2, 2018), https://www.uscourts.gov/news/2018/08/02/using-evidence-based-strategies-protect-communities

#Probation and Supervised Release

B. Smith, "*A Call for Principle-Based International Agreements to Govern Law Enforcement Access to Data*" (Microsoft on the Issues: Sept. 11, 2018), https://blogs.microsoft.com/on-the-issues/2018/09/11/a-call-for-principle-based-international-agreements-to-govern-law-enforcement-access-to-data/

#International

A. Sumar, "*Prior Restraints and Digital Surveillance: The Constitutionality of Gag Orders Issued Under the Stored Communications Act*," 20 Yale J. L. & Tech. 74 (2018), https://yjolt.org/prior-restraints-and-digital-surveillance-constitutionality-gag-orders-issued-under-stored

#SCA (Stored Communications Act)

R.M. Thompson & C. Jaikaran, "*Encryption: Selected Legal Issues*" (Cong. Research Service: Mar. 6, 2016), https://fas.org/sgp/crs/misc/R44407.pdf

#Encryption

USDOJ, "*Attorney General William P. Barr and FBI Director Christopher Wray Announce Significant Developments in the Investigation of the Naval Air Station Pensacola Shooting*" (Office of Public Affairs: May 18, 2020), https://www.justice.gov/opa/pr/attorney-general-william-p-barr-and-fbi-director-christopher-wray-announce-significant

#Encryption

Cybersecurity Unit, USDOJ, "*Legal Considerations When Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources*" (Version 1.0: Feb. 2020), https://www.justice.gov/criminal-ccips/page/file/1252341/download

#Miscellaneous

USDOJ Office of the Inspector General, "*Management Advisory Memorandum for the Director of the Federal Bureau of Investigation Regarding the Execution of Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons*" (Audit Div. 20-047: Mar. 31, 2020), https://oversight.gov/report/doj/management-advisory-memorandum-director-federal-bureau-investigation-regarding-execution

#Miscellaneous

The US-UK Data Access Agreement: A New Dawn for Transatlantic Criminal Investigations? Crime & Corruption - White Collar Defense & Investigations (posted May 1, 2020), https://cc.cooley.com/2020/05/01/the-us-uk-data-access-agreement-a-new-dawn-for-transatlantic-criminal-investigations/

#Miscellaneous