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

Ronald J. Hedges, Editor

Maverick James, Research Assistant

Maria Ermakova, Research Assistant

December 2017

Table of Contents

FOREWARD

Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials was published in first published in February of 2016. The first edition attempted to be a "comprehensive" collection of representative case law and related materials. Later editions followed that updated the first. This new edition consolidates everything into one compilation and adds additional case law and materials. My intent is to update the new edition on a regular basis.

This edition features links to materials. The links were last visited as this edition was being compiled in December of 2017 and the reader is cautioned that specific links may become stale over time. Anything in the Publications or Articles sections that is not accompanied by a link is behind a paywall.

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 in a time when electronic information is ubiquitous and comes in many shapes and sizes or, put in other terms, in 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 content of criminal investigations and proceedings and figure in the commission, investigation, and prosecution of crimes. Among other things, those

issues often raise questions of how the Constitutions of the United States and the States apply to electronic information. I hope that this compilation can inform any group of actors in the criminal justice system, whether judicial, law enforcement, prosecution, defense, or support, on how these issues might be presented and resolved.

Finally – and in many ways most importantly – I need to recognize and thank those who made these editions possible and available:

Every edition has been posted on the website of the Massachusetts Attorney General's office. I want to thank Tom Ralph, Cameron Evans, and that Office for making the prior and current posting possible.

Not to be forgotten are the research assistants whose names appear on the cover page who worked with me and made this compilation possible: Maverick James and Maria Ermakova, current students of New York Law School and Cardozo School of Law in New York City. I owe you both for your time and commitment. Thanks.

RJH December, 2017

TAGS

#Admissibility

#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

#Fourth Amendment Warrant Required or Not

#Miscellaneous

#Preservation and Spoliation

#Probation and Supervised Release

#Sixth Amendment Assistance of Counsel

#Sixth Amendment Right of Confrontation

#Stored Communications Act" (SCA)

#Social Media

#Third-Party Doctrine #Trial-Related

ABBREVIATION

"Cell Site Location Information" – CSLI

DECISIONS – UNITED STATES SUPREME COURT

Birchfield v. North Dakota, 136 S.Ct. 2160 (2016)

"The cases now before us involve laws that go beyond that [suspension or revocation of a driver's license] and make it a crime for a motorist to refuse to be tested after being lawfully arrested for driving while impaired. The question presented is whether such laws violate the Fourth Amendment's prohibition against unreasonable searches." To answer that question the Supreme Court followed the "same mode of analysis" of *Riley v. California* (*q.v*.) to examine the individual privacy interests implicated by breath and blood tests and the degree to which those tests were needed for legitimate government interests. The Court held that breath tests ("no more demanding than blowing up a party balloon") did not implicate significant privacy interests but that blood tests (which were far more intrusive) did. The Court then held that the laws in issue served a "very important function." The Court concluded that warrantless breath tests were permitted under the Fourth Amendment but that blood tests required search warrants.

#Fourth Amendment Warrant Required or Not

Bullcoming v. New Mexico, 564 U.S. 647 (2011)

The petitioner had been convicted of driving while intoxicated. The principal evidence against him was a "forensic laboratory report certifying that Bullcoming's blood-alcohol concentration was well above the threshold for aggravated DWI." The analyst who signed the certification did not testify at trial. Instead, there was testimony from an analyst "who was familiar with the laboratory's testing procedures, but had neither participated in nor observed the *** test." The New Mexico Supreme Court held that the report was "testimonial" but that the "substitute" testimony did not violate the Confrontation Clause. "The question presented is whether the Confrontation Clause permits the prosecution to introduce a forensic laboratory report containing a testimonial certification – made for the purpose of proving a particular fact – through the in-court testimony of a scientist who did not sign the certification or perform or observe the test reported in the certification. We hold that surrogate testimony of that order does not meet the constitutional requirement. The accused's right is to be confronted with the analyst who made the certification, unless that analyst is unavailable at trial, and the accused had an opportunity, pretrial, to cross-examine that particular scientist."

#Trial Related

Carpenter v. United States, No. 16-402, cert. granted (U.S. June 5, 2017)

The Government obtained disclosure of the historical CSLI of an individual pursuant to an order issued under the SCA rather than by a search warrant. The Sixth Circuit concluded that there was no reasonable expectation of privacy in the CSLI and denied a motion to suppress. The Question Presented on the *certiorari* petition: Whether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment.

#Fourth Amendment Warrant Required or Not

#SCA

#Third-Party Doctrine

***Florida v. Jardines*, 569 U.S. 1 (2013)**

The Supreme Court granted *certiorari* to consider whether police officers had engaged in a "search" under the Fourth Amendment when they took a drug-sniffing dog to the defendant's front porch, the dog "alerted" to the presence of narcotics, the police then secured a warrant, and found marijuana plants inside the defendant's home. The Florida Supreme Court had suppressed the evidence. The Supreme Court affirmed: "That principle [that physical intrusion of a constitutionally protected area is a "search"] renders this case a straightforward one. The officers were gathering information in an area belonging to Jardines and immediately surrounding his house – in the curtilage of the house, which we have held enjoys protection as part of the house itself. And they gathered that information by physically entering and occupying the area to engage in conduct not explicitly or implicitly permitted by the homeowner."

#Fourth Amendment Warrant Required or Not

In re Information Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, In re Two email accounts stored at Google, Inc., No. 17-M-1234, No. 17-M- 2235 (E.D. Wisc. Feb. 21, 2017)

At issue were two warrant applications made by the Government pursuant to the SCA to compel Yahoo and Google to disclose records associated with email accounts no matter where the information was located. One application stated that a person in the United States communicated with an associate outside the country through email sent to and received from the target email address. The other application was intended to further the investigation of already-indicted persons but there was no indication that relevant accounts were used by persons outside the United States. "In neither application does government state that it knows

where the data might be stored, although both state that is possible that some of the information sought might be stored on servers located outside the United States." The question entertained by the court was whether a warrant issued pursuant to the SCA could compel service providers to disclose email held outside the country. The court adopted the reasoning of the opinion dissenting from the denial of *en banc* review in *Microsoft Corp. v. United States* (*q.v.*) and held it was "immaterial where the service provider chooses to store its customer data; what matters in the location of the service provider. Because Google and Yahoo were within the jurisdiction of the court there were no extraterritoriality concerns and the warrants issued.

#SCA

***Maryland v. King,* 569 U.S. 435 (2013)**

The respondent was arrested for assault in 2009. A DNA sample was taken from him through a buccal swab as part of a routing booking procedure. The DNA matched DNA taken from a rape victim in 2003. The respondent was arrested for the rape. The Maryland Court of Appeals reversed the respondent's conviction for rape, ruling that the 2009 DNA was taken as a result of an unlawful seizure. The Supreme Court reversed: "In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks. By contrast, that same context of his arrest gives rise to significant state interests in identifying respondent not only so that "In light of the context of a valid arrest supported by probable cause respondent's expectations of privacy were not offended by the minor intrusion of a brief swab of his cheeks. By contrast, that same context of his arrest gives rise to significant state interests in identifying respondent not only so that the proper name can be attached to his charges but also so that the criminal justice system can make informed decisions concerning pretrial custody. Upon these considerations the Court concludes that DNA identification of arrestees is a reasonable search that can be considered part of a routine booking procedure. When officers make an arrest supported by probable cause to hold for a serious offense and they bring the suspect to the station to be detained in custody, taking and analyzing a cheek swab of the arrestee's DNA is, like fingerprinting and photographing, a legitimate police booking procedure that is reasonable under the Fourth Amendment."

#Fourth Amendment Warrant Required or Not

***Maryland v. Kulbicki*, 136 S. Ct. 2 (2015)**

The defendant shot his mistress in 1993. During his 1995 trial, the State offered expert ballistics testimony. The defendant was convicted of murder. After his petition for postconviction relief

had lingered for years, the Maryland Court of Appeals granted the relief on grounds of ineffective assistance of counsel because the defendant's attorney should have found a 1991 report coauthored by the expert that raised a speculative question about the ballistics evidence. The Supreme Court summarily reversed. Among other things, the Court held that a diligent search would have been unlikely to find the report: "The Court of Appeals offered a single citation in support of its sweeping statement that the report 'was available' in 1995 – a *** Web page accessed by the Court of Appeals, apparently conducting its own Internet research nearly two decades after the trial," that indicated that the report had been distributed to public libraries in 1994. The ballistics evidence was uncontroversial at the time of trial and counsel was not obligated to look "for a needle in a haystack" in "an era of card catalogues, not a worldwide web."

#Miscellaneous

***Microsoft Corp. v. United States*, No. 17-2, cert. granted (U.S. Oct. 16, 2017)**

After the panel decision in this matter, an active circuit judge requested a poll on whether to rehear the case *en banc.* The circuit judges split four-to-four and rehearing was denied. Four judges dissented from the denial, contending that the "focus" of the SCA was disclosure by a service provider to a third party and that no extraterritorial concerns were implicated by disclosure to the Government within the United States.

#SCA

Packingham v. North Carolina, 137 S. Ct. 1730 (2017)

The defendant was a registered sex offender. He was convicted under a North Carolina statute which made it a felony for him to access a commercial Web site which he knew minor children could use after he posted on Facebook a statement about being acquitted of a traffic offense. The Supreme Court reversed the conviction, concluding that the statute failed to survive intermediate scrutiny under the First Amendment. Justice Alito, joined by the Chief Justice and Justice Thomas, concurred but questioned the "undisciplined dicta" of the majority.

#Miscellaneous

#Probation and Supervised Release

#Social Media

Perez v. Florida, 137 S.Ct. 853 (2017), Sotomayor, J., concurring in denial of *certiorari*

The petitioner had been convicted in Florida under a statute which criminalized threats to use a destructive device with the intent to do harm to a person or a person's property. He argued on appeal that the jury instruction "contravene[d] the traditional rule that criminal statutes be interpreted to require proof of *mens rea* ***" because it permitted the jury to find him guilty based solely on what he had "stated." Justice Sotomayor "reluctantly" concurred in the denial of *certiorari* "because the lower courts did not the reach the First Amendment question" but noted that, in an appropriate matter, the Court should declare that the First Amendment required some level of intent beyond mere utterance and also decide what level of intent is required."

#Social Media

#Trial-Related

DECISIONS – FEDERAL

In re Application for Search Warrant, 236 F.Supp.3d 1066 (N.D. Ill. Feb. 16, 2017)

This was a warrant application for seizure of, among other things, electronic storage media and computer equipment at subject premises. The Government demonstrated probable cause to believe that someone has been receiving and trafficking in child pornography using the premises' internet services although the court criticized the application for having a "somewhat dated view of technology." However, the court rejected the application insofar as it sought to compel anyone present at the time of the search to provide fingerprints and/or thumbprints for Apple devices "in order to gain access to the contents." The application was not limited to a particular person or device and there no specific facts as to who was involved in criminal conduct or what device was used in the conduct. The court found that probable cause was not established. The court also raised Fourth Amendment concerns about "forced fingerprinting" because of the "method of obtaining the print" as well as Fifth Amendment self-incrimination concerns. The court noted that its opinion "should not be understood to mean that the government's request for forced fingerprinting will always be problematic."

#Encryption

#Fifth Amendment Self-Incrimination

#Fourth Amendment Warrant Required or Not

In re Application for Search Warrant, Mag. No. 09-320 (D.D.C. June 6, 2009)

The court denied the Government's request for reconsideration. The court had refused to authorize the search of electronic devices. In denying the request, the court affirmed that mere references to use of a computer are insufficient: "Without proof of a consistent use of the computer to communicate or otherwise advance of the conspiratorial scheme, it cannot be said that the computer is being used as an instrumentality of a crime." The court also denied reconsideration of its refusal to allow a search for foreign language documents: "Many Americans (including me) grew up in bilingual homes. That alone cannot be justification to search those homes for documents in a foreign language."

#Fourth Amendment Warrant Required or Not

In re Applications for Search Warrants for Information Associated With Target Email Address, Nos. 12–MJ–8119–DJW, 12–MJ–8191–DJW, 2012 WL 4383917 (D. Kan. Sept. 21, 2012)

The Government applied under the SCA for the issuance of warrants allowing it to obtain and search electronic communications from internet service providers. Adopting the rationale of *Warshak* (*q.v.*) to the applications, that the court held that "an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through" an ISP. The court then founds that the warrants did not satisfy the particularity requirement of the Fourth Amendment because (1) all electronic communications were to be disclosed in their entirety and without any limitation based on the crimes being investigated and (2) no limits were placed on the Government review of the electronic information sought. The court denied the applications without prejudice and suggested that the Government identify "an appropriate procedural safeguard" to limit any search.

#Fourth Amendment Warrant Required or Not

In re Application for Telephone Information Needed for a Criminal Investigation, 119 F.Supp.3d 1011 (N.D. Ca. July 29, 2015)

The Government applied for an order under the SCA for CSLI associated with a number of "target cell phones" for 60 days before and 60 days after issuance of the order. A magistrate judge denied the application, concluding that a search warrant supported by probable cause was required. The district court affirmed. Relying primarily on *United States v. Jones* (*q.v.*), it found that "individuals have an expectation of privacy in the historical CSLI associated with their cell phones, and that such as expectation is one that society is willing to recognize." The court also relied on concessions by the Government that, "over the course of sixty days an

individual will invariably enter constitutionally protected areas, such as private residences", and that "[c]ell phones generate far more location data because, unlike the vehicle in *Jones*, cell phones typically accompany the user wherever she goes." The court also rejected the Government's reliance on the third party doctrine "because the generation of historical CSLI via continually running apps or routine pinging is not a voluntary conveyance by the cell phone user in a way those cases demand."

#Fourth Amendment Warrant Required or Not

Application for Warrant for E-Mail Account, 946 F.Supp.2d 67 (D.D.C. Nov. I, 2010)

A magistrate judge had ordered the Government to notify the subscriber or customer of an e-mail account that a warrant had been issued for its contents. Interpreting the Electronic Communications Privacy Act, the district court reversed. The district court held that the ECPA incorporated the procedural provisions of *Fed. R. Crim. P.* 41, and the rule was satisfied by serving the warrant on the ISP provider.

#Fourth Amendment Warrant Required or Not

In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [redacted], No. BR 13-158 (FISA Ct. Oct. 11, 2013)

The court issued a "Primary Order" pursuant to Section 215 of the USA PATRIOT Act directing certain "Custodians of Records" to produce, "all call records or 'telephony metadata' created by [redacted]," on a continuing basis. In an accompanying Memorandum the court, citing *Smith v. Maryland,* 442 U.S. 735 (1979), held that, "the production of call detail records *** does not constitute a search under the Fourth amendment." The court then discussed the concurring opinions in *United States v. Jones,* 132 S.Ct. 945 (2012), and concluded that, "[t"]he Supreme Court may someday revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not yet arrived."

#Fourth Amendment Warrant Required or Not

I/M/O Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021 (N.D. Ill. Nov. 9, 2015)

"This opinion explains the Court's requirements relating to the use of cell-site simulators in a typical drug-trafficking investigation. To date, the requirements *** have not interfered with effective law enforcement." The requirements focus on the rights of innocent third-parties

whose information is collected by a stimulator: (1) law enforcement must make "reasonable efforts to minimize the capture of signals used by people other than the target of the investigation;" (2) law enforcement must "immediately destroy all data other than the data identifying the cell phone used by the target; and (3) law enforcement are "prohibited from using any data acquired beyond that necessary to determine the cell phone information of the target."

#Fourth Amendment Ex Ante Conditions #Miscellaneous

In re Application of the United States of America for Historical Cell-Site Data, 724 F.3d 600 (5th Cir. 2013)

At issue in this appeal was whether, "court orders authorized by the SCA to compel cell phone service providers to produce historical CSLI of their subscribers are pre se [*sic*] unconstitutional." A magistrate judge had denied three Government applications, concluding that warrantless disclosure violated the Fourth Amendment. The district court affirmed: "The records would show the date, time called, number, and location of the telephone when the call was made. These data are constitutionally protected from this intrusion. The standard under the SCA is below that required by the Constitution." The Court of Appeals reversed. After rejecting various objections to ruling on the merits, the court addressed the merits and analyzed the facts under this "framework:" "cell site information is clearly a business record. The cell service provider collects and stores historical cell site data for its own business purposes, perhaps to monitor or optimize service on its network or to accurately bill its customers for the segments of its network that they use. The Government does not require service providers to record this information or store it. The providers control what they record and how long these records are retained. The Government has neither "required [n]or persuaded" providers to keep historical cell site records. [*United States v.*] *Jones*, 132 S. Ct. at 961 (Alito, J., concurring in the judgment). In the case of such historical cell site information, the Government merely comes in after the fact and asks a provider to turn over records the provider has already created."

With that analysis, the court held that the warrant requirement of the Fourth Amendment was inapplicable: "The statute conforms to existing Supreme Court precedent. This precedent, as it now stands, does not recognize a situation where a conventional order for a third party's voluntarily created business records transforms into a Fourth Amendment search or seizure where the records cover more than some specified time period or shed light on a target's activities in an area traditionally protected from governmental intrusion. We decline to create a new rule to hold that Congress' balancing of privacy and safety is unconstitutional" (footnote omitted).

However, the court cautioned:

“Recognizing that technology is changing rapidly, we decide only the narrow issue before us. Section 2703(d) orders to obtain *historical* cell site information for specified cell phones at the points at which the user places and terminates a call are not categorically unconstitutional. We do not address orders requesting data are from all phones that use a tower during a particular interval, orders requesting cell site information for the recipient of a call from the cell phone specified in the order, or orders requesting location information for the duration of the calls or when the phone is idle (assuming the data are available for these periods). Nor do we address situations where the Government surreptitiously installs spyware on a target’s phone or otherwise hijacks the phone’s GPS, with or without the service provider’s help.”

#Fourth Amendment Warrant Required or Not

In re Application of U.S. for an Order Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283 (4th Cir. 2013)

Sealed access order pursuant to the SCA was entered at pre-grand jury phase of an ongoing criminal investigation to require Twitter to turn over subscriber information to the United States concerning accounts and individuals of interest. Those individuals of interest moved to vacate and to unseal. The magistrate judge denied their motion. The subscribers then filed objections to the magistrate judge's sealing and docketing decisions. The district court overruled their objections and the subscribers petitioned for writ of mandamus. The Court of Appeals held that there was no First Amendment right to access orders issued under 18 U.S.C. Sec. 2703(d) relevant to an ongoing criminal investigation and related to "the unauthorized release of classified documents to WikiLeaks.org" at the pre-jury phase of an ongoing trial. The Court described the 2703(d) process as “investigative, and openness of the orders [that did] not play a significant role in the functioning of investigations.” found that the common law right of access to the 2703(d) order was outweighed by the government’s interest in “preventing potential suspects from being tipped off, or altering behavior to thwart the government’s ongoing investigation.” Further, the Court concluded that the common law presumption of access was outweighed by the government’s interest in continued sealing because the publicity surrounding the Wikileaks investigation.”

#Discovery Materials

#Trial-Related

#Social Media

Belleau v. Wall, 811 F.3d 929 (7th Cir. 2016)

The plaintiff was convicted of various sex offenses involving children and thereafter adjudicated a "sexually violent person." On release from civil commitment a Wisconsin statute required him to wear a GPS monitoring device for the rest of his life. The plaintiff challenged the requirement, contending that the statute violated the Fourth Amendment. (He also challenged the statute on *ex post* facto grounds that is beyond the scope of this digest.). A district judge found the statute unconstitutional. The State appealed and the appellate court reversed: "The 'search' conducted in this case is less intrusive that a conventional search. Such monitoring of sex offenders is permissible if it satisfies the reasonableness test applied in parolee and special-needs cases." The court held that the condition in issue did.

#Miscellaneous

In re Boucher, No. 2:06–mj–91 (D. Vt. Feb. 19, 2009)

A magistrate judge had quashed a grand jury subpoena on the grounds that it violated the defendant's Fifth Amendment right against self- incrimination. In reversing the magistrate judge, the court held requiring the defendant to produce an unencrypted version of a laptop drive would not be a "compelled testimonial communication" as the Government was already aware of the existence and location of the drive and its contents (child pornography). However, the court did bar the Government from using the production to authenticate the drive or the contents.

#Fifth Amendment Self-incrimination

Bill v. Brewer, 799 F.3d 1295, cert. denied (9th Cir. Aug. 31, 2015)

The Phoenix Police Department sought to exclude individuals as contributors of DNA at a crime scene by taking DNA samples from them. Several police officers refused to have samples taken and their DNA was collected only after orders were secured from a State judge. Three of the nonconsenting officers filed a Section 1983 action, alleging that their Fourth Amendment rights had been violated. The district court dismissed the complaint for failing to state a claim. The Court of Appeals affirmed. "[T]he issue before us is whether the defendants 'respected relevant Fourth Amendment standards' in collecting plaintiffs' DNA." The Court of Appeals analyzed the orders and concluded that these satisfied the Warrant Requirement: The orders were issued by a neutral judge, particularly described what was to be seized and searched, and the supporting affidavits demonstrated probable cause to believe that the evidence sought would aid in apprehension or conviction for a specific crime. The Court of Appeals also held that had been

no undue intrusion: “It was hardly unreasonable here to ask sworn officers to provide saliva samples” and there was no danger of potential misuse.

Fourth Amendment Warrant Required or Not

In re Cell Tower Records Under 18 U.S.C. 2703(D), 90 F.Supp.3d 673 (S.D. Tex. Mar. 8, 2015)

This was an application for an order under Section 2703(d) “unusual” in that the targeted account is not specified; neither the phone number nor the identity of the phone’s subscriber or customer are currently known to law enforcement. By obtaining the records of all wireless devices using a nearby tower at the scene of the crime, the Government hopes to identify the particular device used by the suspect and any confederates, and ultimately to enable their capture and arrest.

The court recognized a split of authority on what was sought, a “dump” of cell tower records. Nevertheless, relying on binding Fifth Circuit precedent, it granted the application, concluding the records should be characterized as “ordinary business records entitled to no constitutional protection.” The court also concluded that the SCA contemplated the issuance of a single order for records for multiple accounts. However, it reduced the temporal scope of the application from one hour to ten minutes in issuing the order. Finally, the court admonished that its order had “no application to a related through very different investigative technique using a device known as a cell site simulator, sometimes referred to as a “StingRay.”

#Fourth Amendment Warrant Required or Not

In re the Decryption of a Seized Data Storage System, No. 13-M-449 (E.D. Wisc. May 21, 2013)

Here, the Government renewed its application to compel an individual to decrypt a data storage system so that a search warrant could be executed for its contents. The original application had been denied because there were insufficient facts to demonstrate that the inevitable discovery doctrine applied. On the renewed application, the Government presented evidence that some of the system had been decrypted and that images of child pornography had been found, as well as other images and documents that belonged to the individual. For these reasons, and because the system was found in the defendant’s residence (where he lived alone for 15 years), the court was persuaded that the individual had access to and control over the system, that the act of decryption would not be testimonial, and that the doctrine applied.

#Discovery Materials

Doe v. Shurtleff, 628 F.3d 1217, *cert. denied* (10th Cir. 2010)

In this action, the anonymous plaintiff had been convicted of sex offenses involving a minor in a United States military court. The plaintiff challenged in the District Court a Utah statute that required him, as a resident and convicted sex offender, to provide to the Utah Department of Corrections, among other things, all "Internet identifiers." After the District Court found that the statute had no restrictions on the dissemination of information and held it unconstitutional as an infringement of the plaintiff's First Amendment right to anonymous speech, Utah amended the statute. The District Court then granted a Rule 60(b) motion and upheld the statute. On appeal, the Court of Appeals affirmed (and denied a motion for panel rehearing and rehearing *en banc*). The Court of Appeals concluded, among other things, that the amended statute was "content-neutral" and did *not* require strict scrutiny, that the statute did *not* allow unrestricted dissemination to the general public, and that the plaintiff did not have a reasonable expectation of privacy in his "online identifiers."

#Fourth Amendment Warrant Required or Not

E.E.O.C. v. Burlington Northern Santa Fe R.R., 669 F.3d 1154 (10th Cir. 2012)

This case involved two job candidates were not hired by the defendant company after receiving conditional offers of employment and a medical screening procedure. The job candidates filed EEOC charges, claiming they were being discriminated against in violation of the Americans with Disabilities Act. As part of its investigation, the EEOC issued a letter to the defendant requesting "any computerized or machine-readable files ... created or maintained by you . . . that contain electronic data or effecting [sic] current and/or former employees ...throughout the United States." The defendant objected to the request. The EEOC then served a subpoena and indicated in a letter to the defendant that it was broadening its investigation to include "pattern and practice discrimination," thus warranting the demand for nationwide information. After the defendant again refused to provide the information, the EEOC filed an enforcement action. The district court discharged the EEOC's show cause order and sustained BNSF's refusal to comply with the subpoena. On appeal, the Tenth Circuit noted that the EEOC may access "'any evidence of any person being investigated' so long as that evidence 'relates to unlawful employment practices ... and is relevant to the charge under investigation.'" The Tenth Circuit emphasized, however that the information demanded in the EEOC's subpoena went far beyond the allegations in the underlying charge and that enforcing it may "render null the statutory requirement that the investigation be relevant to the charge." In ruling against the EEOC's efforts to give their investigation a national scope, the Court also stated that "nationwide

recordkeeping data" was not relevant to individual discrimination claims "filed by two men who applied for the same type of job in the same state."

#Discovery Materials

E.E.O.C. v. Kronos Inc., 694 F.3d 351 (3d Cir. 2012), as amended (Nov. 15, 2012)

For the second time in this case, the Third Circuit addressed the enforcement of an administrative subpoena issued by the EEOC seeking to compel Kronos Incorporated ("Kronos"), a non-party to the underlying action, to disclose information about its employment tests. The EEOC issued the disputed subpoena as part of its investigation into an allegation that a grocery store violated the ADA by failing to hire a disabled applicant after she took an employment test created by Kronos. The Third Circuit previously held that the EEOC was entitled to Kronos's data without the geographic, temporal, and topical restrictions originally imposed by the district court, except for discovery regarding racial discrimination. Kronos appealed and the Third Circuit remanded for the district court to conduct a good cause balancing test to determine if a confidentiality order was warranted. On remand, the district court expanded the scope of its original order, but again placed certain limitations on the disclosure of information related to the Kronos tests. Regarding Kronos's request for a confidentiality order, the court found there was good cause to enter a modified version of the order previously reviewed by the Third Circuit. The district court also required Kronos and the EEOC to split evenly the costs of production. The Third Circuit remanded "solely for the purpose of allowing the district court to consider how the specific limitations it ordered are tied to Kronos's justifiable fears regarding the disclosure of proprietary information." The Third Circuit also specified that it was "reversing the district court's cost-sharing order not because we necessarily disagree with the result, but to allow the court to make an individualized determination of whether the costs of production under the newly expanded subpoena are outside the scope of what Kronos can reasonably expect to bear as the cost of doing business."

#Discovery Materials

Free Speech Coalition, Inc. v. Attorney General, 825 F.3d 149 (3d Cir. 2016)

Two recent Supreme Court cases requires a renewed analysis of two previous holdings by this court: *Reed v. Town of Gilbert*, 135 S. Ct. 2218 (2015), and *City of Los Angeles v. Patel*, 135 S. Ct. 2443 (2015). Under *Reed*, only if a law is content neutral on its face may the court begin to look at any benign purpose. Thus, strict scrutiny applies since the statutes restrictions, "depend entirely on the communicative content" of the speech. Under *Patel*, the court reasoned that

the need for warrantless searches is most clear when the element of surprise would both help detect and deter violations.

#Miscellaneous

Gilman v. Marsh & McLennan Cos. Inc., 654 F. App'x 16 (2d Cir. 2016)

The court concluded that the interview demands of two former employees were reasonable as a matter of law because at the time they were made, the employees were Marsh employees who had been implicated in an alleged criminal conspiracy for acts that were within the scope of employment and that imperiled the company. The court also found that there are no triable issues of facts as to whether Marsh fired the employees for cause.

#Discovery Materials #Trial Related

Grady v. North Carolina, 135 S. Ct. 1368 (2015) (per curiam)

The petitioner, a convicted sex offender, was ordered to enroll in a lifelong satellite-based monitoring system. He challenged the order, arguing that it violated his Fourth Amendment right to be free from unreasonable searches and seizures. The Supreme Court held:

The State's program is plainly designed to obtain information. And since it does so by physically intruding on a subject's body, it effects a Fourth Amendment search.

That conclusion, however, does not decide the ultimate question of the program's constitutionality. The Fourth Amendment prohibits only *unreasonable* searches. The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations. ***. The North Carolina courts did not examine whether the State's monitoring program is reasonable – when properly viewed as a search – and we will not do so in the first instance.

The court remanded for further proceedings.

#Fourth Amendment Warrant Required or Not

In re Grand Jury Empanelled on May 9, 2014, 786 F.3d 255 (3d Cir. 2015)

An anonymous corporation had been held in contempt for refusing to comply with a grand jury subpoena served on its custodian of record, identified as "John Doe," the sole owner and

employee of the corporation. He argued on appeal that compliance with the subpoena would violate his Fifth Amendment privilege against self-incrimination. The Court of Appeals affirmed. Doe relied on the "act of production doctrine," which recognizes that an individual can refuse to comply when doing so would reveal something "testimonial" that might be used against him. However, the subpoena was not directed to Doe as an individual but to him as the corporate custodian. This implicated the "collective entity doctrine," which provides that an individual cannot rely on the Fifth Amendment to avoid production of corporate records because he would be acting in a representative rather than an individual capacity.

#Fifth Amendment Self-incrimination

In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011, 670 F.3d 1335 (11th Cir. 2012)

John Doe was subpoenaed to before a grand jury investigating child pornography and to produce the unencrypted contents of hard drives. Doe was given immunity for the act of production but not for the Government's use of any content. Doe refused to decrypt the hard drives and was held in contempt. The Court of Appeals reversed on Fifth Amendment self-incrimination grounds. Distinguishing *Boucher* (*q.v.*), it held that, although the contents were not testimonial in nature, "decryption and production would be tantamount to testimony by Doe of his knowledge of the existence and location of potentially incriminating files." The court also held that Doe could have been compelled to turn over the unencrypted contents if it had given him appropriate immunity.

#Fifth Amendment Self-incrimination

In re: Grand Jury Subpoena to Facebook, 16-MC-1300 (JO) through 16-MC-1314 (JO) (E.D.N.Y. May 12, 2016)

The government submitted fifteen separate "boilerplate" applications for an order that would prohibit the recipients of subpoenas, service providers such as Facebook, not to disclose the existence of the subpoena. The SCA provides for the entry of such orders if the court determines that "there is reason to believe that notification" will result in a specified harm. The judge found that none of the applications make the showing required by the Act and denied the applications without prejudice.

#Miscellaneous

#Social Media

In re Grand Jury Subpoenas, 627 F.3d 1143, cert. denied (9th Cir. 2010)

The United States appealed from an order quashing subpoenas on the respondent law firms. The subpoenas, issued under Fed. R. Crim. P. 17(c), sought nonprivileged materials in aid of a grand jury investigation of the firms' clients. The materials had been obtained by the firms through discovery in a private antitrust action. The Court of Appeals reversed, holding that the District Court had abused its discretion. There was no proof of "collusion between the civil suitors and the government" and the Government had not engaged in any bad faith tactics. "By a chance of litigation, the documents [in issue] had been moved from outside the grasp of the grand jury to within its grasp. No authority forbids the government from closing its grip on what lies within the jurisdiction of the grand jury."

#Discovery Materials

Hart v. Mannina, 798 F.3d 578 (7th Cir. Aug. 17, 2015)

This was a Section 1983 action brought against detectives and the Indianapolis Metropolitan Police Department. The police allowed a film crew from a TV program to follow them in the investigation of a home invasion. The plaintiff was arrested and spent nearly two years in prison awaiting trial for crimes he did not commit. The plaintiff contended that he was arrested without probable cause and that false and misleading statements were made against him. Summary judgment was granted in favor of the defendants. On appeal, the plaintiff argued, among other things, that evidence had been spoliated because raw video footage of interviews conducted by the police that had been taken by the TV program had been destroyed. The Court of Appeals rejected this argument. "A police officer's duty to preserve evidence applies when the officer knows the evidence is exculpatory or destroys the evidence in bad faith." However, there was no evidence that the lost footage was exculpatory to the plaintiff or destroyed in bad faith.

#Preservation & Spoliation

House v. Napolitano, No. 11–10852–DJC (D. Mass. Mar. 28, 2012)

In this Section 1983 action, the plaintiff, who alleged that he had been targeted for supporting Bradley Manning, arrived at a Chicago airport from a vacation in Mexico, where his electronic devices were searched and seized for 59 days. He alleged that the search and prolonged seizure violated his First and Fourth Amendment rights. In ruling on a motion to dismiss by the

Government defendants, the court held that the search and seizure at the functional equivalent of a border crossing was not sufficiently intrusive to trigger a need to show some level of suspicion. The court denied the motion as to the length of the seizure, finding reasonableness to be in dispute. The court also denied the motion on the First Amendment claim, rejecting the argument that its ruling on the search and seizure foreclosed an associational claim. Finally, the court declined to rule on the plaintiff's request for the issuance of an injunction to require the defendants to disclose who they had disclosed or disseminated ESI to.

#Fourth Amendment Exigent Circumstances

Huff v. Spaw, 794 F.3d 543 (6th Cir. 2015)

This was a Title III action brought against a defendant for intentional interception of oral communications involving the husband and wife plaintiffs. The husband inadvertently placed a "pocket-dial call" to the defendant, who remained on the line for 91 minutes, transcribed what she heard, and used an iPhone to record a portion of the conversations. The district court granted summary judgment, holding that the plaintiffs had no reasonable expectation of privacy. The Court of Appeals affirmed in part. Applying the "reasonable expectation of privacy test" of *Katz v. United States,* 389 U.S. 347 (1967) (Harlan, J., concurring), the court held that the husband, who made the pocket-dial call to the defendant, "exposed his statements to her and therefore failed to exhibit an expectation of privacy with regard to those statements." He was aware of the risk of making such calls and took no precautions against doing so. "Huff is no different from the person who exposes in-home activities by leaving drapes open or a webcam on and therefore has not exhibited an expectation of privacy." However, the Court of Appeals reversed and remanded as to the plaintiff wife because since she "made statements in the privacy of her hotel room, was not responsible for exposing those statements to an outside audience, and was *** unaware of the exposure, she exhibited an expectation of privacy."

#Miscellaneous

In re Information Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, In re Two email accounts stored at Google, Inc., No. 17-M-1234, No. 17-M- 2235 (E.D. Wisc. Feb. 21, 2017)

At issue were two warrant applications made by the Government pursuant to the SCA to compel Yahoo and Google to disclose records associated with email accounts no matter where the information was located. One application stated that a person in the United States communicated with an associate outside the country through email sent to and received from the target email address. The other application was intended to further the investigation of

already-indicted persons but there was no indication that relevant accounts were used by persons outside the United States. "In neither application does government state that it knows where the data might be stored, although both state that is possible that some of the information sought might be stored on servers located outside the United States." The question entertained by the court was whether a warrant issued pursuant to the SCA could compel service providers to disclose email held outside the country. The court adopted the reasoning of the opinion dissenting from the denial of *en banc* review in *Microsoft Corp. v. United States* (*q.v.*) and held it was "immaterial where the service provider chooses to store its customer data; what matters in the location of the service provider. Because Google and Yahoo were within the jurisdiction of the court there were no extraterritoriality concerns and the warrants issued.

#SCA

***Kelly v. Rogers*, No. 1:07–cv–1573 (M.D. Pa. June 13, 2012) [Affirmed, *Kelly v. Borough of Carlisle,* 544 Fed.Appx. 129 (3rd Cir. 2013)]**

In this Section 1983 action, the plaintiff recorded the defendant police officer at a traffic stop. The plaintiff was arrested for violation of a Pennsylvania wiretap law. After appeal and trial on discrete factual questions, the court held that the defendant was entitled to qualified immunity for the arrest based on erroneous advice given to him by a prosecutor but that the defendant had no reasonable basis to seize the recording device.

#Miscellaneous

***Lane v. Anderson*, 660 F. App'x 185 (4th Cir. 2016)**

The Fourth Circuit concluded that a Sheriff was not entitled to qualified immunity after firing a police officer for making statements against the department. The court determined that the First Amendment protected the police officer's speech on the basis that he spoke out on a matter of public concern when he discussed the potential police misconduct to the media.

#Miscellaneous

***Luis v. Zang,* 833 F.3d 619 (6th Cir. 2016)**

Defendant filed suit against Awareness the manufacturer of a WebWatcher alleging violations of the federal Wiretap Act, 18 U.S.C. 2511-2512, the Ohio Wiretap Act, and Ohio common law. The Sixth Circuit reversed the lower court's dismissal stating that it failed to take into account

the extent to which Awareness itself was allegedly engaged in the asserted violations, noting Awareness's continued operation of the WebWatcher program, even after that program is sold to a user.

#Trial Related

In re Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016)

A magistrate judge denied an application brought under the SCA to search three email accounts based on his findings that the it failed to show probable cause and to satisfy the Particularity Requirement of the Fourth Amendment. He suggested that the application be renewed with the addition of search protocols and other *ex ante* conditions. The government sought review. The district judge declined to rule on the reasonableness of the magistrate judge's suggestions but concluded, among other things, that the application met the Particularity Requirement because it identified the target accounts and the evidence to be seized. However, the district judge agreed with the magistrate judge that the application failed to establish probable cause "to support a connection between the investigation and four of the individuals/identifiers listed in the warrant." The district judge declined to consider a new warrant application but noted that the government could resubmit an application to a magistrate judge.

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

Microsoft Corp. v. United States Dept. of Justice, 233 F. Supp. 3d 887 (W.D. Wash. Feb. 8, 2017)

This is a First Amendment challenge to orders issued under Section 2705(b) of the SCA which delay Microsoft from providing notice to subscribers of its services that the Government has obtained information from them. Microsoft alleged that these "gag orders" violate its right to free speech. The Government moved to dismiss pursuant to *Fed. R. Civ. P.* 12(b)(1) and (6). The court held that Microsoft had standing and that the gag orders, "which indefinitely prevent Microsoft from speaking out about government investigations," impeded Microsoft's First Amendment rights. However, the court dismissed Microsoft's Fourth Amendment claims because Microsoft could not assert the Fourth Amendment rights of its subscribers.

#Miscellaneous

Miller v. Mitchell, 598 F.3d 139 (3d Cir. 2010)

The Court of Appeals affirmed the entry of a preliminary injunction against a district attorney. The district attorney had threatened prosecution of minors for "sexting" unless they attended an education program. The court held that plaintiffs (a minor and her mother) were engaged in constitutionally protected activity, that the threatened prosecution was retaliatory, and that there was a causal relationship between the two.

#Miscellaneous

In re National Security Letter, 863 F.3d 1110 (9th Cir. 2017)

A national security letter (NSL) is an administrative subpoena authorized by statute and issued by the FBI to an electronic communication service provider which requires the provider to turn over specified subscriber information relevant to an authorized national security investigation. The NSL may include a provision that bars the provider from disclosing that the FBI sought or obtained access to information under the authorizing statute. Recipients of NSLs challenged the nondisclosure provision, arguing that it violated their First Amendment rights. The Court of Appeals held that the nondisclosure provision was content-based and subject to strict scrutiny. The court then held that the provision survived strict scrutiny because it was narrowly-tailored, procedures were in place to limit duration of NSLs, and judicial review was available to ensure that the provision remained in place only as long as necessary.

#Miscellaneous

In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, No. 15MISC1902, (E.D.N.Y. Oct. 9, 2015) [Subsequent Determination, In re Apple Inc., 149 F.Supp.3d 341 (E.D.N.Y. 2016)]

The Government sought an order compelling Apple to assist in the execution of a search warrant by disabling the security of an Apple device lawfully seized pursuant to a search warrant. The Government "discovered the device to be locked, and have tried and failed to bypass that lock." The court questioned whether the relief sought was authorized by the Act. However, it deferred ruling to afford Apple an opportunity to address the question of burdensomeness of any order and the Government to respond. After the matter was briefed the defendant pled guilty. By letter dated October 29, 2015, the Government advised the Court that it "persists in the application."

#Miscellaneous

In re Order Requiring Apple, Inc., to Assist in the Execution of a Search Warrant, No. 15-MC-1902 (JO) (E.D.N.Y. Apr. 22, 2016) OR In re Apple, Inc., 149 F. Supp. 3d 341 (E.D.N.Y. 2016

This letter advised the court that, "an individual provided the passcode to the iPhone in issue in this case. Late last night, the government used that passcode by hand and gained access to the iPhone. Accordingly, the government no longer needs Apple's assistance to unlock the iPhone, and withdraws its application."

#Miscellaneous

In re Order Requiring Apple, Inc. to Assist in the Execution of a Search Warrant Issued by this Court, Case No. 16-mj-02007-MBB (D. Mass. Feb. 1, 2016)

This order, issued pursuant to the All Writs Act, compelled Apple to "assist law enforcement agents in enabling the search of a digital device seized in the course of a previously issued search warrant in this matter." The order also provided that, "to the extent that data on the Device is encrypted, Apple may provide a copy of the encrypted data *** but Apple is not required to attempt to decrypt, or otherwise enable *** attempts to access any encrypted data." Moreover, Apple was not "required to maintain copies of any user data as a result of the assistance ordered herein; all evidence preservation shall remain the responsibility of law enforcement agents."

#Miscellaneous

Owner-Operator Indep. Drivers Ass'n v. United States Department of Transportation, 840 F. 3d 879 (7th Cir. 2016), cert. denied, 137 S. Ct. 2246 (2017)

The Federal Motor Carrier Safety Administration, in 2015 required ELDs (electronic logging devices) in all motor commercial vehicles to automatically record data relevant to engine run time and vehicle location to lessen fatigue related accidents. The Owner Operator Independent Drivers Association filed suit arguing that the regulation does not advance safety, is arbitrary and capricious and violates Fourth Amendment protections against unreasonable searches and seizures The court found no Fourth Amendment violation reasoning that if the rule itself imposes a search or a seizure, inspection of data recorded on an ELD would fall within the

"pervasively regulated industry" exception to the warrant requirement.

#Fourth Amendment Search Required or Not

Patel v. City of Los Angeles, 738 F.3d1058 (9th Cir. Dec. 24, 2013) (*en banc*) [Affirmed, *City of Los Angeles v. Patel*, 135 S.Ct. 2443 (2015)]

The Los Angeles municipal code requires that hotel and motel owners maintain detailed records on their guests. The appellant motel owners brought a facial challenge to a code provision that authorized, "warrantless, on-site inspections of those records upon the demand of any police officer." The district court dismissed the complaint for declaratory and injunctive relief. The Ninth Circuit, sitting *en banc,* reversed and remanded. The court reasoned: (1) "Records inspections *** involve both a physical intrusion upon a hotel's papers and an invasion of the hotel's privacy interests in those papers" and constitute a "search" under the Fourth Amendment, (2) based on assumptions about the intent of the challenged provision, the court applied, "the Fourth Amendment principles governing administrative record inspections, rather than those that apply when the government searches for evidence of a crime or conducts administrative searches of a non-public areas of a business," and (3), the provision was facially invalid because it authorized, "inspection *** without affording an opportunity to 'obtain judicial review of the reasonableness of the demand prior to suffering penalties for refusing to comply'" (citation omitted).

#Fourth Amendment Warrant Required or Not

Pierce v. Emmi, No. 16-11499 (E.D. August 23, 2017)

The plaintiff in this civil rights action alleged that the defendant, a sheriff's officer who led a search that resulted in the arrest of her fiancé and the seizure of his cell phone, viewed the plaintiff breastfeeding her infant through an application on the phone. A magistrate judge ordered, among other things, that the phone be produced for inspection by the plaintiff's expert and that a representative of the sheriff's office be permitted to attend. The district court modified the order to require the office to secure a warrant or the consent of the fiancé. Otherwise, anything learned by the representative might be obtained in violation of the Fourth Amendment rights of the fiancé.

#Fourth Amendment Warrant Required or Not

Rann v. Atchison, 689 F.3d 832, cert. denied (7th Cir. 2012)

The petitioner was convicted for criminal sexual assault and child pornography in Illinois. After

exhausting State remedies, he sought *habeas* relief, alleging ineffective assistance of counsel because his attorney did not seek suppression of images on digital storage devices secured without a search warrant. The district court denied the petition and the Court of Appeals affirmed. The devices had been delivered to law enforcement by the victim and her mother. They knew what images were on the devices. The subsequent search of the contents by law enforcement did not violate the respondent's Fourth Amendment right and, accordingly, his ineffective assistance of counsel claim could not prevail.

#Fourth Amendment Warrant Required or Not

***Sams v. Yahoo Inc.,* 713 F.3d 1175 (9th Cir. 2013)**

The plaintiff filed a putative class action against the defendant, alleging that its disclosure of noncontent subscriber information in response to grand jury subpoenas violated the SCA. The district court granted the defendant's motion to dismiss, concluding that the defendant was statutorily immune from suit. Affirming the district court, the Court of Appeals held that the test of "good faith reliance" under the SCA contained both an objective and subjective element. No facts were pled to give rise to a plausible inference that the defendant knew that the subpoenas were invalid and the defendant's production was objectively reasonable as the subpoenas appeared to be lawful.

The Court of Appeals also rejected the argument that liability could attach because documents had been produced before the return date of the subpoenas: "The principle Sams would apparently have us adopt would, among other things, outlaw the negotiated resolution of discovery disputes, and related cooperation among counsel to minimize inconcenience and costs to the parties."

#Fourth Amendment Good Faith Exception

***Schlossberg v. Solesbee*, 844 F. Supp. 2d 1165 (D. Or. 2012)**

Police officer defendant conducted a warrantless search of plaintiff's digital camera incident to his arrest. Plaintiff filed § 1983 claim against defendant. The court found that the warrantless search violated the Fourth Amendment. The court found that because a large volume of personal data can be stored on modern mobile devices entitling, such devices were entitled to a higher standard of privacy. The court rejected the rationale of previous cases that held electronic devices were like "closed containers" subject to warrantless searches. Thus, absent exigent circumstances, the court held that an officer was required to obtain a warrant to search any electronic device found on a suspect. Plaintiff's motion for summary granted was granted.

#Fourth Amendment Warrant Required or Not

In re Sealed Case, 717 F.3d 968 (D.C. Cir. 2013)

(PER CURIAM)

Government agents executed search warrants as part of a grand jury investigation. After the parties failed to reach agreement as to which seized documents could be reviewed without exceeding the scope of the warrants or breaching attorney-client privilege, motions were made pursuant to Criminal Rule 41(g) to return "any documents the government lacked authority to review." The district court denied the motions and the moving parties appealed. Addressing the only issue that was not moot – the refusal of the district court to order the parties to implement protocols to identify documents beyond the scope of the warrants – the Court of Appeals concluded that it lacked jurisdiction because there was no finality. The Court of Appeals also held that the order here was not appealable under the *Perlman* doctrine.

[Note that this decision is heavily redacted].

#Fourth Amendment Particularity Requirement

I/M/O Search of an Apple iPhone Seized During the Execution of a Search Warrant on a Black Lexus IS300, California License Plate #5KGD203, No. 16-cm-00010-SP (C.D. Ca. March 28, 2016)

In this status report, the government advised the court that it "has now successfully accessed the data stored on Farook's iPhone and no longer requires the assistance from Apple, Inc." required by an order and requested that the order be vacated.

#Miscellanous

I/M/O Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263-LB (N.D. Ca. Apr. 25, 2017)

The Government secured a warrant under the SCA requiring Google to produce the stored content of certain email accounts. Relying on *Microsoft Corp.,* (*q.v.*), Google moved to quash, arguing that the information was stored outside the United States and beyond the reach of the Act. The court distinguished *Microsoft*: "Unlike *Microsoft*, where storage of information was tethered to a user's reported location ***, there is no storage decision here. The process of distributing information is automatic, via an algorithm, and in aid of network efficiency." The

court denied the motion, concluding that the warrant was directed to Google "in the only place where it can access and deliver the information that the government seeks."

#SCA

In re Search of Electronic Communications (Both Sent and Received) in the Account of Chakafattah@gmail.com at Internet Service Provider Google, Inc., 802 F.3d 516 (3d Cir. 2015)

The appellant is a sitting Congressman subject to a grand jury investigation. He was advised by Google that it had received a warrant that authorized the FBI to search his personal email account. His motion to quash was denied by a district judge. The Court of Appeals affirmed. The court concluded that it lacked appellate jurisdiction under either the collateral order or the *Perlman* doctrines. The court also held that *Fed. R. Crim. P.* 41(g) did not confer jurisdiction: "Denial of a pre- indictment *** motion is immediately appealable, only if the motion is[] (1) solely for the return of property and (2) is in no way tied to an existing criminal prosecution against the movant."

#Miscellaneous

In re Search of Google Email Accounts, 99 F.Supp.3d 992 (D. Alaska Apr. 13, 2015)

The Government secured a search warrant compelling Google to produce specified content of six Gmail accounts over a limited time period. Google declined to comply, arguing that it should not be required to perform a search for the content sought. The Government then applied for a second warrant for all content, which was rejected as overbroad as it went beyond the time period of the first warrant. Google moved for relief from the first warrant. The court granted the relief sought and issued an *ex ante* order that "relieve[s] Google of any obligation to inspect content ***, while also providing the government with full access to the content *** for which its application establishes probable cause."

#Fourth Amendment Ex Ante Conditions

#Miscellaneous

I/M/O Search of Information Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH) (D.D.C. June 2, 2017)

"[A]s a matter of first impression in this circuit, the undersigned must now resolve whether this Court will follow the Second Circuit's decision in *Microsoft* [*q.v.*]." The Government had secured a warrant under the SCA compelling Google to produce all information associated with an email account that the Government believed was used by the subject of a criminal investigation. Relying on *Microsoft*, Google refused to provide information stored on servers outside the United States and the Government moved to compel. The information in issue was broken down into component parts stored on servers located throughout the world and the components automatically moved across servers to optimize Google's data network. The components were "effectively meaningless on their own—for purposes of an SCA warrant, a recognizable file useful to law enforcement may exist only when its component parts are compiled remotely from within Google's California headquarters and then produced to the government pursuant to a warrant." Engaging in a detailed analysis of the governing law, the court held that the "most relevant conduct *** is not the provider's *accessing* customer data, but rather its *disclosure* of that data to law enforcement." Since the components in issue could be accessed, compiled, and produced in the United States there would be no prohibited extraterritorial application of the Act. The court ordered Google to comply in full with the warrant.

#SCA

I/M/O Search of Info. Associated with E-Mail Addresses Stored at Premises Controlled by Microsoft Corp., 212 F. Supp. 3d 1023 (D. Kan. 2016)

The government submitted to a magistrate judge an application for a search warrant to search three email accounts. The government suspected that these email accounts were being used to further criminal activity. The magistrate judge issued an order denying the application. On appeal, the Court argued that courts need to ensure that search warrants seeking ESI are sufficiently particular so that officers executing a warrant do not exceed their scope and perform a "general rummaging" of a person's private information. The court found that the warrant in this case was sufficiently particular under the Fourth Amendment.

#Fourth Amendment Particularity Requirement

I/M/O Search of Information Associated with Fifteen Email Addresses Stored at Premises Owned, Maintained, Controlled or Operated by 1 & 1 Media, Inc., Google, Inc., Microsoft Corp., and Yahoo! Inc., Case No. 17-cm-03152-WC (M.D. Ala. September 28, 2017)

This order addressed fifteen separate applications for search warrants related to a federal investigation of alleged identity theft and related fraudulent tax practices. The court denied the applications, finding that the warrants would require disclosure of "essentially all data *** without limitation as to time" in the accounts and observing that the applications included "no protocol requiring the destruction, discarding, return, or quarantining of data that the Government does not 'seize.'" The court held that the lack of temporal limitation would result in unconstitutional general warrants. Moreover, the court expressed concern about the "lack of any protocol for the Government's handling of non-pertinent information that the Government would compel *** to disclose but that it ostensibly would not 'seize.'" The court did observe that the defects in the applications could be "either easily avoided or remediated."

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Particularity Requirement

In re the Search of Motorola Cellular Telephone, Mag. Nos. 09-m-652 through 09-653 (D.D.C. Dec. 7, 2d009)

The Government sought the issuance of search warrants for two seized cell phones. Noting the ability of cell phones to hold vast amounts of data, that the supporting applications did not specify what information the Government sought, and that no limitations on the searches were proposed, the court found that a "general search" was being requested. The court denied the application.

#Fourth Amendment Particularity Requirement

In re Search of premises known as Three Cellphones & One Micro-SD Card, No. L4-MJ-8013-DJW (D. Kan. Aug. 4, 2014)

The Government submitted a search warrant application for information stored on various devices. The court denied the application because the Government did not propose a search methodology. Relying on earlier decisions, including *Riley v. California,* the court explained that "an explanation of the government's search techniques is being required in order to determine whether the government is executing its search in good faith and in compliance with the probable cause and particularity requirements of the Fourth Amendment. And a protocol is not required to accompany every type of search. It is only because of the substantial differences in the search of large amounts of electronically stored information[] that the Supreme Court discussed in *Riley,* that a search protocol is being requested."

#Fourth Amendment Particularity Requirement

#Fourth Amendment Ex Ante Conditions

***In re Search Warrant Application*, No. 17 M 85 (N.D. Ill. Sep. 18, 2017)**

The Government sought review of the magistrate judge's "denial of one aspect of the government's search-warrant application: authorization to require the four residents of a home to apply their fingers and thumbs (as chosen by government agents) to the fingerprint sensor on any Apple-made devices found at the home during the search." The District Court held that the fingerprint seizure of the four residents did not violate the privilege against self-incrimination of the Fifth Amendment. "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." "The government chooses the finger to apply to the sensor, and thus obtains the physical characteristic—all without need for the person to put any thought at all into the seizure." Moreover, "the fingerprint seizure itself does not reveal the contents of the person's mind in the way that disclosure of a passcode would or in the way that disclosure of a cryptography key would." Finally, *Riley v California* was not controlling: "the interpretive task is to decide whether the fingerprint seizure amounts to requiring a person to be a "witness" against himself or herself, as barred by the Fifth Amendment." "That is a different exercise in interpretation from the balancing test necessitated by the word "unreasonable" in the Fourth Amendment. The word "witness" still limits the scope of the privilege against self-incrimination to those acts that are themselves testimonial in nature, regardless of how the digital age has raised the stakes on the amount and type of information that might result from the compelled, non-testimonial act."

#Fifth Amendment Self-incrimination

I/M/O Search Warrant for [Redacted]yahoo.com, No. 16-2316M (FFM) (C.D. Ca. Mar. 31, 2017)

The Government secured a sealed warrant under the Stored Communications Act directed to Adobe Systems Incorporated that included a notice preclusion order ("NPO"). The NPO prohibited Adobe from notifying anyone, including the target of the investigation that led to issuance of the warrant, of the existence of the warrant. The NPO had no duration. Adobe applied for a modification of the NPO to include a date certain for its expiration. The court held that the SCA did not require a "finite NPO period." However, the NPO implicated the First Amendment rights of Adobe. The NPO was a prior restraint and content-based. Accordingly, it

was subject to strict scrutiny. The court concluded that the NPO was not narrowly-tailored given its unlimited duration and modified the NPO to include a set expiration date. The court also partially granted Adobe's request to unseal the parties' filings and its order.

#Miscellaneous

#SCA

In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017)

The Government secured warrants pursuant to Section 2703 0f the SCA compelling Google to disclose electronic data in the accounts of targets of two investigations. "Each account holder resides in the United States, the crimes they are suspecting of committing occurred solely in the United States, and the electronic data at issue was exchanged between persons located in the United States." Google partially complied with the warrants by producing data that it could confirm was stored on servers in the United States but refused to produce other data, relying on the panel decision in *Microsoft v. United States* (*q.v.*). Google contended that it might break user data into component parts, that the parts might be stored in different locations outside the United States, and that it did not have the technological capability to "determine the location of the data and produce that data to a human user at any particular point in time." The Government moved to compel Google to comply with the warrant and the court granted the relief sought. Rejecting the reasoning of Microsoft, the court held that there was no seizure of data outside the United States because there was no meaningful interference with the account holders' possessory interests in the data. Moreover, the "conduct relevant to the SCA's focus will occur in the United States." The court also rejected Google's arguments that the sovereignty of any other nation would be implicated and rejected *Microsoft's* holding that multilateral assistance treaties ("MLAT") could be resorted to by the Government.

#SCA

In re Search Warrants for Info. Associated with [redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 25 F. Supp. 3d 1 (D.D.C. 2014)

The magistrate judge denied the Government's application for a warrant to search the records and content of an email account: "Despite this Court's repeated prior warnings about the use of formulaic language and overbroad requests that –if granted—would violate the Fourth Amendment, this Court is once again asked by the government to issue a facially overbroad search and seizure warrant." The court's explanation included:

(1) Drafting errors in the application had "the potential to confuse the provider *** which must determine what information must be given to the government."

(2) The Government's application's "ask for the entire universe of information tied to a particular account, even if it has established probable cause only for certain information."

(3) Although the court had imposed "minimization procedures" in the past, it had warned the Government to adopt strict protocols to avoid submitting applications for "general" warrants.

(4) "To follow the dictates of the Fourth Amendment and to avoid issuing a general warrant, a court must be careful to ensure that probable cause exists to seize each item specified in the warrant application."

(5) "[I]n light of the government's repeated submission of overly broad warrants that violate the Fourth Amendment, this Court can see no reasonable alternative other than to require the provider *** to perform the searches."

(6) The application failed to provide that the Government would "destroy all contents and records that are not within the scope of the investigation ***."

The magistrate judge denied a renewed application in its Second Memorandum Opinion and Order filed on April 7, 2014.

On August 8, 2014, a district judge vacated the order denying the renewed application and granted the application. The district judge reasoned in part:

(1) "[T]he government's search warrant properly restricts law enforcement discretion to determine the location to be searched and the items to be seized."

(2) "[T]he information contained in the [supporting] affidavit *** supports a finding of probable cause because there is a fair probability that the electronic communications and records that the government seeks, which are described in detail ***, will be found in the particular place to be searched."

(3) "[T]he procedures the government adopts for executing the search warrant comply with the Fourth Amendment and are permissible under Rule 41."

(4) "[B]ecause the government's proposed procedures comply with the Fourth Amendment and are authorized by Rule 41, there is no need for Apple to search *** and determine which e-mails are responsive ***."

(5) "Enlisting a service provider to execute the search warrant would also present nettlesome

problems."

(6) "[T]he practical realities of searches for electronic records may require the government to examine information outside the scope of the search warrant to determine whether specific information is relevant to the criminal investigation and falls within the scope of the warrant."

(7) The Government's presented "valid" concerns that the destruction or return of information

might implicate its *Brady* obligations or hinder its ability to introduce evidence.

#Fourth Amendment Particularity Requirement

#Fourth Amendment Ex Ante Conditions

In re Search Warrants for Info. Associated with Target Email Accounts/Skype Accounts, No. 13-MJ-8163-JPO (D. Kan. Aug. 27, 2013)

The Government submitted five applications for search warrants directed to Internet service providers in aid of an investigation of various crimes. The proposed warrants sought the disclosure of information under Section 2703 of the SCA and the seizure of that information as "fruits, evidence, and instrumentalities" of the crimes.

The court denied the applications without prejudice: First, it found "the rationale of [*United States v.*] *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails stored with, sent to, or received through an electronic communications service provider. Accordingly, the Fourth Amendment protections, including a warrant 'particularly describing' the places to be searched and the communications to be seized, apply ***. A warrant seeking stored electronic communications such as emails therefore should be subject to the same basic requirements of any search warrant: it must be based on probable cause, meet particularity requirements, be reasonable in nature of breadth, and be supported by affidavit."

Next, the court observed that, "whether a description of a place to be searched is sufficiently particular is a complicated question because of the differences because of the differences between the physical worlds" (footnote omitted). The court then, citing *United States v. Carey,* 172 F.3d 1268 (10th Cir. 1999), for the proposition that computers often contain "intermingled documents" such that, "law enforcement must engage in the intermediate step of sorting various types of documents and then only search the ones specified in a warrant," concluded that a warrant should specify "what type of file is sought."

The court then ruled that the applications were deficient: (1) "The warrants fail to set any limits on the email communications and information that the *** provider is to disclose ***, but instead requires each Provider to email communications in their entirety and all information about the account without restriction," (2) "the warrants fail to limit the universe of *** communications and information to be turned over *** to the specific crimes being investigated," and (3) the warrants, "fail to set out any limits on the *** review of the potentially large amount of *** communications and information *** [and] do not identify any sorting or filtering procedures ***," and (4) even assuming probable cause existed (which it did not for the preceding reasons), there were no limits on the Government's review of content.

The court made this suggestion should the applications be renewed: "While not endorsing or suggesting any particular safeguard, some possible options would be asking the *** provider to provide specific limited information such as emails containing certain key words or emails sent to/from certain recipients, appointing a special master with authority to hire an independent vendor to use computerized search techniques to review the information for relevance and privilege, or setting up a filter group or taint-team to review the information for relevance and privilege. Only with some such safeguard will the *** protection against general warrants be insured."

#Fourth Amendment Particularity Requirement

#Fourth Amendment Ex Ante Conditions

Sec. & Exch. Comm'n v. Huang, **No. CV 15-269, (E.D. Pa. Sept. 23, 2015)**

The defendants in this insider trading civil action had been provided with smartphones by their employer. The employer owned the devices and any corporate information but allowed the defendants to create passwords. The defendants returned the devices when their employment was terminated. The employer believed that relevant information was on the devices and gave the devices to the SEC but the SEC could not access content. The defendants refused to provide the passwords on Fifth Amendment grounds and the SEC moved to compel them to do so, arguing that they were "corporate custodians in possession of corporate records" and could not assert the Fifth Amendment. The court denied the motion. It concluded that, although the content might be corporate, the passwords were "personal in nature." The court also rejected the argument that the "foregone conclusion" doctrine applied.

#Fifth Amendment Self-Incrimination

Sennett v. United States, 667 F.3d 531 (4th Cir. 2012)

In this civil action brought to recover damages under the Privacy Protection Act, a search warrant was served on the plaintiff, a photojournalist identified by video surveillance as being present at a violent demonstration. Pursuant to the warrant, law enforcement seized various electronic media from the plaintiff. The Court of Appeals affirmed an award of summary judgment against the plaintiff, concluding, among other things, that probable cause existed to believe that the defendant was engaged in criminal acts and thus fell within the "suspect exception" of the Act.

#Fourth Amendment Exigent Circumstances

In re Smartphone Geolocation Data Application, 977 F.Supp.2d 129 (E.D.N.Y. 2013)

The Government secured an arrest warrant for a doctor based on a showing that he had issued thousands of prescriptions for controlled substances to the wrong people. The doctor refused to provide his location, so the Government sought an order for "prospective geolocation data relating to the cell phone believed to be used by the physician." The order was issued and the physician located and arrested. Explaining his rationale for granting the order, the magistrate judge concluded that the Government had shown that the data sought could reasonably assist in the doctor's apprehension and that, "[i]n light of the development and general awareness of geolocation technologies, I believe that the voluntary disclosure doctrine provides the most important point in evaluating requests for prospective data." In other words, "as to prospective geolocation data, cell phone users who fail to turn off their cell phones do not exhibit an expectation of privacy and such expectation would not be reasonable in any event." The court also held that a cell phone was not a "tracking device" under the SCA.

#Fourth Amendment Warrant Required or Not

In re Subpoenas, 692 F. Supp. 2d 602 (W.D. Va. 2010)

The Government served two investigative subpoenas on Abbott Laboratories "for a number of potential federal violations arising out of Abbott's impermissible off-label marketing" of a drug and for related health care fraud. After Abbott argued that the subpoenas were unduly burdensome, the Government offered to narrow the scope of the subpoenas to seek email from three people. In granting the Government's motion to compel compliance with the subpoenas as modified (which required Abbott to produce "live" e-mail and "snapshots" from backup tapes over a specific time period), the court found the subpoenas to be "reasonable" under the Fourth Amendment: The email sought was relevant to the investigation. The email

was on backup tapes preserved for other litigation and Abbott had nearly $30 billion in annual sales. Moreover, "if retrieving the e- mails the government requests is as difficult as Abbott conveys, then the fault lies not so much with an overly broad governmental request as it does with Abbott's policy or practice of retaining documents (documents Abbott has been required to retain for litigation purposes) in a format that shrouds them in practical obscurity." The court also rejected Abbott's argument that it was unduly burdensome "to formulate search terms relating to the off-label marketing of other FDA approved drugs."

#Discovery Materials

In the Matter of the Search of Content Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, No. 16-mc-80263-RS (N.D. Ca. Aug. 14, 2017).

The District Court ordered Google to produce all content responsive to the search warrant authorized by the Magistrate Judge, under 18 U.S.C. § 2703(a), that is accessible, searchable, and retrievable from the United States pursuant to the terms of the warrant. The Court conducted a two-part test to determine the applicability of the SCA. First, "whether the statute gives a clear, affirmative action that it applies extraterritorially," and second, if it does not, does the case involve "a domestic application of the statute." The Magistrate Judge reasoned that the conduct relevant to the focus of the SCA is the disclosure of the data in the service provider's possession and that such disclosure happens where Google accesses and delivers the information, which is here in the United States.

#Miscellaneous

#SCA

***United States v. Ackerman,* 831 F. 3d 1292 (10th Cir. 2016)**

Defendant convicted of possession and distribution of child pornography argued on appeal that NCMEC (National Center for Missing and Exploited Children) actions amounted to an unreasonable search of his email and attachments because no one sought a warrant or invoked any lawful basis for failing to obtain one. The district court denied Ackerman's motion to suppress both because NCMEC was not a governmental actor and, because NCMEC's search didn't exceed the scope of AOL's private search. The Tenth Circuit disagreed with that conclusion, finding that NCMEC was indeed a governmental entity or agent and searched Ackerman's email without a warrant.

#Fourth Amendment Warrant Required or Not

United States v. Aguiar, 737 F.3d 251, cert. denied (2d Cir. 2013)

The defendants moved before the trial court to suppress evidence derived from a GPS device that had been placed in a vehicle without a warrant over a six-month period. The motion was denied and the defendants were convicted of drug offenses. After the convictions, the Supreme Court decided *United States v. Jones. "Jones* left open the question of whether the warrantless use of GPS devices would be 'reasonable – and thus lawful – under the Fourth Amendment [where] officers ha[ve] reasonable suspicion, and indeed probable cause' to conduct a search." On appeal, the Court of Appeals declined to address the constitutionality of the search in issue because it concluded that the good faith exception to the exclusionary rule applied: (1) the GPS device had been installed in 2009, (2) no court of appeals had held that attaching a GPS device violated the Fourth Amendment until 2010, and (3) "sufficient Supreme Court precedent existed at the time the GPS device was placed for the officers here to reasonably conclude a warrant was not necessary ***."

#Fourth Amendment Good Faith Exception

United States v. Ahrndt, 475 Fed. Appx. 656 (9th Cir. 2012)

The defendant, a previously-convicted sex offender, was charged with transportation and possession of child pornography. He moved to suppress evidence derived from his use of a wireless network to connect with the Internet. A neighbor using the same network accessed shared files of the defendant indicative of child pornography and notified the police who, with the neighbor, observed child pornography. The police identified the defendant as a registered sex offender, accessed the network and determined its IP address after securing a search warrant, served a summons on Comcast and learned that the defendant was the subscriber for the IP address, and then secured a second warrant for media containing child pornography at the defendant's home. The defendant argued that the police violated the Fourth Amendment when the police initially accessed the defendant's files through the neighbor's computer. The court held that the defendant had a lower expectation of privacy in information broadcast over an unsecured wireless network than through a hardwired or password-protected one and that the defendant had no reasonable expectation of privacy in the file-sharing program in issue (iTunes). The court also rejected the defendant's argument that the neighbor and the police had violated the Electronic Communications Privacy Act when they accessed his network because his network was "readily accessible to the general public." Finally, the court found that the defendant had no subjective expectation of privacy: He was a "somewhat sophisticated computer user" and should have known about shared files and the unsecured nature of his network even if he did not know these facts. The Ninth Circuit reversed and remanded, holding it was clearly erroneous for the district court to find that the defendant used multi-media

downloading software to share files, and from that finding to conclude that he lacked a reasonable expectation of privacy. The Ninth Circuit directed the district court to conduct further fact finding to determine whether the defendant had a reasonable expectation of privacy in his computer files. The Court also instructed the district court to evaluate whether a search occurred in light of *United States v. Jones,* 565 U.S. ——, 132 S.Ct. 945 (2012).

#Fourth Amendment Warrant Required or Not

***United States v. Albertson*, 645 F.3d 191, cert. denied (3d Cir. 2011)**

The defendant pled guilty to one count of receiving child pornography and the district court sentenced him to 60 months of imprisonment and 20 years of supervised release with special conditions. On appeal, the defendant challenged, inter alia, the reasonableness of three of the special conditions of his supervised release, including a restriction on internet access and mandatory computer monitoring. The defendant argued that the special conditions were overbroad because they disproportionate to his criminal history and offense characteristics. The Third Circuit set out three factors for assessing whether a supervised release condition is overbroad: the scope of the condition with respect to substantive breadth; the scope of the condition with respect to its duration; "the severity of the defendant's criminal conduct and the facts underlying the conviction, with a particular focus on whether the defendant used a computer or the internet to solicit or otherwise personally endanger children"; and, "the proportion of a supervised release restriction to the total period of restriction (including prison time)." Applying the factors to the case, the court held that restriction prohibiting internet access unless preapproved by probation was too broad, unless the defendant has used the internet as an instrument of harm. Citing its decision in *United States v. Holm,* 326 F.3d 872, 878 (7th Cir.2003), the court reasoned that "such a ban renders modern life—in which, for example, the government strongly encourages taxpayers to file their returns electronically, where more and more commerce is conducted on-line, and where vast amounts of government information are communicated via website—exceptionally difficult." With regard to the duration of the supervised release term, the Circuit Court found the length of the supervised release term (20 years) was relative to the defendant's age (42 years). Turning to the conduct factor, the Court stated that a key consideration -- whether the defendant used the internet "to actively contact a child and solicit sexual contact" -- favored the defendant. Finally, the "relatively short incarceration sentence" imposed on the defendant (25 years) suggested to the Court that the length of the supervised release term was reasonable. In light of these factors, the Third Circuit concluded that the internet restriction condition failed for overbreadth because it was too restrictive. The Court vacated both conditions and remanded, directing the district court to achieve its sentencing purpose through a more targeted internet restriction, as well as a monitoring requirement "that allow computer inspections and the installation of

monitoring or filtering software."

#Miscellaneous

United States v. Andres, 703 F.3d 828, cert. denied (5th Cir. 2013)

The defendant appealed his conviction and sentence for drug conspiracy. He had been subjected to a traffic stop in Illinois. The vehicle he had been operating had been the subject of GPS surveillance from Texas to Illinois over a three-day period. Federal officers had informed Illinois police of the likely presence of drugs, but the stop was made on police observation of traffic offenses. After the stop, the defendant acted nervously when being questioned and, after consenting to a search, a dog alerted to the presence of cocaine. On appeal, the defendant argued that the initial traffic stop was a pretext and that the search of his vehicle violated the Fourth Amendment. The Court of Appeals disagreed: The initial stop was justified based on observed traffic violations. The initial duration of the stop was reasonable. The defendant's behavior led to reasonable suspicion that justified the continued stop and the search. The Court of Appeals also rejected the defendant's reliance on *United States v. Jones,* 565 U.S. — —, 132 S.Ct. 945 (2012). Declining to decide whether warrantless GPS are "per se unreasonable," and assuming that there was a Fourth Amendment violation, federal law enforcement had acted in an objectively reasonable manner in relying on existing precedent and reasonable suspicion of drug trafficking when the GPS device was installed.

#Fourth Amendment Warrant Required or Not

United States v. Archambault, 13-CR-100A (W.D.N.Y. Jul. 8, 2016)

Defendant found guilty of various child pornography charges filed a third Rule 33 motion requesting a new trial claiming that the government offered no proof regarding the victim's age. However, it was offered in the form of testimony. The Court found the argument suggesting that the government must introduce a birth certificate to prove a minor victim's age, without merit and denied the Rule 33 new trial motion.

#Trial Related

United States v. Ayache, No. 3:13-CR-153, (M.D. Tenn. Mar. 10, 2014)

The defendants were indicted for, among other things, conspiracy to defraud the Government. They moved to suppress evidence derived from searches of their *entire* email accounts for a

period of over one year. After a *Franks* hearing, the district judge struck as untrue statements in one paragraph of the affidavit submitted to the magistrate judge who issued the search warrants. Despite having stricken the untrue statements, the district judge found that probable cause existed to search all of the accounts. The district judge rejected the argument that the warrants were overbroad given the conspiracy allegations: "Neither the facts nor the law require that a 'reasonable' search should have been limited – artificially – only to emails between *** [the defendants]."

#Fourth Amendment Particularity Requirement

#Miscellaneous

United States v. Baez, 744 F.3d 30 (1st Cir. 2014)

The defendant was convicted of multiple arsons. In aid of its investigation of the defendant, the Government installed, without a warrant, a GPS device in the defendant's vehicle and tracked him for almost one year in. At issue on this appeal was whether the tracking fell within the good faith exception to the Warrant Requirement. The Court of Appeals affirmed: "It is enough for us to say that what occurred in this case was not the indiscriminate monitoring that Baez describes. This was relatively targeted (if lengthy) surveillance of a person suspected, with good reason, of being a serial arsonist." Here, "the agents were acting in objectively reasonably reasonable reliance on then-binding precedent."

#Fourth Amendment Good Faith Exception

United States v. Bah, 794 F.3d 617, cert. denied (6th Cir. 2015)

The defendants were in a rented vehicle that had been stopped for a speeding violation. One was arrested for driving on a suspended license and the second detained after a number of credit, debit, and gift cards were found in the vehicle. They were taken to a police department, where officers—without a warrant—looked at a text message and several incriminating images on one cell phone. Again without a warrant, officers used a magnetic card reader to access information from the cards and discovered that most if not all had been stolen and re-coded. Thereafter, a search warrant was secured to search the content of the other cell phones that had been seized. The supporting affidavit did not refer to anything that had been reviewed on the one phone. The defendants were charged with various crimes and moved to suppress evidence taken from the vehicle, the cards and the phones. The motions were denied and the defendants entered conditional pleas. On appeal, they challenged the denial of their motions.

The Court of Appeals affirmed: (1) The defendant passenger had no possessory interest in the vehicle and lacked standing to challenge the search of its content; (2) he did have standing to challenge the length of his pre- arrest detention, but the length was reasonable under the circumstances; (3) the scans of the magnetic strips on the cards was not a "search" because the scans were not a "physical intrusion on a constitutionally protected area" and did not violate the cardholders' reasonable expectations of privacy; (4) the reasoning of *Riley v. California* (*q.v.*) was inapplicable because the cards had little storage capacity and did not tend to store "highly personal information;" and (5) the application for the later search warrant was not tainted by the unconstitutionally obtained evidence as it was not relied on by the issuing judge.

#Fourth Amendment Required or Not

United States v. Banks, 556 F.3d 967 (9th Cir. 2009)

In this pre-*CDT* decision, the Court of Appeals affirmed the defendant's conviction for child pornography-related offenses. The defendant argued, among other things, that the district court had erred in denying his motion to suppress evidence seized pursuant to a search warrant. The court held that the supporting affidavit established an adequate foundation for issuance of the warrant. There was sufficient information that the defendant was engaged in the transmission of images of minors engaged in sexually explicit conduct and expert opinion was not necessary to show how "pedophiles act in the digital age." The court also held that the warrant, which did not exclude the defendant's home-based business from any search, could not have been more specific given the nature of computer systems.

Fourth Amendment Warrant Required or Not

United States v. Bari, 599 F.3d 176 (2d Cir. 2010) (*per curiam*)

On this appeal from the revocation of the defendant's supervised release, the Court of Appeals concluded that the district judge had not committed reversible error by "conducting an Internet search to confirm his intuition regarding a matter of common knowledge." The judge had done a Google search about yellow hats to confirm his belief that a yellow hat found in the garage of the defendant's landlord was the same type as that worn by the defendant when he robbed a bank.

The Court of Appeals looked to the Federal Rules of Evidence for "guidance," although the Rules did not apply "in full" at supervised release revocation proceedings. Undertaking a plain error review, the court held that the judge had used the Internet to confirm a "common sense supposition" and that, in so doing, the judge had taken permissible judicial notice of a fact as

allowed by "relaxed" Rule 201: "As the cost of confirming one's intuition decreases, we would expect to see more judges doing just that."

#Miscellaneous

United States v. Barnes, 803 F.3d 209 (5th Cir. 2015)

The defendants were convicted of various drug-related offenses. On appeal, one defendant argued, among other things, that "certain Facebook and text messages attributed to him at trial were introduced into evidence with insufficient authentication." The Court of Appeals rejected the argument:

Holsen [a cooperating witness] testified that she had seen Hall [the defendant] use Facebook, she recognized his Facebook account, and the Facebook messages matched Hall's manner of communicating. She also testified that Hall could send messages from his cell phone, she had spoken to Hall on the phone number that was the source of the texts, and the content of the cell messages indicated they were from Hall. Although she was not certain that Hall authored the messages, conclusive proof of authenticity is not required for the admission of the disputed evidence.

The Court of Appeals also held that any error in admitted the evidence was harmless given the overwhelming evidence of the defendant's guilt.

#Trial-Related #Social Media

United States v. Beckett, 369 Fed. Appx. 52, cert. denied (11th Cir. 2010) (*per curiam*)

The defendant created a fake MySpace account that appeared to belong to an underage girl and used it to contact underage boys through MySpace and Instant Messaging. He would then coerce the boys into engaging in sexual acts. After being convicted of various crimes arising out of the "scam," the defendant appealed, arguing that the trial court should have suppressed subscriber information received by law enforcement in response to "exigent circumstances" letters sent to Internet Service Providers and phone companies ("providers"). Based on the information, a warrant was secured, the defendant's computers and related media were seized, and he was arrested. A computer search revealed "a plethora of child pornography and evidence that connected the computer to conversations" with the boys. The defendant argued on appeal that no "emergency" existed under the Electronic Communications Privacy Act which justified the disclosure of subscriber information in response to mere letters. In affirming the defendant's conviction, the Court of Appeals held that the ECPA does not provide a statutory

suppression remedy absent a constitutional violation. There was no Fourth Amendment violation, as the defendant had no reasonable expectation of privacy in "identifying information transmitted during internet usage and phone calls that is necessary for the ... [providers] to perform their services" (as opposed to content)— and that the defendant had entered into written agreements with the providers that prohibited use of services for illegal activities and that allowed the providers to turn over subscriber information related to such activities. The court also rejected the defendant's argument that law enforcement exceeded the scope of the warrant when the content of his computers were searched.

#Fourth Amendment Exigent Circumstances

United States v. Beckmann, 786 F.3d 672 (8th Cir. 2015), *cert. denied*, 136 S.Ct. 270 (2015).

The appellant was convicted of possession of child pornography. He was visited by two officers to confirm his address and ensure compliance that conditions that had been imposed. An officer observed a computer monitor and saw the appellant "messing with wires/cords." After being given consent to look at the monitor, additional devices, including an unconnected external hard drive, were observed. Although he was not given specific consent to do so, an officer searched the drive and uncovered evidence of child pornography. A search warrant was then secured that was to be executed on a date certain. However, the inspection did not begin until several months after the date had passed and an inventory was not filed for several years. The defendant was indicted for possession. His motion to suppress was denied in part and he entered a conditional plea thereafter. The Court of Appeals held that the consent to search did not extend to the hard drive and that the failure to comply with the execution deadline and to make a timely return warranted concern. However, "exclusion of evidence is not the proper remedy without showing prejudice or reckless disregard" and the appellant failed to make that showing.

#Fourth Amendment Warrant Required or Not

United States v. Berg, No. CR10-310 RAJ (W.D. Wash. Jan. 23, 2012)

The defendant was incarcerated pending sentencing. He requested access to a dedicated stand-alone computer at his place of detention to access discovery provided by the Government, "particularly an extensive Excel spreadsheet created by the Government which summarizes financial records." The court allowed the access, having found that "special and unusual circumstances" existed: "This case has an unusually large amount of discovery that can only be effectively reviewed on a computer. The typical availability of a computer for the defendant ***

would be insufficient to review the large amounts of financial materials in time for his sentencing."

#Discovery Materials

United States v. Blagojevich, 612 F.3d 558 (7th Cir.) (en banc), rehearing en banc denied, 614 F.3d 287 (7th Cir. 2010).

During the criminal trial of former Illinois Governor Blagojevich, the trial judge decided not to reveal the names of the jurors until the trial ended. Media organizations moved to intervene to challenge this decision. The judge denied the motion as untimely and held the deferred disclosure did not violate the Fourth Amendment. On an appeal brought under the collateral order doctrine, a panel of the Seventh Circuit reversed. The panel held that the judge had abused his discretion in finding the motion to be untimely. (The judge had promised the juror's that their names would not be released during trial). On the merits, the panel held that there was a presumptive right of access to the names and remanded to the judge to conduct a hearing and balance that right with the risks of releasing the names. Several Circuit judges dissented from the denial of *en banc* rehearing, criticizing the panel for amending its initial opinion during the Circuit's internal deliberations on the rehearing and contending that the panel had erred.

#Trial Related

United States v. Blake, No. 15-13395 (11th Cir. Aug. 21, 2017).

The Eleventh Circuit affirmed the conviction of defendants Blake and Moore for child sex trafficking for managing a prostitution ring involving at least two girls under the age of eighteen. The Court held that the district court did not exceed its authority in compelling, under the All Writs Act, the manufacturer of the tablet computer to assist FBI agents in bypassing the tablet's security features taken from the defendants, the warrant search for defendant's email account satisfied the Fourth Amendment particularity requirement, and the exclusionary rule did not apply to require suppression of evidence discovered upon execution of search warrants for the social networking website account of the defendant.

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

United States v. Borowy, 595 F.3d 1045 (9th Cir.) (per curiam), cert. denied, Borowy v. United States, 562 U.S. 1092 (2010).

The defendant entered a conditional plea to possession of child pornography and appealed from the denial of his motion to suppress evidence. (He also appealed from a Rule 11 error). An FBI agent had conducted a keyword search on a publicly available peer-to-peer file- sharing network and, using a software program, identified images of child pornography. The agent then downloaded and viewed files from the defendant's IP address, several of which contained child pornography. The agent then secured a search warrant and seized the defendant's laptop, CDs, and floppy disks. Forensic examination revealed hundreds of child pornographic images. The Court of Appeals affirmed, holding that the defendant had no expectation of privacy in a file-sharing network. The court also held that the defendant's "ineffectual effort" to prevent the sharing of his files did *not* create an objectively reasonable expectation of privacy. The court rejected the defendant's argument that the agent's use of the software program constituted an unlawful search, as the contents of the defendant's files were already available to the public. Finally, the court held that the agent had probable cause to download files. The court did not resolve "whether downloading a file constitutes a seizure." The court also noted that it was only presented "with the limited case of a targeted search of publicly exposed information for known items of contraband" and rejected the defendant's argument that its decision would "allow unrestricted government access to all internet communications."

#Fourth Amendment Warrant Required or Not

***United States v. Bowen,* 799 F.3d 336 (5th Cir. Aug. 20, 2015), *denying rehearing and rehearing en banc,* 813 F.3d 600 (5th Cir. 2016).**

The defendant police officers shot and killed unarmed men in New Orleans during the "anarchy" that followed Hurricane Katrina. They were convicted of serious crimes but were awarded a new trial by the district court. The Court of Appeals affirmed:

The reasons for granting a new trial are novel and extraordinary. No less than three high-ranking federal prosecutors are known to have been posting online. Anonymous comments to newspaper articles about the case through its duration. The government makes no attempt to justify the prosecutors' ethical lapses, which the court described as having created an 'online 21st century carnival atmosphere.' Not only that, but the government inadequately investigated and substantially delayed the ferreting out of information about its in-house contributors to the anonymous postings. The district court also found that cooperating defendants called to testify by the government lied, an FBI agent overstepped, defense witnesses were intimidated from testifying, and inexplicably gross sentencing disparities

resulted from the government's pleas bargains and charging practices.

Like the district court, we are well aware of our duty normally to affirm convictions that are tainted only by harmless error. In this extraordinary case, however, harmless error cannot be evaluated because the full consequences of the federal prosecutors' misconduct remain uncertain after less-than-definitive DOJ internal investigations. The trial, in any event, was permeated by the cumulative effect of the additional irregularities found by the district court. We conclude that the grant of a new trial was not an abuse of the district court's discretion.

#Miscellaneous

#Trial Materials

United States v. Bowen, No. 13-30178 (5th Cir.) (per curiam) (on petition for rehearing en banc) (D. Conn. Feb. 24, 2016)

On petition for rehearing en banc for a Rule 33(b)(1) motion for new trial, the officers needed to present newly discovered evidence that was not introduced at their original trial. The only newly discovered evidence at issue is the identity of three anonymous commenters on Nola.com. extension is unwarranted and creates tension in case law.

#Trial Related

United States v. Bradbury, 2:14-cr-00071-PPS-APR (N.D. Ind. June 15, 2015)

The defendant posted a Facebook message about a plot to kill officials and destroy public buildings. This led to a police investigation and the issuance of search warrants for residences and the defendant's Facebook postings. After he was indicted the defendant moved to, among other things, suppress evidence derived from the searches. He argued that the warrants violated the Particularity Requirement because neither limited the scope of the searches and the Facebook warrant had no time limitation. As the court noted, the warrants "authorize[d] precisely the type of 'exploratory rummaging' the Fourth Amendment protects against." However, the supporting affidavits, which were incorporated by reference, limited the warrants. Moreover, this was a "textbook case" for application of the good faith exception because the officers had applied for warrants—*prima facie* evidence of good faith—and had

not acted dishonestly or recklessly in preparing the applications.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Particularity Requirement

#Social Media

United States v. Brooks, 715 F.3d 1069 (8th Cir. 2013)

The defendant was convicted of offenses related to a bank robbery. During the robbery, a bank teller concealed a GPS device among monies turned over to the defendant. Police and private security tracked the device. The defendant was arrested. A cell phone was seized incident to the arrest, a warrantless search revealed relevant images, a search warrant was subsequently secured, and a more thorough search conducted. The defendant unsuccessfully challenged the admission of the evidence taken from the cell phone as well as the GPS device. On appeal, the conviction was affirmed: (1) "Even if we assume that the initial search of the cell phone was improper, the subsequent search warrant satisfies both of the independent source requirements;" (2) Evidence Rule 404(b) "did not apply to the photos and video from the cell phone because the evidence was intrinsic to the charged crimes;" (3) the probative value of the images was not substantially outweighed by the potential for unfair prejudice under Evidence Rule 403; (4) the district court has not abused its discretion by taking judicial notice under Evidence Rule 702 of the accuracy and reliability of GPS technology; (5) the GPS data constituted a business record and was admissible under Evidence Rule 803(6); and (6) the admission of the GPS data did not violate the Confrontation Clause because the data "was not created to establish some fact at trial."

#Fourth Amendment Warrant Required or Not

United States v. Brooks, 648 F. App'x 791 (11th Cir. 2016)

The introductory paragraph of a warrant stated that probable cause exists if there is a digital device at the residence containing child pornography. Some of the items to be seized had no express reference to child pornography, however, the court states that this does not render a search warrant impermissibly overbroad in violation of the Fourth Amendment. Moreover, search warrants are not required to have a search protocol specifying the computer files to be searched.

#Fourth Amendment Particularity Requirement

United States v. Brown, 857 F.3d 334 (6th Cir. May 15, 2017)

The defendant was convicted of a number of wire fraud and extortion offenses. The evidence included a "trail of digital breadcrumbs" that led to him. Those breadcrumbs included anonymous postings on a website. The FBI secured records from the operator of the website that showed that the postings had been made using the TOR network to hide the user's IP address. The FBI then took possession of flash drives that the defendant had mailed to the victims of his plots. Information on the flash drives led the FBI to perform Google searches for a particular identifier that eventually led to the defendant's email address and tied him further to the plots. All this led to the issuance of a search warrant for the defendant's home and a forensic search of his computers and more incriminating evidence. The defendant appealed from, among other things, the denial of his motion to suppress. The Court of Appeals concluded that there were no falsities in the affidavit submitted in support of the warrant and that, even if these were edited out, probable cause still remained because the "unedited" facts included all the information secured from the anonymous postings as well as the content of the mailed flash drives, etc. The court of appeals also rejected the defendant's challenge to the trial judge's decision to permit jurors to pose questions during trial:

Understanding the evidence required the jury to grasp the Secret Service's forensic analysis of thumb drives, online posts, and Brown's computers, as well as the TOR network, Bitcoin, fingerprint matching, and digital photo manipulation. That's enough complexity for a district court to believe that permitting questions might aid jurors in their search for truth. And the precautionary measures taken by the trial judge ensured that the jury would retain its proper role and that the parties would not be prejudiced.

The Sixth Circuit did, however, remand for resentencing.

#Fourth Amendment Warrant Required or Not

#Trial-Related

United States v. Browne, 834 F. 3d 403 (3d Cir. 2016), *cert. denied,* 137 S. Ct. 695 (2017)

On appeal, the Third Circuit rejected the government's claim that under Rule 902(1), the contents of Facebook messages were "self authenticating" as business records. The court reasoned that the exception is designed to capture records that are accurate and reliable in context by the trustworthiness of the underlying information sources and the process by which the information is recorded.

#Social Media

United States v. Burgess, 576 F.3d 1078 (10th Cir. 2009), cert. denied, Burgess v. United States, 558 U.S. 1097 (2009).

The defendant appealed from the denial of his motion to suppress evidence of possession of child pornography. The evidence was on a laptop and two hard drives seized during the warrantless search of his motor home after a traffic stop and canine alert and searched thereafter pursuant to a warrant. In affirming, the Court of Appeals declined to adopt the Government's argument that the media could be searched under the "automobile exception" to the Fourth Amendment warrant requirement. It did question in *dicta,* however, whether the Supreme Court would treat computers differently from traditional "closed containers" because of the storage capacity of the former. Decided shortly before *United States v. Comprehensive Drug Testing, Inc.*, the Court of Appeals also stated: "It is folly for a search warrant to attempt to structure the mechanics of the search and a warrant imposing such limits would unduly restrict legitimate search objectives."

#Fourth Amendment Warrant Required or Not

***United States v. Burnett,* Crim. No. 12-CR-2332-CVE (D.N.M. Mar. 8, 2013)**

The defendant was indicted for illegally giving notice of electronic surveillance, wrongful disclosure of wire communication, and making a false statement. During discovery, the Government produced over 8,000 pages of materials on 15 CDs, including CDs secured from the office of the defendant's spouse. The defendant moved to, among other things, compel the production of forensic copies of hard drives and devices seized from the office of the defendant's spouse, formerly the head of the criminal division of the Office of the United States Attorney. The Government argued that some data had been inadvertently erased. The district court found this "unsatisfactory" and ordered the Government to take additional steps to attempt to locate the data.

[Note this statement by the district court: "[T]he Tenth Circuit has recognized the doctrine of spoliation of evidence in the civil context ***. However, the Tenth Circuit has not expressly adopted this doctrine in criminal cases ***. Even so, the Court may consider giving the jury an adverse inference instruction concerning the loss of evidence and what inferences may be drawn if the imaged files cannot be recovered"].

#Discovery Materials

United States v. Bynum, 604 F.3d 161 (4th Cir.), cert. denied, Bynum v. United States, 560 U.S. 977 (2010).

The defendant appealed from his conviction for transportation and possession of child pornography. The defendant had been identified after an agent entered a "child-pornography online chat group administered" by Yahoo and observed an unknown person uploading photos. The Government served an administrative subpoena on Yahoo, which provided subscriber information and IP addresses. The Government located the associated ISP, which provided an email address and telephone number in response to a subpoena. The Government secured the defendant's name and address from the "subscriber information." Then, and after again observing the person in the chat group, the Government secured a search warrant for the defendant's residence, seized his laptop, and found child pornographic images. On appeal, the defendant argued that he had a reasonable expectation of privacy in the subscriber information secured through the subpoenas. The Court of Appeals disagreed. The defendant "voluntarily conveyed all this information to his internet and phone companies" and had no subjective expectation of privacy. Moreover, even if he did, "such an expectation would not be objectively reasonable." The appellate court also rejected, among other things, the defendant's argument that minor errors in the affidavit supporting the search warrant negated probable cause.

#Fourth Amendment Warrant Required or Not

***United States v. Caira*, 833 F. 3d 803 (7th Cir. 2016)**

Caira appealed and argued that a warrant was required to obtain the information associated with his IP address and since no warrant was obtained, his rights under the Fourth Amendment were violated. The issue on appeal was whether Ciara possessed a reasonable expectation of privacy in the IP login information such that the Fourth Amendment requires the government to obtain a search warrant, rather than a subpoena, to obtain the information. The court reasoned that Caira shared his computer's IP address with Microsoft, a third party so he had no reasonable expectation of privacy in those addresses and therefore there is no Fourth Amendment violation.

#Fourth Amendment Warrant Required or Not

***United States v. Caraballo,* 831 F. 3d 95 (2d Cir. 2016), *cert. denied*, 137 S. Ct. 654 (2017)**

Defendant, convicted of murder and various drug related charges, argued that the "pinging" of his cell phone was a search that violated the Fourth Amendment. Officers asked Sprint, to track

the GPS coordinates of defendant's cell-phone over a two-hour period during which the murder occurred. On appeal, the Court reasoned that the officers reasonably believed that defendant posed an exigent threat to undercover officers and confidential informants involved in his drug operation. This threat justified the pinging of defendant's phone, constituted a limited intrusion into his privacy interests, and was the most limited way to This Court found that allowing the Rule 33 request would open the door for additional expansion of Rule 33 by importing other habeas doctrines blurring the line between direct and collateral review. The court here found this achieve the officers' necessary aim.

#Fourth Amendment Exigent Circumstances

United States v. Carpenter, 819 F. 3d 880 (6th Cir. 2016), *cert. granted,* 137 S. Ct. 2211 (2017)

Two defendants were convicted of aiding and abetting robberies that affect interstate commerce. On appeal, the court found no Fourth Amendment violation in the government's use of cell-site records to establish that two suspects used their cell phones close to the locations of armed robberies. The court ruled that the FBI's collection of cell-site data was not a search under the Fourth Amendment. The government had obtained information under the SCA. The law requires only that the government have reasonable grounds to believe the requested business records are "relevant and material to an ongoing criminal investigation."

#Fourth Amendment Warrant Required of Not

United States v. Carpenter, No. 12-20218 (E.D. Mich. Dec. 6, 2013), aff'd, United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016), cert. granted, Carpenter v. United States, 137 S.Ct. 2211.

The defendants, who were alleged to act as "lookouts" for store robberies, moved to suppress cell phone data secured through orders issued under Section 270(d) of the SCA. The motion was denied: (1) "the Sixth Circuit views obtaining routine cell phone data quite differently that it does data obtained via a G.P.S. device being placed on a vehicle without a warrant" and Section 2703(d) was not unconstitutional and, (2) reasonable grounds existed to obtain the orders given the factual basis set forth in the Government's applications. (As an additional basis for denying the motion, the court found that, "the agents relied in good faith on the Act in obtaining the evidence").

The court also denied a defense motion to, among other things, bar expert testimony on the operation of cell towers. The court held that it was not obligated to hold a *Daubert* hearing and that it was, "unnecessary in light of the full briefing *** and the materials submitted ***." The

court found that the proposed testimony would assist the trial of fact and was sufficiently reliable, but that the Government must lay an appropriate foundation at trial.

#Fourth Amendment Warrant Required or Not #Fourth Amendment Good Faith Exception #Trial Related

United States v. Carroll, 750 F.3d 700 (7th Cir. 2014)

The defendant pled guilty to possession of child pornography and sexual exploitation of a child. The Government secured a warrant to search the defendant's residence and his electronic devices based on information from the victim that was five years old. "The issue *** is whether this information was too stale to create a fair probability that evidence of child pornography or sexual exploitation *** would be found on a computer or other digital storage devices *** at the time the search warrant was issued. *** we recognize that a staleness inquiry must be grounded in an understanding of both the behavior of child pornography collectors and of modern technology." The Court of Appeals affirmed the conviction because the supporting affidavit adequately addressed why five-year old images might have been retained and how deleted images might be recovered from the defendant's devices.

#Miscellaneous

United States v. Chavez, 14-cr-00185 (JAM) (D. Conn. Feb. 24, 2016)

Defendant moves to suppress information acquired by the government from his telephone company, Verizon, concerning the location of cell phone towers that were used or accessed in connection with communications involving a specific telephone number that the government associates with defendant. Defendant principally contends that this information should be suppressed because the government did not obtain it by means of a search warrant. The court held that the acquisition of the information was neither a "search" nor "seizure" that is subject to the Fourth Amendment and that any legal violation in this case would not warrant a remedy of suppression of evidence.

#Fourth Amendment Warrant Required or Not

United States v. Christie, 624 F.3d 558 (3d Cir. 2010), *cert. denied, Christie v. United States*, 562 U.S. 1236 (2011).

On this appeal from his conviction for various child pornography- related offenses, the defendant challenged, among other things, the admissibility of two posts he had made on a web site. In rejecting the challenge, the Court of Appeals held that the posts (which the

defendant admitted he had made) were relevant and that, although the posts were "no doubt prejudicial," the district court had not abused its discretion in admitting the posts. The Court of Appeals also held that the district court had not erred in denying a motion to suppress: "no reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including ISPs."

#Trial Related

United States v. Cioffi, 668 F.Supp.2d 385 (E.D.N.Y. 2009)

Ruling on the defendant's motion to suppress evidence seized from his personal email account pursuant to a search warrant, which had been served and responded to by Google, the court found that the application used to establish probable cause had not been attached or incorporated into the warrant and that the warrant did not limit any emails to be seized to emails evidencing crimes. The court found that the defendant had a reasonable expectation of privacy in his personal email account. The court noted heightened concerns over the need for specificity when searching electronic information and considered several approaches to address those concerns, including that taken in *United States v. Comprehensive Drug Testing, Inc.* Rejecting the pre- search protocol approach of *CDT,* the court granted the motion as the warrant lacked specificity. The court also rejected the Government's argument s that the "good faith' and "inevitable discovery" exceptions applied.

#Fourth Amendment Warrant Required or Not

United States v. Comprehensive Drug Testing, Inc., 579 F.3d 989 (9th Cir. 2009), *opinion revised and superseded*, 621 F.3d 1162 (9th Cir. 2010) (*en banc*)

In what is fair to say is a controversial ruling stemming from grand jury investigations of steroid use by baseball players, the Court of Appeals set forth detailed protocols on how the Government and magistrate judges should proceed with search warrant applications where electronic information will be sought. These include Government waiver of reliance on the plain view doctrine, use of taint teams or third parties to segregate and redact information, disclosure of the risk of destruction of information seized, use of a search protocol tailored to locate only information for which probable cause exists and examination of such information only by case agents, and destruction or return of nonresponsive information. In *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (*en banc*), the Court of Appeals "dropped" the protocols described above and, in a concurring opinion, three judges referred to the protocols as "guidance" that "offers the government a safe harbor, while protecting the people's right to privacy and property in their papers and effects."

#Fourth Amendment Warrant Required or Not #Discovery Materials

United States v. Conner, 521 F. App'x 493 (6th Cir. 2013)

The defendant was convicted of receipt of visual depictions of child pornography and possession of child pornography. On appeal, he argued that the district court erred in not suppressing evidence derived from an officer's use of LimeWire, a peer-to-peer file-sharing program, to access files on his computer containing the images. Affirming the conviction, the Court of Appeals distinguished *United States v. Warshak,* 631 F.3d 266 (6th Cir. 2010 (*en banc*): "*Warshak* does not

control because peer-to-peer file sharing is different in kind from e-mail, letters, and telephone calls. Unlike these forms of communication, in which third parties have incidental access to the content of messages, computer programs like LimeWire are expressly designed to make files on a computer available for download by the public, including law enforcement." This defeated any objectively reasonable expectation of privacy. The court also rejected the defendant's argument that he had a reasonable expectation of privacy based on an alleged lack of knowledge that downloaded files would be publically accessible.

#Fourth Amendment Warrant Required or Not

United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011) *cert. granted, judgment vacated*, 132 S. Ct. 1534 (2012)

Suspecting the defendant was engaged in trafficking heroin, ICE agents and city police installed a pole camera outside his home in Phoenix. When the camera recorded the defendant "manipulating" the hatch and rear door panels on his vehicle, the officers suspected the defendant of utilizing secret compartments in his vehicle to transport heroin. In an effort to conduct intensive surveillance of the vehicle, officers attached a GPS tracking device to the vehicle while it was parked in a public place. The officers programmed the unit to transmit text messages of the vehicle's whereabouts every four minutes. A day or so later, the defendant drove his vehicle from Phoenix to Illinois. The GPS unit tracked him through various states. ICE agents began conducting visual surveillance once the tracking device's batteries began running low. GPS surveillance – which lasted about 60 hours -- was terminated once the defendant arrived in Illinois. ICE agents then asked the Illinois state police to try to "find a reason" to stop the Jeep. A state police officer pulled it over for a minor traffic infraction and, during the course of the stop, a drug detecting dog alerted to the vehicle and nine packages of heroin were found hidden in the vehicle's doors and the lining of the ceiling. The defendant was arrested and charged with possessing heroin with intent to distribute. After his motion to suppress the heroin was denied, the defendant pled guilty. On appeal to the Seventh Circuit, the defendant argued that his motion to suppress should have been granted because the warrantless GPS surveillance constituted an illegal "search". The Seventh Circuit ruled that the motion to

suppress was properly denied, and it affirmed his conviction. The Court reasoned that "the surveillance here was not lengthy and did not expose, or risk exposing, the twists and turns of [the defendant's] life, including possible criminal activities, for a long period. Judgment was vacated by the U.S. Supreme Court and the case was remanded to the Seventh Circuit for further consideration in light of *United States v. Jones,* 565 U.S. ——, 132 S.Ct. 945 (2012).

#Fourth Amendment Warrant Required or Not

United States v. Darby, 190 F. Supp. 3d 520 (E.D. Va. 2016)

"The instant prosecution is the result of an FBI investigation into a website that facilitated the distribution of child pornography. The government seized control of this website and for a brief period of time operated it from a government facility in the Eastern District of Virginia." The government sought a warrant from an Eastern District magistrate judge that would allow it to deploy a "Network Investigative Technique" (NIT) to determine the IP addresses of individuals who logged onto the website. The FBI arrested the alleged administrator of the website, who moved to suppress evidence derived from the NIT and a subsequent search of his home. The court denied the motions. Among other things, the district court noted that the relevant inquiry on the motions was whether the defendant had a reasonable expectation of privacy in the content of his personal computer in his home. The court found that the deployment of the NIT was a search under the Fourth Amendment and that the "abundance of child pornography available more than establishes probable cause to search the computers of visitors who knew about the site's contents." The court also held that Criminal Rule 41(b)(4) authorized a magistrate judge to issue a warrant for installation of a tracking device in that judge's district and, once installed, "the tracking device may continue to operate even if the object tracked moves outside the district."

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

#Miscellaneous

United States v. Davis, 750 F.3d 1186 (10th Cir. 2014) , *cert. denied, Davis v. United States*, 135 S.Ct. 989 (2015).

This appeal arises out of a series of armed robberies. The FBI suspected that a particular vehicle was being used to commit the crimes and, without a warrant, installed a GPS device to track the vehicle. The vehicle belonged to the girlfriend of an accomplice of the defendant. The FBI used the tracking information to locate and arrest the defendant and the accomplice after one

robbery. The defendant was convicted of various offenses and appealed, contending that, among other things, evidence found in the vehicle should have been suppressed under *United States v. Jones.* The Court of Appeals affirmed: "The warrantless attachment and use of the GPS device was the Fourth Amendment violation—the poisonous tree—that allowed agents to locate, stop, and seize evidence from the car in which Mr. Davis was riding—the tainted fruit. *** Mr. Davis does not allege a possessory interest or reasonable expectation of privacy in *** [the] girlfriend's car; the district court found he had neither. Because the poisonous fruit was planted in someone else's orchard, Mr. Davis lacks standing to challenge its fruits." The Court of Appeals declined to address the good faith exception to the Warrant Requirement.

#Fourth Amendment Warrant Required or Not

***United States v. Davis*, 573 F. App'x 925 (11th Cir. 2014), *vacated and en banc rehearing granted*.**

The defendant was convicted of armed robbery and other offenses. At trial, the Government introduced into evidence CSLI from cell service providers that placed the defendant and his codefendants near the locations of the robberies. The evidence was secured through an order issued under the SCA. The defendant objected to the admission evidence, arguing that his Fourth Amendment rights were violated by the warrantless "search" of the CSLI. The district court overruled the objection. On appeal, the defendant, among other things, pressed his objection. The Court of Appeals agreed with the defendant:

(1) Although *United States v. Jones* was distinguishable, "it concerned location information obtained by a technology sufficiently similar to that furnished in the cell site information to make it clearly relevant to our analysis."

(2) "[T]he Fourth Amendment protection against unreasonable searches and seizures shields the people from the warrantless interception of electronic data or sound waves carrying communications."

(3) "[C]ell site data is more like communications data than it is like GPS information. That is, it is private in nature rather than being public data that warrants privacy protection only when its collection creates a sufficient mosaic to expose that which would otherwise be private."

(4) "Davis has not voluntarily disclosed his CSLI to the provider in such a fashion as to lose his reasonable expectation of privacy."

However, the Court of Appeals affirmed the conviction under the good faith exception to the exclusionary rule: Law enforcement acted in good faith reliance on an order, that order was a "judicial mandate" to conduct the search in issue, and there was no "governing authority

affecting the constitutionality of this application of the Act."

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

***United States v. Davis*, 785 F.3d 498 (11th Cir.) (*en banc*), *cert. denied,* 136 S.Ct. 479 (2015).**

The defendant was convicted of a series of armed robberies. A panel of the Eleventh Circuit held that a court order issued pursuant to the SCA, 18 U.S.C. Section 2703(d), for CSLI that linked the defendant to the robberies violated the Warrant Requirement. Sitting *en banc*, the Court of Appeals construed the matter before it as follows:

On appeal, Davis argues the government violated his Fourth Amendment right by obtaining historical *** [CSLI] from MetroPCS's business records without a search warrant and a showing of probable cause. Davis contends that the SCA, as applied here, is unconstitutional because the Act allows the government to obtain a court order compelling MetroPCS to disclose its historical *** [CSLI] without a showing of probable cause. Davis claims the Fourth Amendment precludes the government from obtaining a third-party's business records showing historical *** [CSLI], even for a single day, without a search warrant issued to that third party.

In the controversy before us, there is no GPS device, no physical trespass, and no real-time or prospective cell tower location information. This case narrowly involves only (1) government access to the existing and legitimate business records already created and maintained by a third-party telephone company and (2) historical information about which cell tower locations connected Davis's cell calls during the 67-day time frame spanning the seven armed robberies.

The *en banc* Court reversed the panel decision:

In sum, a traditional balancing of interests amply supports the reasonableness of the [] 2703 order at issue here. Davis had at most a diminished expectation of privacy in business records made, kept, and owned by MetroPCS; the production of those records did not entail a serious invasion of any such privacy interest, particularly in light of the privacy-protecting provisions of the SCA; the disclosure of such records pursuant to a court order authorized by Congress served several substantial governmental interests; and, giving the strong presumption of constitutionality applicable here, any residual doubts concerning the reasonableness of any arguable 'search' should be resolved in favor of the government. Hence, the [] 2703(d) order *** comports with applicable Fourth Amendment principles and is not constitutionally unreasonable.

Alternatively, the court held that "the prosecutors and officers here acted in good faith and, therefore, under the well-established *Leon* exception, the district court's denial of the motion to suppress did not constitute reversible error."

There were a number of concurring and dissenting opinions.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. DE L'Isle, 825 F. 3d 426 (8th Cir. 2016)

The defendant was stopped for following a truck too slowly. An officer smelled burnt marijuana and saw air fresheners as he approached the defendant's car. A dog then alerted to controlled substances. After the defendant was arrested the police seized a stack of credit, debit and gift cards inside a duffle bag. Law enforcement scanned the magnetic strips on the cards and discovered that, among other things, the cards contained information from legitimate users of the cards. The defendant was charged with possession of counterfeit and unauthorized access devices. He moved to suppress, arguing that the scanning was an unconstitutional warrantless search. The motion was denied as untimely but the judge addressed the merits and found that there had not been a "search." The defendant was found guilty and appealed the holding that he had no privacy interest. The appellate court affirmed on the merits. The court held that scanning was not a physical intrusion and that the defendant did not have either a subjective or objective expectation of privacy because the information found in the strips was identical to that on the front of the cards. Moreover, at least some of the cards were counterfeit and the strips revealed that the defendant was in possession of contraband.

#Fourth Amendment Warrant Required or Not

United States v. DeLuca, 663 F. App'x 875 (11th Cir. 2016) (*per curiam*), *cert. denied,* 137 S. Ct. 1216 (2017)

The defendant was indicted for defrauding financial institutions in his role as president and sole shareholder of a company. The government seized the computers and hard drives of the company. Data seized included communications between the defendant and his attorneys. The government and the defendant signed a stipulation that included creation of a "filter team" for review of such communications. Thereafter, an assistant United States attorney decided that the stipulation was not in effect and provided at least some communications to the prosecution team without notice to the defendant. The defendant learned what the government had done when a communication appeared on an amended exhibit list just before the start of a second trial. The defendant moved to dismiss. The email was not introduced into evidence. The trial

judge deferred ruling until after the trial. After defendant was convicted he renewed the motion, which the district judge denied, having found no prejudice. The appellate court affirmed because existing precedent required a showing of "demonstrable prejudice" and the defendant had not made that showing. The court declined the defendant's invitation to revisit precedent because it was "outmoded as applied to modern- era digital communications and data storage."

#Discovery Materials

#Trial-Related

#Miscellaneous

United States v. Deppish, 944 F.Supp.2d 1211 (D. Kan. 2014)

Acting on a tip from Russian law enforcement about two photo albums on a Russian image board site, the Government secured a warrant to search an email account belonging to the defendant to search for child pornography. There were no temporal limitations on the warrant. The Government performed a "filtered, keyword search" of the email in the account but did not locate any child pornography. The defendant was then interviewed and he admitted that a minor depicted in the albums looked like his granddaughter. Then, based on information from the defendant's stepdaughter, the Government secured a warrant to search the defendant's home and seized electronic devices. He moved to suppress evidence derived from both warrants. The district court denied the motions:

(1) Probable cause existed for the warrants because the images met the definition of "sexually explicit conduct" under the controlling statute.

(2) There was a sufficient nexus between the criminal activity on the image board site and the defendant's email account.

(3) There was a sufficient nexus between the criminal activity and the defendant's home.

(4) The Particularity Requirement was satisfied because, although the warrant sought disclosure of the entire account, it "limited seizure to instrumentalities and evidence tending to show and identify persons engaged in sexual exploitation of children."

(5) "Defendant complains that the particular search methodology employed *** was overbroad but *** offers no alternative search methods that would protect his interests while permitting a search of the *** account."

(6) "A temporal limitation was not reasonable because child pornography collectors tend to

hoard their pictures for long periods of time."

(7) The good faith exception to the Warrant Requirement would apply in any event.

(8) There was no basis to conduct a *Franks* hearing. #Fourth Amendment Particularity Requirement #Fourth Amendment Good Faith Exception #Miscellaneous

***United States v. Diamreyan*, 684 F.3d 305 (2d Cir. 2012) (*per curiam*), *cert. denied*, 568 U.S. 1037 (2012).**

The defendant was convicted of wire fraud. His sentence was based on findings that he played a "managerial role" in the fraud and that it involved five or more participants. He appealed, arguing, among other things, that the sentence was unreasonable. The Court of Appeals affirmed. The findings were based on email from an email account that the defendant used for over ten years and which he had exclusive access to.

#Trial Related

***United States v. Djibo*, 151 F.Supp.3d 297 (E.D.N.Y. Dec. 16, 2015)**

Acting on information from a "cooperator," the defendant was stopped for a border inspection as he prepared to fly out of the United States. He was found to be carrying an iPhone5 and was asked for its phone number and password, both of which he provided. The defendant was then arrested for drug-related offenses and read his *Miranda* rights. He moved to suppress evidence derived from a warrantless "peek" at the content of his phone as well as a later search. The court found that (1) the defendant was in custody at the time he provided the number and the password and those statements should be suppressed as he had not been "*Mirandized*;" (2) the peek led to incriminating information which should be suppressed for the same reason; and (3) although the Government did secure a warrant to search the phone a second time, that search should be suppressed as the "fruit of the poisonous tree,"

specifically, the peek. The Government argued it would have "inevitably been able to hack the phone using IP-BOX." The court rejected this argument as it found that technology was unreliable.

#Fourth Amendment Warrant Required or Not #Miscellaneous

***United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)**

In this matter of first impression arising out of postings on a website by the defendant and others that led to a minor's suicide, the court held that the intentional breach of an Internet

website's terms of service could not survive a constitutional "vagueness" challenge and be punished under a provision of the Computer Fraud and Abuse Act.

#Miscellaneous

United States v. DSD Shipping, Crim. No. 15-00102-CG-B (S.D. Ala. Sept. 2, 2015)

The Coast Guard bordered a tanker when it docked in response to an email from a crewman that the crew had installed a pipe that allowed oily water to be discharged. The Coast Guard conducted a warrantless search and, among other things, seized electronic media. Thereafter, the Coast Guard secured a warrant to search the media and seized incriminating data. The district court denied the defendant owner's motion to suppress evidence derived from the warrantless search of the tanker and from the search of the media. The court found that there was no expectation of privacy in the areas of the vessel searched and, even if there was, probable cause existed to conduct a "stem to stern" search. The court also rejected the applicability of *City of Los Angeles v. Patel* (*q.v.*) to the search of a vessel. The court then rejected the challenge to the warrant. The court noted that "a temporal restriction appears to be an element of determining particularity of data seized, but the case law does not indicate temporal restrictions are mandatory requirements." The court found that temporal restrictions had been incorporated by reference into the warrant through attachments, which also limited the scope of the search and, that in any event, the good faith exception to the Warrant Requirement would apply.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

United States v. Durdley, No. 1:09-cr-00031-MP-AK (N.D. Fla. Mar. 11, 2010), *aff'd,* 436 F.App'x 966 (11th Cir. 2011), *cert. denied*, 565 U.S. 1127 (2012).

The defendant was indicted for distribution and possession of child pornography. He moved to suppress evidence seized pursuant to a search warrant. The defendant was employed by a public entity as a paramedic. While working, he accessed a computer owned by the entity. When the defendant left, he left a thumb drive in the computer. A supervisor opened the thumb drive and related ESI. A police officer arrived and conducted a warrantless search and seizure of the thumb drive. After an interview, the defendant was arrested, a State search warrant was issued, and hardware and software was seized from the defendant's residence. In denying the motion to suppress, the court found that the defendant had inadvertently shared his ESI with the users of the public computer and that the supervisor had not acted as a law enforcement officer in accessing the ESI. Moreover, the warrantless search by the officer did

not exceed that of the supervisor. Thus, he had no reasonable expectation of privacy. The court also held that the inclusion of erroneous information in the search warrant did not negate probable cause.

#Fourth Amendment Warrant Required or Not

United States v. Elonis, 841 F. 3d 589 (3d Cir. 2016), *cert. denied,* No. 16-1231 (U. S. Oct. 2, 2017)

The Supreme Court reversed the conviction of the defendant when it held that a jury instruction regarding the defendant's state of mind was erroneous. On remand, the court of appeals affirmed the conviction because the error was harmless. The defendant had been convicted of transmitting a threat to injure another through Facebook postings. The appellate court concluded that, despite the erroneous instruction, there was "overwhelming evidence demonstrating beyond a reasonable doubt that Elonis knew the threatening nature of his communications, and therefore would have been convicted absent the error."

#Trial-Related

#Social Media

United States v. Epich, No. 15-CR-163-PP (E.D. Wisc. Mar. 14, 2016)

The defendant was indicted for child-pornography related offenses. He moved to suppress evidence gathered from a search of his home because it had resulted from a warrant issued in Virginia that gave the FBI permission to use a "Network Investigative Technique" to "determine the identities of registered users of an anonymous web site hosted through a network hosted through a network called 'Tor.'" The district court adopted a magistrate judge's report and recommendation and denied the motion because "anyone who ended up as a registered user on the website was aware that the site contained, among other things, pornographic images of children," thus establishing probable cause. The district judge also held that the warrant complied with the Particularity Requirement given its content. The court rejected the defendant's argument that the motion should be granted because the magistrate judge lacked jurisdiction under Criminal Rule 41 to issue a warrant outside the geographic limits of that judge's authority: "Suppression of evidence is rarely, if ever, the remedy for violation of Rule 41, even if such a violation has occurred."

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

***United States v. Escamilla,* 852 F.3d 474 (5th Cir. Mar. 29, 2017)**

The defendant was convicted of conspiracy to possess and possession with intent to distribute narcotics. When stopped in a vehicle the defendant verbally consented to a search of a flip phone and the phone was returned to the defendant after the search. After the defendant had been arrested, and relying on the original consent, a warrantless manual search of the phone was conducted. Later, there was a forensics search. A second flip phone, broken in half but otherwise identical to the one found with the defendant, was seized from a second vehicle involved in the conspiracy. The trial court denied the defendant's motion to suppress evidence derived from the searches of the phone found with him. On appeal, the defendant challenged, among other things, the initial search and the two post-arrest searches of that phone. The Court of Appeals held that the defendant had voluntarily consented to the first manual search but that the consent did not extend to the second one. The Court of Appeals also held that the defendant had no standing to challenge the forensic search because he had disclaimed ownership of the phone after his arrest. Despite the one unconstitutional manual search the Court of Appeals affirmed, concluding that the jury could have convicted the defendant based on evidence derived from the broken phone and that any derived evidence from the unconstitutional search was merely duplicative of other admissible evidence.

#Fourth Amendment Warrant Required or Not

***United States v. Epstein,* No. CR 14-287 (FLW) (D.N.J. Apr. 14, 2015), *aff'd,* 864 F.3d 253 (3d Cir. 2017).**

The defendants in this kidnapping prosecution moved to suppress CSLI and other location information obtained from third party providers pursuant to a Section 2703(d) order issued by a magistrate judge. The defendants argued that the information could only be secured pursuant a search warrant. The court denied the motion:

Jones and *Riley* are distinguishable from this case because the facts here do not concern the search or seizure of a cell phone, or the content of any communication. Rather, the subscriber information provided by the third party cell phone service providers was cell site location data from their historical databases. Indeed, these were business records created and maintained by the service providers, which are not entitled to protection under Defendants' Fourth Amendment rights.

The court also held, in the alternative, that the evidence would be admissible in any event under the good faith exception to the Warrant Requirement.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

***United States v. Espinal-Almeida*, 699 F.3d 588 (1st Cir. 2012), cert. denied, 569 U.S. 936 (2013).**

Defendants appealed their drug conspiracy conviction. One argued, among other things, that data from a GPS device should not have been admitted. The device had been seized from a mothership and its content loaded into software which produced a track of the vessel that was admitted in both hard copy and electronic form. Rejected the defendant's argument, the Court of Appeals held that (1) there was a sufficient chain of custody to authenticate the device as having been the one taken from the vessel and (2) there was sufficient testimony about the processes used by both the GPS and the software to authenticate ("adequately, if not extensively") the data itself. The court also rejected the argument that authentication required expert testimony: "The issues surrounding the processes employed by the GPS and software, and their accuracy, were not so scientifically or technologically grounded that expert testimony was required to authenticate the evidence, and thus the testimony of [], someone knowledgeable, trained, and experienced in analyzing GPS devices, was sufficient."

#Miscellaneous

***United States v. Esquivel-Rios*, 725 F.3d 1231 (10th Cir. 2013), aff'd, 786 F.3d 1299 (10th Cir. 2015), cert. denied, 136 S.Ct. 280 (2015).**

This description is worth quoting in full:

"Garbage in, garbage out. Everyone knows that much about computers: you give them bad data, they give you bad results. There was a time when the enforcement of traffic laws depended on officers lying in wait behind billboards watching cars flow past. Today, officers nearly as often rely on distant computer databases accessed remotely from their dashboards, stopping passersby when the computer instructs. But what if the computer turns out to be a good deal less reliable than the officer's eagle eye? What if the computer suggests you've broken the law only because of bad data — garbage in, garbage out? Today's case requires us to wrestle with these questions for the first time, bringing the Fourth Amendment face-to-face with Charles Babbage."

The defendant's was stopped by a Kansas trooper described to be, "a regular before this court." The trooper decided to verify an out-of-state temporary registration tag. "Because of – and only because of – the dispatcher's 'no return' report, Trooper Dean *** stopped *** [the vehicle]. After a brief discussion, the trooper sought and received permission to conduct a search," which yielded a secret compartment containing drugs and led to the defendant's arrest. The defendant challenged the search on Fourth Amendment grounds. The motion was denied because the "no return" report justified the stop. The defendant was convicted on federal drug changes and, on appeal, challenged the denial of his motion.

The Court of Appeals reversed and remanded: (1) "This court and others have regularly upheld traffic stops based on information that the defendant's vehicle's registration failed to appear in a *** database – at least when the record suggested no reason to worry about the database's reliability," but (2) "the dispatcher replied not only that the tag yielded a 'no return' response ***. The dispatcher also added that *'Colorado temp tags usually don't return.'* This led to questions about the reliability of the database, including, (1) was the information available "'particularized evidence' that supplied *** some *** reason to think" that the van might be involved in a crime and, (2) how the Colorado database functioned. There were also questions about the trooper's credibility as a witness. The court remanded for further proceedings.

#Fourth Amendment Warrant Required or Not

***United States v. Farkas*, 474 F. App'x 349 (4th Cir. 2012), *remanded*, Nos. 1:10cr002200 (LMB), 1:13cv01191 (LMB) (E.D.Va. 2014), *appeal dismissed*, 592 F. App'x 211 (4th Cir. 2015), *cert. denied*, 136 S.Ct. 243 (2015).**

In this appeal from his fraud conviction, the defendant argued, among other things, that the district court violated his Sixth Amendment right to assistance of counsel when it denied his fourth motion for a continuance. In this motion, the defendant cited the need to review new discovery that had been added to the electronic database created by the Government, as well as "the ongoing invocation of privilege by a number of legal and accounting firms," which he argued prevented the disclosure of potentially exculpatory materials. The Court of Appeals disagreed, noting that the Government "had provided considerable assistance to defense counsel in reviewing documentary discovery production, including instituting an open file policy and holding regular meetings."

#Trial Related

***United States v. Farlow,* No. CR-09-38-B-W (D. Me. Dec. 3, 2009), *aff'd,* 681 F.3d 15 (1st Cir.), *cert. denied*, 568 U.S. 955 (2012).**

The court declined to suppress evidence of child pornography seized from a computer pursuant to a search warrant. Before the warrant had issued, the defendant had been communicating with a minor (actually a New York City police officer) over the Internet while speaking with a police officer in Maine, who secured a first warrant during the communications. A second warrant followed the search of the defendant's computer when Maine was searching for non-pornographic images and came upon child pornography. Rejecting the defendant's reliance on *Comprehensive Drug Testing,* ("Even the most computer literate of judges would struggle to know what protocol is appropriate in any individual case"), the court denied the motion. The warrant was not overbroad but was limited in scope to evidence of crimes under investigation and the plain view doctrine applied.

#Fourth Amendment Warrant Required or Not

United States v. Farrell, No. 2:15-cr-00029-RAJ (W.D. Wash. Feb. 23, 2016)

The defendant was charged with narcotics-related offenses in his role of administrator of the "Silk Road 2.0" website. The government alleged that "the site operated on the Tor network with the ostensible purpose of its operation being to mask Internet Protocol *** addresses of users of the network." The defendant moved to compel discovery into the relationship between the government and the Software Engineering Institute of Carnegie Mellon University (SEI), which conducted research on the TOR network pursuant to a government grant. Information produced by SEI to the government was used to secure a warrant and identify the defendant's IP address. The court denied the motion because, among other things, discovery of "additional technical details as to how SEI operated and captured" the IP address was unwarranted. Moreover, existing Circuit precedent held that Internet users had no reasonable expectation of privacy in their IP addresses. The court also denied discovery into the substance of meetings between SEI and the government.

#Discovery Materials

#Fourth Amendment Warrant Required or Not

United States v. Feiten, No. 15-cr-20631 (E.D. Mich. Mar. 9, 2016)

The defendant was indicted on child-pornography related offenses after he arrived on an international flight and was subjected to a secondary inspection at the airport. Images of child pornography were discovered on the defendant's personal computer during the inspection and a subsequent forensic examination revealed more images. He moved to suppress arguing, among other things, that the court should expand *Riley v. California* to hold that all warrantless searches of electronic devices at the border would be unconstitutional. The court denied the

motion because *Riley* "did not generate a blanket rule applicable to any data search of any electronic device in any context."

#Fourth Amendment Warrant Required or Not

United States v. Fluker, 698 F.3d 988 (7th Cir. 2012)

The defendants were convicted of mail and wire fraud. On appeal, one argued, among other things, that email introduced by the Government to rebut a defense had not been properly authenticated. Citing FRE 901(a), the Court of Appeals held that there was sufficient circumstantial evidence to make a prima facie showing that the email was authored by a particular person. The court also rejected the defendant's argument that the email was inadmissible hearsay: The email had not been offered to prove the truth of the matter asserted but, instead, to show context and rebut the defense.

#Trial Related

United States v. Frechette, 583 F.3d 374 (6th Cir. 2009), cert. denied, 562 U.S. 1053 (2010).

In this appeal from an order suppressing evidence seized pursuant to a search warrant, the defendant had paid for a one-month subscription to a child pornography web site, but the district court found that the subscription was over a year old and "stale," thus not supporting probable cause. In reversing, the Court of Appeals held that the supporting affidavit demonstrated the likely continued presence of child pornography on the defendant's computer despite the passage of time and the presence of the defendant at an address identified with the subscription.

#Fourth Amendment Warrant Required or Not

United States v. Galpin, 720 F.3d 436 (2d Cir. 2013)

The defendant entered a conditional guilty plea to, among other things, production of child pornography. Before the plea, the district court had denied the defendant's motion to suppress all the evidence gathered pursuant to a search warrant, finding that, although the warrant was overbroad and probable cause was lacking, the warrant was severable and images found during the execution of the warrant were in plain view. On appeal, the Court of Appeals held that, (1) the warrant was facially overbroad, as there was no probable cause to believe that the defendant possessed or produced child pornography, and (2) the district court failed to develop a record to support its findings related to severability and plain view. The Court of Appeals

vacated the judgment and remanded for further proceedings, during which the district court was directed, if appropriate, to address the good faith exception to the exclusionary rule under *Leon.*

[Note the following from the decision: "Where, as here, the property to be searched is a computer hard drive, the particularity requirement assumes even greater importance. As numerous courts and commentators have observed, advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain" (footnote omitted)].

#Fourth Amendment Particularity Requirement

***United States v. Ganias*, 755 F.3d 125 (2d Cir. 2014), *en banc rehearing granted* (2d. Cir. June 29, 2015),**

In 2003, the Army secured a search warrant in connection with an investigation of the defendant's business. It did not seize computers but, instead made forensic mirror images of the hard drives, "including files beyond the scope of the warrant, such as files containing Ganias' personal financial records." In 2004, based on evidence derived from paper records it also seized, the IRS joined the investigation and was

given copies of the imaged hard drives. Both agencies extracted files that were within the scope of the warrant but did not purge or delete non-responsive files. In 2005, the investigation expanded into possible tax violations. In 2006, two-and-a-half years after the images had been made, the Government secured a warrant to search for the defendant's personal financial records. "Because Ganias had altered the original files shortly after the 2003 warrant, the evidence obtained in 2006 would not have existed but for the Government's retention of those images." The defendant was indicted for tax evasion. He moved to suppress the evidence derived from the 2006 search. The motion was denied. He was found guilty and appealed.

The Court of Appeals vacated the conviction on Fourth Amendment grounds. It began with a restatement of the applicable law:

(1) "In light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror-images for off-site review is constitutionally permissible in most instances, even if wholesale removal of tangible things would not be."

(2) "The off-site review *** is still subject to the rule of reasonableness."

(3) “Even where a search and seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution.”

The Court of Appeals applied the law to the facts and concluded:

(1) “This combination of circumstances enabled the Government to

possess indefinitely personal records of Ganias that were beyond the 78

scope of the [2003] warrant while it looked for other evidence to give it probable cause to search the files.”

(2) Without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias’ Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation.”

(3) “If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant.”

(4) The Government acted unreasonably and “could not have had a good-faith belief that the law permitted them to keep the non- responsive files indefinitely.”

The Court of Appeals also considered the defendant’s juror misconduct claim “because the increasing popularity of social media warrants consideration of this question.” One juror had posted comments about the trial and became a Facebook “friend” of another juror. The defendant’s motion for a new trial was denied. The Court of Appeals affirmed the denial of that motion but recommended that cautionary instructions be given both at the start of a trial and at the beginning of deliberations.

#Fourth Amendment Warrant Required or Not #Fourth Amendment Good Faith Exception

#Trial Related

#Social Media

United States v. Ganias, **824 F.3d 199 (2d Cir.) (*en banc*), *cert. denied,* 137 S. Ct. 569 (2016)**

The defendant had been convicted of tax evasion. An appellate panel held that the government violated the defendant’s Fourth Amendment rights when, “after lawfully copying three of his

hard drives for off-site review pursuant to a 2003 search warrant, it retained these full forensic copies (or 'mirrors'), which included data both from responsive and non-responsive to the 2003 warrant, which included data both responsive and non-responsive to the 2003 warrant, while its investigation continued, and ultimately searched the non-responsive data pursuant to a second warrant in 2016." Sitting *en banc*, the Second Circuit held: "Because we find that the Government relied in good faith on the 2006 warrant, we need not and do not decide whether the Government violated the Fourth Amendment."

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

***United States v. Gatson,* Criminal No. 13-705 (D.N.J. Dec. 16, 2014)**

The defendant was indicted for crimes arising out of a scheme to burglarize homes and convert stolen goods into cash. Among other things, he moved to suppress evidence derived from searches of various electronic devices because the warrants did not include a sufficient search protocol. Noting that the Third Circuit had declined to adopt any particular procedures for searches of devices, the court found that the warrants were narrowly tailored and denied the motion. The court also denied the defendant's motion to suppress evidence obtained from his Instagram webpages: "law enforcement agents used an undercover account to become 'friends' with Gatson. Gatson accepted the request *** law enforcement officers were able to view photos and other information ***. No search warrant is required for the consensual sharing of this type of information."

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

#Social Media

***United States v. Gatson,* Crim. No. 2:13-CR-705 (WJM) (D.N.J. Oct. 9, 2015)**

The Government intended to introduce CSLI at trial through an FBI agent that would show that the defendant's cell phone was in the general location of the burglaries. He moved for a *Daubert* hearing to determine whether a Government witness was qualified to testify at trial about his analysis of the CSLI. The court denied the motion as the reliability of the agent's testimony was "firmly established" because it had been "widely accepted across the country"

and the testimony would be offered only to show general rather than precise location.

Trial-Related

United States v. Gilliam, 842 F.3d 801, denying cert. (2d Cir. Dec. 1, 2016)

A minor worked for the defendant as a prostitute in Maryland. He took the minor to New York City where she continued that work. The defendant abused the minor physically and emotionally in Maryland and New York City. After the defendant's foster mother and social worker expressed concern, Maryland police requested GPS data from the defendant's cell phone provider because of an "exigent situation." The provider gave real time GPS data to the Maryland police, which passed the data on to the FBI and NYPD. The defendant was located and arrested using the data. He was convicted of sex trafficking with a minor and transporting a minor in interstate commerce for prostitution. On appeal, the defendant challenged the district court's denial of his motion to bar use of the data. The Court of Appeals affirmed the conviction. First, it held that disclosure of the data was authorized by Section 2702(c)(4) of the SCA. The appellate court then considered whether "such a disclosure and arrest without a warrant violated the Fourth Amendment." Assuming that the Warrant Requirement applied, the Court of Appeals held that exigent circumstances existed given the need to protect the minor from being prostituted and subject to serious physical harm.

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Warrant Required or Not

United States v. Glassdoor, Inc. (In re Grand Jury Subpoena), No. 17-16221 (9th Cir. Nov. 8, 2017)

The Government secured a grand jury subpoena duces tecum compelling Glassdoor to disclose the identifying information of eight users who posted anonymous reviews about another company on its website. Glassdoor argued that complying with the subpoena would violate its users' First Amendment rights to associational privacy and anonymous speech. The Court of Appeals affirmed the lower court's order denying the motion to quash: "the proper test was the good-faith test the Supreme Court established in *Branzburg v. Hayes*, 92 S. Ct. 2646 (1972). Because the good faith test controls, "the only question is whether there is evidence that the grand jury is acting in bad faith." Glassdoor did not allege or establish bad faith and only asserted that there was a tenuous connection between the information the grand jury seeks and the subject of its investigation. "The information the government sought will allow the grand jury to contact and question employees "who have observed potentially fraudulent behavior by the company. Thus, there is a clear connection between the nature of the investigation—waste,

fraud, and abuse by the subject—and the information the government seeks—the identity of potential witnesses to that fraud and abuse."

#First Amendment

United States v. Graham, No. 1:05-CR-45 (S.D. Ohio May 16, 2008)

The defendants, indicted for tax violations, moved to dismiss the indictment on Speedy Trial Act grounds. Voluminous electronic information had been produced by the Government on a rolling basis. The information was tainted and incomplete. Defense counsel had been unable to manage review of that information. Faulting the Government, defense counsel, and itself, the court dismissed the indictment without prejudice.

#Discovery Materials

#Trial Related

United States v. Graham, 824 F.3d 421 (4th Cir. 2016)

The Court held that the government did not violate the Fourth Amendment by obtaining historical cell-site location information from cell phone provider without a warrant because of precedent "long held that an individual enjoys no Fourth Amendment protection 'in information he voluntarily turns over to [a] third part[y]"

The appellants were convicted of offenses arising out of a series of armed robberies. On appeal, they challenged the admission of evidence derived from CSLI over a 221-day period obtained from a third-party service provider pursuant to 2703(d) orders. The Court of Appeals rejected the argument that the privacy policy of the provider disproved any expectation of privacy because (1) the policy only spoke of collection by the provider rather than disclosure to others and (2) there was no evidence that the appellants read or understood the policy. Over a "spirited" dissent, the court then held:

The government conducts a search under the Fourth Amendment when it obtains and inspects a cell phone user's historical CSLI for an extended period of time. Examination of a person's historical CSLI can enable the government to trace the movements of the cell phone and its user across public and private spaces and thereby discover the private activities and personal habits of the user. Cell phone users have an objectively reasonable expectation of privacy in this information, its inspection by the government, therefore, requires a warrant, unless an established exception applies.

The court rejected the applicability of the third-party doctrine because cell phone users do not "convey" CSLI; rather, "[t]he service provider automatically generates CSLI in response to connections made between the cell phone and the provider's network, with or without the user's active participation." The court also held that the good faith exception to the Warrant Requirement applied because the government "reasonably relied on the SCA in exercising its option to seek a [] 2703(d) order rather than a warrant."

The appellants also challenged the admission of testimony related to the CSLI:

. (1) The court found no abuse of discretion in allowing lay testimony about the "range of operability" of cell sites because it required "no greater than minimal technical knowledge."

. (2) Although the court was "troubled" by other testimony that "went into technical detail" and appeared to be expert in nature, the admission was harmless error because, "[a]ll that really matters in that the cell site had a particular range of connectivity and that the phone connected to a cell site at a particular time—facts established through *** records and admissible portions of *** testimony."

. (3) There was no abuse of discretion in allowing lay testimony regarding the creation of maps based on the CSLI because it required "minimal technical knowledge or skill."

#Warrant Requirement Good Faith Exception

#Warrant Requirement Warrant Required or Not

#Trial Materials

United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (*en banc*)

The defendants had been convicted of crimes arising out of a series of armed robberies. On appeal, they challenged, among other things, the denial of a motion to suppress evidence derived from the warrantless search of historical CSLI by law enforcement that had been secured from the defendant's cell phone provider. An appellate panel held that the warrantless search violated the Fourth Amendment but affirmed the conviction on the basis of the good faith exception to the Warrant Requirement. Sitting *en banc*, the Fourth Circuit held that the defendants had no expectation of privacy in information that they voluntarily turned over to a third party. "The Supreme Court may in the future limit, or even eliminate, the third-party doctrine. Congress may act to require a warrant for CSLI. But without a change in controlling law, we cannot conclude that the Government violated the Fourth Amendment in this case." The court rejected the defendants' reliance on, among other things, "inapposite state cases

that either interpret broader state constitutional provisions instead of the Fourth Amendment, or do not consider historical CSLI records, or both." (footnote omitted).

#Fourth Amendment Warrant Required or Not

United States v. Halliburton Energy Services Inc., No. 13-cr-00165 (E.D. La. Sept. 12, 2013) ("Joint Memorandum in Support of *** Guilty Plea Pursuant to Cooperation Guilty Pleas Agreement")

This criminal action arose out of the Government's investigation into the Deepwater Horizon oil disaster in the Gulf of Mexico. The defendant agreed to pled guilty to "intentionally causing damage without authorization to a protected computer" in violation of 18 U.S.C. Sec. 1030(c)(a)(5)(A). The facts as described in the Joint Memorandum included that, "HESI's Cementing Technology Director, acting without HESI's authorization, intentionally ordered the deletion of computer- generated Displace 3D models related to the Malcondo well created in the weeks following the blowout ***, despite having been previously directed by a HESI executive to preserve material ***."

#Preservation & Spoliation

United States v. Harry, 816 F.3d 1268 (10th Cir. 2016)

The defendant was convicted of sexual assault in Indian Country while at the home of friends and while the victim was sleeping after a party. On appeal, he challenged, among other things, the admission into evidence of text messages between one of his hosts and himself after the assault. He argued that the government's failure to preserve text messages *sent by the host* deprived him of his due process rights and that the proper remedy would have to been to exclude the text messages *sent by him*. The appellate court disagreed because the exculpatory value of the messages was not apparent on their face and there was no evidence that the government acted in bad faith in failing to preserve the messages.

#Preservation and Spoliation

#Trial-Related

United States v. Heckman, 592 F.3d 400 (3d Cir. 2010)

The Court of Appeals reversed the imposition of special conditions on a convicted child pornographer, included one that imposed an unconditional lifetime ban on Internet access by

the defendant. Distinguishing *United States v. Thielemann,* the court noted that the defendant's conviction involved the "transmission of child pornography rather than the direct exploitation of children." Regardless of whether the defendant was a "serial offender" (which he was), there were other less restrictive conditions, which could control his behavior.

#Miscellaneous

United States v. Hernandez, **No. 15-CR-2613-GPC (S.D. Ca. Feb. 8, 2016)**

The defendant's vehicle was subjected to a "customary" search as she entered California from Mexico. Drugs were found during that search and during a secondary search. During interrogation, Homeland Security officers also searched the defendant's cell phone and found a text message that indicated she had met with someone in Mexico. One of the officers applied for a search warrant to search the phone on the basis that the phone was used to communicate with co- conspirators. A warrant was issued and the phone searched. The defendant moved to suppress, arguing that the initial search was unreasonable and that the search warrant, among other things, was not sufficiently particularized. The district court denied the motion. It found that the initial search was not intrusive. As to the second search, the court found that the absence of a search protocol did not violate the Particularity Requirement.

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

United States v. Hock Chee Koo**, 770 F. Supp. 2d 1115 (D. Or. 2011)**

Three defendants were charged with conspiring to commit wire fraud in violation of 18 U.S. Code § 1343, economic espionage in violation of 18 U.S. Code § 1832, and computer fraud in violation of 18 U.S. Code § 1030(a)(4). A defendant named Wu had not appeared in the case. Soutavong worked in the sales department of a manufacturer and distributor of after-market auto, Wu worked for a subsidiary in China, and Khoo was a former employee, who worked in warehouse and shipping. After Wu and Soutavong were fired from the company, the owner ("Hoffman") of the company took Wu's laptop to the FBI. According to the court, the FBI "had no idea [that owner] had seized Wu's laptop" when it "made an image of the laptop" using forensic software (the "Forensic Image") and an image using nonforensic software (the "Nonforensic Backup" The FBI kept these *images,* but returned the actual laptop and the Backup Image to Hoffman on November 20, 2006." The defendants were indicted on August 19, 2009, and as noted above, Khoo and Soutavong moved to exclude the Nonforensic Backup and

the Forensic Image. The defendants were indicted on August 19, 2009, and Khoo and Soutavong moved to exclude images of Wu's laptop and external hard drive, claiming neither image was an accurate copy of "Wu's computer *before it was seized.*" The defendants argued that the images should be excluded for lack of authentication, as required by Rule 901 of the Federal Rules of Evidence. In response, the prosecution said it intended "to offer the images as duplicates of what the FBI took into custody, and [did] not intend to offer" them "as proof of what was on Wu's computer before it was taken by Hoffman and Hansen." The district court denied the defendants' motion with respect to both images "if the government only intends to offer the Images as proof of what it obtained from Hoffman." The district court added, however, that the image Nonforensic Backup could be offered "to prove some of the contents of the laptop, if the government introduces it with appropriate testimony or circumstantial evidence to prove its authenticity." Finally, the court held that the Forensic Image could not be offered to prove the contents of the laptop Wu possessed. The court characterized the backup image made with the nonforensic software as best evidence and properly authenticated for purposes of proving what government had taken into custody, even if government intended to argue that it contained content that was on computer prior to its seizure. With regard to the image made with the forensic software, such an image was properly authenticated for purposes of proving what government had taken into custody, but was not properly authenticated for purposes of showing what was on computer prior to its seizure.

#Trial Related

United States v. Hoffman, No. 13-107 (DSD/FLN) (D. Minn. Aug. 1, 2013)

A police officer used a computer program to scan peer-to-peer file- sharing networks. The scanning led to suspected child pornography files and logs of IP addresses that shared the files. The defendant was identified through his IP address and a warrant was issued for his residence. He moved to suppress the evidence obtained as well as statements he made while the warrant was being executed. A magistrate judge recommended the motion be denied. The district judge agreed, concluding, among other things, that "the knowing use of a file-sharing program defeats any claim of a reasonable expectation of privacy in the files shared on the network."

#Fourth Amendment Warrant Required or Not

United States v. Hopson, Crim. Case No. 12-cr-00444-LTB (D. Colo. Sept. 4, 2014)

The defendant was indicted for various child pornography-related offenses. He moved pre-trial to, among other things, bar expert testimony about being the owner and primary user of a computer and digital media and his erasure of ESI. The court reserved ruling until trial, when it

would require a foundation about the witness' "qualifications to testify, based on his experience and training in the examination of computer devices," and that "the process by which he derived his opinions is reliable and based on sufficient facts and/or data."

#Trial Materials

United States v. Horton, 863 F.3d 1041 (8th Cir. July 24, 2017)

The defendants were indicted separately for accessing child pornography. The FBI had gained access to servers of an internet forum for sharing child pornography called "Playpen." The FBI relocated the content of Playpen's servers to a facility in the Eastern District of Virginia and secured a warrant from a magistrate judge in that district to search computers that had accessed Playpen. This would be done via a Network Investigative Technique ("NIT"), which sent code to the computers of Playpen users and caused the computers to send identifying information to the FBI. This led the FBI to the defendants, who resided within the Eighth Circuit. The district court granted the defendants' motions to suppress because the magistrate judge had exceeded her jurisdictional authority under the then-current text of *Fed. R. Crim. P.* 41(b) by issuing an extraterritorial warrant. The Eighth Circuit reversed. It held that, because the NIT retrieved *content* from the defendants' computers (as distinguished from IP addresses), and the defendants had a reasonable expectation of privacy in that content, a warrant was required. The court also held that the warrant was defective and that was void *ab initio*, a constitutional infirmity. However, because law enforcement did not demonstrate bad faith, the Court of Appeals applied the *Leon* exception to the Warrant Requirement.
#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. Houston, 813 F.3d 282 (6th Cir.), *cert. denied,* 137 S. Ct. 567 (2016)

The defendant was convicted of being a felon in possession of a firearm. The primary evidence against him was "video footage of his possessing firearms at his and his brother's rural *** farm. The footage was recorded over the course of ten weeks by a camera installed on top of a public utility pole approximately 200 yards away. Although this ten-week surveillance was conducted without a warrant, the use of the pole camera did not violate Houston's reasonable expectations of privacy because the camera recorded the same view of the farm as that enjoyed by passersby on public roads."

#Fourth Amendment Warrant Required or Not

***United States v. Huart*, 735 F.3d 972 (7th Cir. 2013), cert. denied, 134 S. Ct. 1907 (2014)**

The defendant had been released from federal prison to a halfway house. The house rules barred the possession of a cell phone and provided that all belongings would be searched and inventoried. Staff found that the defendant had a cell phone on which there were images of child pornography. The FBI took the phone, secured a search warrant, found the phone to be password-protected, unlocked the phone, and located the images after the date on which the warrant specified that the search was to have been conducted. The defendant's motions to suppress were denied and he entered a conditional guilty

plea tom possession of child pornography. His convictions were affirmed on appeal. The halfway house rules, "which Huart implicitly agreed to obey, demonstrate that he had surrendered any expectation of privacy in the contents of his cell phone, and that society was not prepared to recognize any such expectation." The Court of Appeals also rejected the defendant's reliance on *United States v. Jones*: "It was not a trespass for the *** Staff to seize contraband ***. Moreover, even if *Jones* applied ***, it would establish only that a search within the meaning of the Fourth Amendment occurred, not that it was unreasonable."

Although it concluded that the defendant had no reasonable expectation of privacy, the court did comment on his argument that the "late" search by the FBI was "essentially warrantless:"

"We do note that, under Federal Rule of Criminal Procedure 41(e)(2)(B), a warrant for electronically stored information is executed when the information is seized or copied—here, when the *** staff seized the phone. Law enforcement is permitted to decode or otherwise analyze data on a seized device at a later time. Huart provides no reason to doubt that Rule 41(e)(2)(B) would defeat his contention, if reached."

#Fourth Amendment Warrant Required or Not

***United States v. Hulscher,* 16-CR-40070-KES (D.S.D. Feb. 17, 2017)**

The defendant was charged with various federal firearms-related offenses. He was being investigated for separate offenses by a South Dakota police agency and the Bureau of Alcohol, Tobacco, and Firearms ("ATF"). The agency, acting pursuant to a South Dakota warrant, created a digital copy of data which it had extracted from the defendant's cell phone. Acting without a warrant, an ATF agent secured and reviewed a copy of the data from the police agency. The defendant moved to suppress the data in the federal action and a magistrate judge recommended that the motion be granted. The district court held that the agent should have secured a second warrant before he searched the copy: "The government's position, which would allow for mass retention of unresponsive cell phone data, is simply inconsistent with the

protections of the Fourth Amendment." The district court rejected, among other things, the Government's argument that the plain view doctrine applied because the agent's search lacked a sufficient justification. The district court also rejected the Government's argument that the good faith exception applied because, among other factors, were it be applied "law enforcement agencies will have carte blanche authority to obtain a warrant for all data on a cell phone, keep the unresponsive data forever, and then later use the data for criminal prosecutions on unrelated charges." However, should the defendant testify at trial the data might be used for impeachment if his testimony was inconsistent with the data.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

#Miscellaneous

#Trial-Related

***United States v. Jarman*, No. CRIM.A. 11-38-JJB (M.D. La. Aug. 4, 2015), *aff'd in part*, 847 F.3d 259 (5th Cir. 2017).**

The defendant requested, and thereafter secured an order, for the production of mirror images of three hard drives seized by the Government. The Government eventually delivered the images but not in "their current state at the time of the request." The Government then produced the images in different formats. Although the court found the Government's conduct "troubling," it declined either to dismiss the indictment or to suppress evidence derived from the hard drives because the defendant had not requested production in any particular format and the conduct had not violated any order. However, the court did afford the defendant the opportunity to "cross-examine the examiner and challenge his credibility regarding what he did during the imaging process."

#Discovery Materials

#Trial-Related

***United States v. Jenkins*, No. 3:13-cr-30125-DRH-11, WL 2933192 (S.D. Ill. 2014) vacated in part, 3:13-CR-30125-DRH-11, 2014 WL 4470609 (S.D. Ill. 2014)**

In this post-*Riley* decision, the defendant moved to suppress evidence derived from the warrantless search of his cellular phones after his vehicle was stopped by police and he was

arrested. The court granted the motion as no exigent circumstances existed.

#Fourth Amendment Exigent Circumstances

***United States v. Jenkins*, No. 12-15-GFVT (E.D. Ky. Nov. 20, 2012)**

In this First Amendment case, the newspaper moved to intervene, to set aside a statute's prohibition of contact with jurors, for access to juror names and addresses, and for an order of the court to release information of willing jury members from *U.S. v. Jenkins* and to permit contact with them. The newspaper argued that the statute which allows courts to limit interaction with jurors was unconstitutional because of its burden on the First Amendment. The district court denied all of the newspaper's motions except its motion for an order of the court to release the information of willing members of the jury and to permit contact with willing jurors. The court reasoned that the statute did not provide a blanket rule prohibiting jurors from speaking to the media. The district court stated that it would contact the jurors in writing to inform them of their right to refrain from speaking with the media, and if they were willing to speak to the media and communicated that willingness to the court, the court would provide their information to the newspaper.

#Trial-Related

#Miscellaneous

***United States v. Johnston,* 789 F.3d 934 (9th Cir.), *cert. denied,* 136 S. Ct. 269 (2015).**

The defendant was convicted of child pornography-related offenses. The government secured a warrant in 2006 to search his computer but performed more extensive reviews of its content in 2011 after the defendant rejected a plea deal. He argued on appeal, among other things, that a latter review exceeded the scope of the warrant. The Court of Appeals disagreed because the search methods were related

directly to the scope of the warrant and the agent was "not digging around in unrelated files or locations that might have prompted the need for a second warrant."

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant required or Not

***United States v. Jones*, 939 F.Supp.2d 6 (D.C. 2013)**

In *Jones,* the Supreme Court held 9-0 that the warrantless and extended 28-day GPS surveillance of a motor vehicle violated the Fourth Amendment. There were three separate opinions, none of which commanded a majority of the Court. One proceeded on a trespass theory, another on the duration of the surveillance, and the third with the premise that technology might require reexamination of Fourth Amendment principles. On remand, the District Court held that the defendant was not entitled to relief under the SCA because the Act does not provide a suppression remedy. The court also concluded that the good-faith exception to the exclusionary rule applied. Law enforcement officers had reasonably relied on the then-existing state of the law (which was "completely uncharted") and on the orders issued by judicial officers that authorized the surveillance.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

***United States v. Katakis*, 21 F. Supp. 3d 1081 (E.D. Cal. 2014), *aff'd*, 800 F.3d 1017 (9th Cir. 2015).**

At his trial for, among other things, obstruction of justice in violation of 18 U.S.C. Section 1519, the Government presented evidence that the defendant deleted email through the use of "DriveScrubber" software and by manual means. The defendant was convicted. The court granted the defendant's post-trial motion for judgment of acquittal: "Although the jury heard extensive and complicated evidence regarding the *** charge and the government resorted to every theory possible, none of the evidence was sufficient for the jury to find beyond a reasonable doubt that Katakis knowingly destroyed or concealed the emails with the intent to obstruct an FBI investigation that he knew of or contemplated."

#Trial Related

***United States v. Katakis,* 800 F.3d 1017 (9th Cir. 2015)**

The defendant had been indicted under 18 U.S.C. Section 1519 for obstruction of justice based on his apparent attempts to destroy ESI relevant to a criminal investigation against him. The jury found him guilty. The trial judge threw out the verdict because of insufficient evidence. The Court of Appeals affirmed: "The Government's theory of liability collapsed during trial, and the Government now raise several alternative theories to try and rescue the conviction. The evidence was insufficient to show that Katakis actually deleted electronic records or files. Further, proving Katakis moved emails from an email client's inbox to the deleted items folder does not demonstrate Katakis actually concealed those emails within the meaning of [] 1519."

#Miscellaneous

#Trial Related

United States v. Kernell, 667 F.3d 746 (6th Cir. 2012), *cert. denied,* 568 U.S. 826 (2012).

The defendant was convicted of obstruction of justice (18 U.S.C. Sec. 1519) for deleting electronic information related to hacking then- Governor Sarah Palin's email account. On appeal, he argued that the statute was unconstitutionally vague. First, the Court of Appeals rejected the Government's argument that the defendant lacked standing to make a facial challenge -- he did *not* actual knowledge of an FBI investigation into the hacking. Turning to the merits, the court held that (1) the statute requires that a defendant act with specific intent, (2) the statute does not have a "nexus" requirement, (3) the "in contemplation" requirement is unambiguous, and (4) the reach of the statute is not limited to those that have a pre-existing legal duty to retain information. The conviction was affirmed.

#Preservation and Spoliation

United States v. Kilbride, 584 F.3d 1240 (9th Cir. 2009), *post-conviction relief denied*, Nos. CV11-0174-PHX-DGC, CR05-0870 PHX DGC (June 28, 2012).

The defendants were convicted of various crimes (including several related to obscenity) arising out of their sending unsolicited bulk email ("spam") advertising adult websites. On appeal, they challenged, among other things, the jury instructions on "contemporary community standards." Rejecting this challenge, the Court of Appeals held that no precise geographic of the relevant community was required. The court also held that "a national community standard must be applied in regulating obscene speech on the Internet, including obscenity disseminated via email," but that, given the unsettled state of the law at the time, the trial court had not committed plain error by failing to give that charge.

#Trial-Related

United States v. Kim, 103 F.Supp.3d 32 (D.D.C. 2015), *appeal dismissed*, No. 15-3035 (D.C. Cir. 2015).

The Government seized the individual defendant's laptop before he boarded a flight from Los Angeles to Korea. It shipped the laptop to San Diego for a forensic examination. The hard drive was copied and searched without a warrant. Evidence was found that incriminated the

defendant and he and his corporation were indicted for export control violations. Later, the Government secured a warrant to search the laptop, which was never executed. The defendants moved to suppress the evidence derived from the warrantless search. The court rejected the argument that this was a border search for which a warrant was not required and granted the motion:

The search of the laptop began well after Kim had already departed, and it was conducted approximately 150 miles away from the airport. The government engaged in an extensive examination of the entire contents of Kim's hard drive after it had already been secured, and it accorded itself unlimited time to do so. There was little or no reason to suspect that criminal activity was afoot at the time Kim was about to cross the border, and there was little about this search – neither its location nor its scope nor its duration – that resembled a routine search at the border. The fundamental inquiry under the Fourth Amendment is

whether the invasion of the defendant's right to privacy in his papers and effects is reasonable under the totality of the circumstances, and the Court finds that it was not.

"Since there were no exigent circumstances present ***, if the search was not a 'border' search ***, then the failure to obtain a warrant requires suppression."

#Warrant Requirement Warrant Required or Not

United States v. King, 604 F.3d 125 (3d Cir. 2010), *cert. denied*, 562 U.S. 1223 (2011).

The defendant appealed from a sentence following a conditional guilty plea to interstate transportation to engage in sex with a minor (and under truly reprehensible facts). Law enforcement had gained entry to the defendant's residence with an arrest warrant for another resident. When that resident was arrested, she consented to the seizure of her computer. The defendant objected, contending that the hard drive belonged to him. The district court denied a motion to suppress evidence secured after this initial seizure. As stated by the Court of Appeals, "[t]hese facts present a novel question of law: when an owner of a computer consents to its seizure, does that consent include the computer's hard drive even when it was installed by another who claims ownership to it and objects to its seizure." Answering "yes," the court held that a computer was a "personal effect," and that the defendant relinquished any privacy in the hard drive when he placed it in a computer shared with another.

#Fourth Amendment Particularity Requirement

United States v. Kinison, 710 F.3d 678 (6th Cir. 2013)

The Government appealed from the district court's granting of the defendant's motion to suppress images and videos of child pornography. The defendant's girlfriend had gone to the police after she had received disturbing text messages from the defendant. With the girlfriend's consent, her phone was searched and the images and videos downloaded. After the girlfriend stated that the defendant was viewing these on his home computer, a search warrant was secured for the defendant's home. The supporting affidavit included the results of the search of the phone. During the course of the search, the defendant's cell phone was seen in plain view in his vehicle and a warrant secured to search the phone's contents. Reversing the district court, the Court of Appeals held that, (1) the police were not required to conduct further investigations to determine the girlfriend's veracity and reliability, (2) there was a sufficient nexus between the property to be searched and the alleged crime, (3) probable cause existed for both warrants. The Court of Appeals also held that, in any event, the good faith exception applied.

#Fourth Amendment Particularity Requirement

#Fourth Amendment Good Faith Exception

United States v. Kitzhaber, 828 F.3d 1083 (9th Cir. 2016)

A broad range of information related to the former Governor of Oregon was sought by a grand jury subpoena served on the State. Much of the information would have been available under Oregon's public records laws. The information included personal email that was archived on State servers. The appellate court held that the Governor had a reasonable expectation of privacy in his personal email (although the Fourth Amendment's protection does not extend to any use of a personal email account to conduct business business), and that the subpoena *** -- which is not even minimally tailored to the government's investigatory goals – is unreasonable and invalid." However, the court held that the Governor could not assert attorney-client privilege for his communications with State attorneys: "Whatever privilege may protect those communications belong to *** Oregon," not the Governor.

#Miscellaneous

United States v. Kolsuz, 185 F. Supp. 3d 843 (E.D. Va. 2016)

Government agents reasonably suspected that defendant's iPhone contained digital receipts of purchases; images of weapons parts, or other information related to illegal exports. Prior to conducting the off-site forensic search of defendant's iPhone, the border officials clearly had a "particularized and objective basis for suspecting" defendant of attempting to commit an ongoing or imminent crime. The court concluded that in light of the extensive evidence the border agents had already discovered, even if probable cause were required, which it is not, the

government agents had sufficient evidence to meet that higher standard.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Particularity Requirement

United States v. LaCoste, 650 F. App'x 302 (9th Cir. 2016)

The defendant pled guilty to conspiracy to commit securities fraud. The defendant was sentenced to prison and a three-year term of supervised release. He challenged two conditions imposed by the sentencing judge. One prohibited him from using the Internet without prior approval by his probation officer. The appellate court held that the facts did not warrant imposition of a total Internet ban because the defendant's use of the Internet "played only a tangential role in his commission of the underlying offense," and he had no history of using the Internet to commit other crimes. The court remanded to craft a more narrowly tailored condition directed to disparaging postings he had made about some of his victims.

#Miscellaneous

#Social Media

United States v. Ladeau, No. 09-40021-FDS (D. Mass. Apr. 7, 2010).

This criminal action began after the RCMP arrested a person who posted child pornography on an online network. Eventually, the Government secured the IP address for another person who participated in the network and, through an administrative subpoena, identified the defendant, secured a search warrant, and seized child pornography. The defendant moved to suppress, arguing that he had a reasonable expectation of privacy because he used software intended to limit public access to the network. In denying the motion, the court found that the defendant had no *objective* expectation of privacy, as others could access the network and disseminate information about him. The court also found, among other things, that probable cause existed to seize evidence of child pornography in any form.

#Fourth Amendment Exigent Circumstances

United States v. Lambis, 197 F. Supp. 3d 606 (S.D.N.Y. 2016), *appeal withdrawn,* No. 16-3149 (2d Cir. 2017)

The defendant moved to suppress narcotics and drug paraphernalia seized during in a search of his apartment. The DEA had secured a warrant for pen register information and CSLI for a target

cell phone. The DEA tracked the phone to its approximate location. To track the location more precisely the DEA used a cell- site stimulator to locate a particular apartment building. An agent entered the building and "walked the halls until he located the specific apartment where the signal was strongest." The DNA was given access to the apartment by the defendant's father and found the evidence. The court granted the motion to suppress. It found the search unreasonable under *Kyllo v. United States*, 533 U.S. 27 (2001), "because the pings from Lambis's cell phone to the nearest cell site were not really available 'to anyone who wanted to look' without the use of a cell-site stimulator." The court rejected the application of the "attenuation" doctrine because it found that the "chain of illegality" had not been broken and also rejected application of the third-party doctrine: "the location information detected by a cell-site stimulator is different in kind from pen register information; it is neither initiated by the sender nor sent to a third party."

#Fourth Amendment Warrant Required or Not

United States v. Lang, 78 F.Supp.3d 830 (E.D. Ill. 2015)

The defendants were charged with violations of the Animal Enterprise Terrorism Act. The Government secured a 2703(d) order for the disclosure of CSLI from two cell phones seized from a vehicle in which the defendants were travelling at the time of their arrest. Thereafter, the Government secured a warrant to search the content of the phones. The Government then moved for a 2703(d) order to obtain CSLI from a third phone used by a defendant through which mostly text messages were exchanged with one of the seized phones. The defendant challenged the motion, arguing that the Warrant Requirement applied. The court relied on the third-party doctrine in rejecting this argument. The court also found that the affidavit submitted in support of the motion established reasonable grounds to believe that the CSLI was relevant and material to an ongoing criminal investigation. In reaching this conclusion, the court relied on, among other things, a pamphlet seized at the time of arrest that contained a "Security Primer" describing how to avoid cell phone tracking.

#Fourth Amendment Warrant Required or Not

United States v. Lara, 815 F.3d 605 (9th Cir. 2016)

The defendant was convicted of being a felon in possession of a firearm and ammunition. Evidence offered against him was derived from two warrantless searches of his cell phone. He was on probation, one of the terms of which was that he consent to warrantless searches. The district court denied his motion to suppress. The defendant pled guilty but reserved his right to appeal from the denial of the motion. The appellate court reversed. The court held that the defendant's consent was only one factor in determining whether the searches were reasonable.

The court also considered that the defendant had not been convicted of a violent drug crime (thus distinguishing Circuit precedent), that the defendant had a lower expectation of privacy because he was a probationer, and that the terms of the warrantless search condition were unclear. The court cited to *Riley v. California* in concluding that the defendant had a substantial privacy interest in the data contained on the phone and that his interest was not overcome by the government's need to conduct warrantless searches of phones of probations with controlled substance convictions. The court also declined to apply a good faith exception to the exclusionary rule.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

***United States v. Lawing*, 703 F.3d 229 (4th Cir. 2012), *cert. denied*, 133 S.Ct. 1851. (2013).**

The defendant was convicted of possession of ammunition by a convicted felon. A confidential informant told the police that someone named "Drew" was selling cocaine. Based on information the CI provided, the police stopped the defendant's vehicle. To confirm that he was "Drew," the police dialed a telephone number that the CI used to reach "Drew." The defendant's cell phone rang, confirming to the police that he was Drew. A resulting search found a weapon and shells. On appeal, the defendant argued that the district court erred in denying his motion to suppress the evidence derived from the stop and search. The Court of Appeals affirmed, concluding, among other things, that the defendant's cell phone was not the subject of a search.

#Fourth Amendment Warrant Required or Not

United States v. Lichtenberger, 786 F.3d 478 (6th Cir. 2015)

The defendant was arrested for failure to register as a sex offender at the home he shared with his girlfriend. After the arrest, the girlfriend hacked into the defendant's laptop, discovered images of child pornography, and contacted the police. She showed some of the images to an officer, who viewed some of the images. The officer then seized various media and secured a warrant. The defendant was charged with child pornography-related offenses. The district court granted his motion to suppress evidence derived from the warrantless search and from the warrant and the Government appealed. The Court of Appeals concluded that the private search doctrine did not justify the officer's search because it exceeded the search conducted by the girlfriend. There was no "virtual certainty" that the officer's search would not tell him only what

he had been told by the girlfriend. Now was there any exigent circumstance that justified the warrantless search by the officer

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Warrant Required or Not

***United States v. Little*, 365 F. App'x 159 (11th Cir. 2010)**

The defendants produced and sold sexually explicit videos that were marketed online at sexually explicit websites. The defendants were convicted of obscenity-related offenses based on the trailers and on DVDs purchased through the websites. On appeal, the Court of Appeals rejected the defendants' argument (among others) that the "contemporary community standards" for defining obscenity was unconstitutional as applied to the Internet. Rejecting *United States v. Kilbride,* the Eleventh Circuit held that the community standards of the trial court (the Middle District of Florida) applied.

#Miscellaneous

***United States v. Lizarraga-Tirado,* 789 F.3d 1107 (9th Cir.), *aff'd,* 607 F.App'x 761 (9th Cir. 2015).**

The defendant was arrested along the Mexican border and charged with illegal reentry into the United States. At trial, he disputed whether he was in the United States at the time of his arrest. An agent testified that she had contemporaneously recorded the coordinates of the defendant's arrest through a GPS device. The Government offered into evidence a Google Earth satellite image which included an automatically-generated "tack" and its coordinates. The defendant objected to the introduction of the image on hearsay grounds. The trial court overruled the objection and the defendant was convicted. On appeal, he challenged the admissibility of both the image and the tack. The Court of Appeals held that the image itself, like a photograph, made no "assertion" and was not hearsay. Turning to the tack and the accompanying coordinates—which did make an assertion—the court held that there was no "statement" because a computer program rather than a person made the tack. The court observed that there was no authentication-based challenge to the evidence. If there had been one, the proponent of the Google-Earth-generated evidence would have to establish Google Earth's reliability and accuracy. That burden could be met, for example, with testimony from a Google Earth programmer or a witness who frequently works with and relies on the program. ***. It could also be met through judicial notice of the program's reliability ***.

[Note: The Court of Appeals did its own *ex parte* research and took judicial notice that the tack was automatically generated by Google Earth once its program was given the GPS coordinates by the court].

#Trial Related

United States v. Lockwood, No. 16-cr-20008-MFL-DRG (E.D. Mich. May 23, 2016)

Defendant was not honest with Pretrial Services, the Court, or law enforcement. He has purchased prescription drugs, frequented locations he is not permitted, used electronic devices to access the Internet, and made plans to escape. Further, he planned to frame a friend for a pipe bomb he may have constructed himself. Defendant's end-goal is to mislead law enforcement and the Court into thinking he provided valuable cooperation and prevented an imminent threat from materializing. Appeal denied.

#Miscellaneous

United States v. Lowe, 795 F.3d 519 (6th Cir. 2015)

The defendant appealed his child pornography-related conviction. He conceded that a laptop found in his home contained images and video files containing child pornography. The evidence against him allowed a juror to reasonably infer certain facts but, "without improperly stacking inferences, no juror could infer from such limited evidence of ownership and use that James [the defendant] knowingly, downloaded, possessed, and distributed the child pornography found on his laptop." Two others shared the defendant's home and could have been responsible for at least some of the images. Moreover, there was no reasonable basis for a juror to determine whether the defendant or one of the others knowingly possessed the child pornography. "In sum, the evidence *** fell well short of what we have found sufficient to convict in other cases involving multiple users of a single device."

#Trial Related

United States v. Mann, 592 F.3d 779 (7th Cir.), *cert. denied*, 561 U.S. 1034 (2010).

The defendant entered a conditional guilty plea of possession of child pornography and appealed the denial of his motion to suppress evidence of the pornography. The State of Indiana had secured a warrant to search for evidence of the crime of voyeurism (the defendant had installed a video camera in a women's locker room).

Several months after the defendant's computers had been seized, an officer used, among other things, a "forensic tool kit" to search the computers and discovered child pornography on files "flagged" by the kit as containing child pornography. Several months thereafter, the officer searched another computer using the kit and found more child pornography. Accepting the district court's findings of fact that the officer was searching for evidence of voyeurism, the Court of Appeals rejected the appeal. Distinguishing precedent and relying in part on *United States v. Burgess*, the court held that the execution of the search was reasonable: "Undoubtedly the warrant's description serves as a limitation on what files may reasonably be searched. The problem with applying this principle to computer searches lies in the fact that such images [of women in locker rooms] could be nearly anywhere on the computers." The court rejected the argument that use of the kit was unreasonable *per se,* although the court held that the officer exceeded the scope of the warrant when he opened the flagged files. The court severed the evidence from those files. The court also rejected the defendant's reliance on *Comprehensive Drug Testing: "*we are inclined to find more common ground with the dissent's position that jettisoning the plain view doctrine entirely in digital evidence cases is an 'efficient but overbroad approach.' " The court was also "skeptical of a rule requiring officers to always obtain pre-approval from a magistrate judge to use the electronic tools necessary." Instead, the Court of Appeals cautioned those "involved in searches of digital media to exercise caution to ensure that warrants describe with particularity the things to be seized and that searches are narrowly tailored to uncover only those things described." The court also found "troubling" the officer's failure to stop the search and apply for a new warrant when he uncovered evidence of child pornography. The court also 1expressed "distaste" for the timeline of the search.

#Fourth Amendment Particularity Requirement

United States v. Matthews, 250 F. Supp. 3d 806 (D. Colo. Apr. 20, 2017)

The defendant was charged with conspiracy to interfere with interstate commerce arising from two pawn shop robberies. At the time of the robberies he was in the custody of the Colorado Department of Corrections as a "community inmate" and, at the direction of his parole officer, was required to wear a GPS ankle monitor. One condition of the defendant's release was that "his" parole officer could conduct searches. Much of the evidence against the defendant derived from the warrantless search of the GPS data by *another* parole officer, who had been assigned to a federal task force investigating the robberies. The defendant moved to suppress. The district court denied the motion, finding that under Colorado law the "deviation from the expectation of privacy" created by the condition to searches that might be conducted by "his" parole officer when another officer conducted a search was "so *de minimus* as to imperceptible." Among other things, the court also denied the defendant's motion to exclude the testimony of the Government's GPS expert, finding that the defendant could cross-examine

the expert on the accuracy of map coordinates the expert had plotted. However, the court required the Government to supplement its Rule 19(a)(1)(G) disclosures.

#Discovery Materials

#Fourth Amendment Warrant Required or Not

#Probation and Supervised Release

#Trial-Related

United States v. Meregildo, 920 F.Supp.2d 434 (S.D.N.Y. 2013), *aff'd,* 785 F.3d 832 (2d Cir.), *cert. denied*, 136 S.Ct. 172 (2015)

In this prosecution for racketeering activity, one defendant entered into a cooperation agreement. A codefendant moved to compel the Government to provide log-in information for a Facebook account made by the cooperator under an alias while in prison, arguing that he was a member of the prosecution team and that his posts were *Brady* materials. The court denied the motion, holding that the cooperator was not part of the team and that the Government did not have the posts in its possession. In any event, the moving defendant had a full set of the posts.

#Discovery Materials

#Social Media

United States v. Michaud, No. 15-cr-05351-RJB (W.D. Wash. Jan. 28. 2016)

According to the Defendant, the NIT Warrant (Network Investigative Technique) violates the general provision of Rule 41(b) of the Federal Rules Of Evidence because the rule prohibits the magistrate judge in the Eastern District of Virginia from issuing a warrant to search or seize a computer outside of her district. Defendant argues that, because the warrant violated Rule 41(b) suppression is required, the good faith exception does not apply; and the warrant was not executed in good faith. The Court reasons that even if the warrant itself is subsequently invalidated, evidence obtained need not be suppressed. Whether a warrant is executed in good faith depends on whether reliance on the warrant was objectively reasonable.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Warrant Required or Not

United States v. Miller, 594 F.3d 172 (3d Cir. 2010)

After the defendant was convicted of possession of child pornography, the trial court imposed a life term of supervised release as well as special conditions that, among other things, barred the defendant from accessing the Internet without prior approval and requiring him to submit to monitoring of his computer activities. Relying on, among other decisions, *United States v. Thielemann,* the Court of Appeals vacated, concluding that the lifetime restriction on access was excessive under the facts. On remand, the trial court was directed that any "new conditions of supervised release should integrate a more focused restriction on internet access with the requirement of computer monitoring into a comprehensive, reasonably tailored scheme."

#Miscellaneous

United States v. Mitchell, No. 2:12-cr-00401-KJM (E.D. Ca. Sept. I, 2015)

The defendant was charged with knowing receipt of child pornography. A magistrate judge compelled the Government to provide the defendant with a mirror image of the media seized subject to a protective order that allowed access only to his defense team and experts. The district judge reversed because, notwithstanding *Fed. R. Crim. P.* 16, the Adam Walsh Act barred the relief sought as long the Government made relevant materials "reasonably available" and the defendant had "ample opportunity" to inspect the materials. The district judge found that the defendant had both.

#Discovery Materials

United States v. Mohamud, 843 F.3d 420 (9th Cir. Dec. 5, 2016)

The defendant was convicted of attempting to detonate a bomb at a ceremony in Portland, Oregon. The defendant resided in the United States but, while in London, created a new email account that would "play a significant role in the prosecution's case." The defendant exchanged email with a United States citizen in North Carolina, wrote articles, and communicated by email with a Saudi citizen. These included jihadist themes. He also provoked fear in his parents that he was planning to leave the United States for Somalia. The FBI then began to investigate the defendant. That included email and in-person meetings with undercover agents that ended when the defendant attempted to detonate what he believed to be a bomb. After conviction but before sentencing the Government advised that it had offered into evidence information collected pursuant to a FISA warrant. The defendant argued that the evidence should be

suppressed because of "late notice" and because the collection violated the Fourth Amendment. The district judge denied the motion. Among other things, the defendant raised the Fourth Amendment issue on appeal. The Court of Appeals affirmed the conviction. The Government had secured a FISA warrant to surveil the defendant and his actions based in part on its monitoring of a foreign national's email account, by which it learned of the defendant's communication with the Saudi citizen. "[T]he Government's monitoring of the overseas foreign national's email account fell outside the Fourth Amendment" and its collection of the defendant's communications was incidental to the lawful search of the foreign national's email. The Court of Appeals then assumed that the defendant had a First Amendment right in the incidentally intercepted communications and concluded that the search of those communications was reasonable: "although we do not place great weight on the oversight procedures, under the totality of the circumstances, we conclude that the applied targeting and minimization procedures adequately protected Mohammed's diminished privacy interest, in light of the government's compelling interest in national security."

#Fourth Amendment Warrant Required or Not

United States v. Molina-Gomez, 781 F.3d 13 (1st Cir. 2015)

The defendant was subjected to a secondary examination when he arrived in Puerto Rico from Columbia. He had made three short trips to Columbia in several months, gave odd and suspicious answers to routine questions, and his phone contained text messages about various monetary transactions. His belongings were returned after the examination other than a laptop and a Sony Playstation, which were detained for further examination when a dog "alerted" to the laptop. The items were dissembled 22 days later and bags were found inside that tested positive for heroin. The defendant was indicted for possession with intent to distribute. He moved to suppress the heroin on Fourth Amendment grounds and enter a conditional plea after the motion was denied. The Court of Appeals affirmed the validity of the search. The airport was the functional equivalent of a border and, absent a non-routine search, the border search exception to the Warrant Requirement applied. Even assuming that the search was non-routine, reasonable suspicion existed to justify it. Moreover, the 22-day delay was not unreasonable under the circumstances.

#Warrant Requirement Warrant Required or Not

***United States v. Montgomery,* 777 F.3d 269 (5th Cir. 2015)**

The defendant was stopped for traffic violations. He was arrested when a frisk for weapons revealed cocaine. His smartphone was seized. The defendant later asked for an officer's

assistance in erasing "naked images" from the phone that he did not want his father to see. In doing so, the officer saw images of an underage nude female. The defendant was indicted for knowing receipt and possession of child pornography. The district court denied the defendant's motion to suppress and he was convicted. On appeal, he challenged the constitutionality of the warrantless search. The Court of Appeals affirmed: "We hold that the pornography on the cell phone was obtained by Montgomery's consent, which was the product of an intervening act of free will on Montgomery's part that purged the taint of any alleged constitutional violation."

#Fourth Amendment Warrant Required or Not

United States v. Moreno-Magana, No. 15-cr-40058-DDC (D. Kan. Feb. 3, 2016)

Defendants contend that the good faith exception cannot apply here because the government has conceded that the agent involved did not rely on the warrants issued by the Kansas court to secure the location information from T-Mobile. The Court finds that the government relied in good faith, on the two warrants issued by the state court judge even though the warrants were not used. The record shows that the agent provided T- Mobile with the judge's warrants before ever requesting T-Mobile track defendants' phones because of exigent circumstances. The court reasons that, "where the alleged Fourth Amendment violation involves a search or seizure pursuant to a warrant, the fact that a neutral magistrate has issued a warrant is the clearest indication that the officers acted in an objectively reasonable manner or, as we have sometimes put it, in 'objective good faith."

#Fourth Amendment Good Faith Exception

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Warrant Required or Not

United States v. Mulcahey, No. CR 15-10112-RGS (D. Mass. Dec. 17, 2015)

The defendants moved to suppress evidence found on computer hard drives seized from their business premises. They argued that the warrant in issue was defective because it only authorized seizure and that a second warrant was required to search content. The court rejected this argument because the warrant clearly authorized both. The defendants also argued, relying on *Riley v. California,* that the warrant was defective because it did not impose conditions on any off- site search of content. The court rejected this argument for two reasons: (1) *Riley* was premised on a warrantless search and a warrant had been issued in the matter *sub judice* and (2) the defendants failed to identify "exactly what the conditions limiting the search might have been or how they would be applied as a practical matter." The court did observe: "It

is not that the desirability of conditions restricting the search of computers has not occurred to judges reviewing warrants like this one."

#Fourth Amendment Ex ante Conditions

#Fourth Amendment Warrant Required or Not

United States v. Muniz, No. H-12-221 (S.D. Tex. Jan. 29, 2013)

The Government secured a Section 2703(d) order compelling a cell- phone service provider to disclose historical cell-site location information ("CSLI") for a phone used by the defendant. The defendant moved to suppress, arguing that the warrantless disclosure violated the Fourth Amendment. In denying the motion, the court observed that, "[i]t is not yet settled whether the government needs probable cause and a search warrant to obtain CSLI, or whether it may do so through the statutory subpoenas authorized under 18 U.SC. Sec. 2703(d), which requires a less demanding 'reasonableness' standard." However, the court did not resolve that question. Instead, it relied on the good faith exception to the warrant requirement and concluded that, "[i]n light of the unsettled law in this area, and the explicit statutory provision for obtaining CSLI by subpoena, it was objectively reasonable for law enforcement and the magistrate judge to believe that Muniz's CSLI had no Fourth Amendment implications."

#Discovery Materials

#Fourth Amendment Warrant Required or Not

United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (en banc), cert. denied.

The defendant had been employed by an executive search firm. After he left employment, he convinced other employees to help him start a competing business. The employees used log-in information to download confidential information from the firm's database and transfer that information to the defendant. The employees were authorized to use the database, but the firm had a policy that prohibited the disclosure of confidential information. The defendant was indicted for, among other things, violations of the Computer Fraud and Abuse Act. The district court dismissed the CFAA counts, relying on *LVRC Holdings LLC v. Brekka,* 581 F.3d 1127 (11th Cir. 2009), which narrowly construed the phrases "without authorization" and "exceeds authorized access" under the CFAA. On interlocutory appeal, the Court of Appeals affirmed: "The government's interpretation would transform the CFAA from an anti-hacking statute into an expansive misappropriation statue."

#Miscellaneous

United States v. O'Keefe, 537 F. Supp. 2d 14 (D.D.C. 2008)

The court "borrowed" from the Federal Rules of Civil Procedure to address the adequacy of searches performed in discovery in a criminal proceeding and suggested that experts qualified under Fed. R. Evid. 702 would be required to testify about search methodology.

#Discovery Materials

United States v. Osborne, 677 Fed.Appx. 648 (11th Cir. Jan. 4, 2017) (*per curiam*)

The defendant was convicted of armed bank robbery. He objected to testimony by a Verizon Wireless records custodian about text messages and phone calls made from two telephone numbers and to the Government's introduction of summary documents containing the text messages. The district court overruled the objections. The Court of Appeals affirmed the conviction. First, it reviewed the defendant's challenge to the introduction of *outgoing* messages for plain error. The Court of Appeals declined to rule whether the messages were admissible under a hearsay exception as "records of a regularly conducted activity" under *Fed. R. Evid.* 803(6) but instead held that, assuming the admission was error, it was not plain error. Turning to the admission of *incoming* messages, the Court of Appeals held that the district court had not abused its discretion because these gave context to the defendant's *outgoing* messages and were not introduced for the truth of the matter asserted. One message did *not* give context but its admission was deemed to be harmless error. The Court of Appeals also held that the district court had not abused its discretion in admitting the summary documents under *Fed. R. Evid.* 1006 because these were supported by the record, the supporting evidence was presented to the jury, and the district court properly instructed the jury on the role of the summary exhibits. The Court of Appeals also held that the supporting evidence, although not lengthy, contained voluminous information and noted that the defendant had the opportunity for cross- examination.

#Admissibility

#Trial-Related

United States v. Patrick, 842 F.3d 540 (7th Cir. Nov. 23, 2016)

The defendant pled guilty to possession of firearms but reserved the right to challenge the

validity of his arrest. He had been released from prison and a warrant issued for his arrest for failure to comply with conditions of release. Law enforcement secured a second warrant that authorized them to locate the defendant using cell phone data. The Court of Appeals affirmed because the defendant did not have a privacy interest in his location since he was in a public place. However, while the appeal was pending, the Government revealed that it had used a Stingray device to locate the defendant. The Court of Appeals stated that this use posed "difficult issues" that it need not resolve in the appeal: "Questions about whether use of a simulator is a search, if so whether a warrant authorizing this method is essential, and whether in a particular situation a simulator is a reasonable means of executing a warrant, have yet to be addressed by ant United States court of appeals." One judge dissented in part based on the belief that the majority underestimated Stingray's capability.

#Fourth Amendment Warrant Required or Not

United States v. Perez, Crim. Action No. 14-611 (E.D. Pa. June 2, 2015), *aff'd*, No. 16-3365 (3rd Cir. Oct. 18, 2017)

The defendant was indicted for child pornography-related offenses. He moved to bar the Government from introducing evidence obtained during the search of his computer and three thumb drives seized pursuant to a warrant. The search was conducted using forensic examination software which, the defendant argued, exceeded the scope of the warrant. The court rejected this argument and found that the use of the software to scan the contents in their entirety to identify and segregate the files sought into a viewable format did not exceed the scope. The court also rejected the defendant's argument that a search of extracted files exceeded the scope because the examining agents only "previewed and/or opened a limited, filtered set of extracted files to determine whether they contained evidence of child pornography" and only limited information was made available for substantive review.

#Fourth Amendment Particularity Requirement

United States v. Phaknikone, 605 F.3d 1099 (11th Cir.), *cert. denied,* 562 U.S. 1066 (2010)

On an appeal from a conviction for, among other things, armed bank robbery, the Court of Appeals held that the trial court had erred in admitting into evidence the defendant's MySpace postings. The postings constituted "classic evidence of bad character" and were inadmissible under Fed. R. Evid. 404(b). However, given the overwhelming evidence of the defendant's guilt, the error was harmless.

#Trial-Related

United States v. Pierce, 785 F.3d 832 (2d Cir.), *cert. denied*, 136 S. Ct. 172 (2015)

The defendants appealed their convictions for various offenses arising out of their membership in a violent street gang. Among other things, defendant Colon challenged the admission of an incriminating rap video and images of tattoos posted on a third person's Facebook page secured pursuant to a 2703(d) order. Colon argued that the SCA was unconstitutional because it did not permit him to obtain like content. However, his attorney had received the content of the page through a private investigator. The Court of Appeals rejected the argument: "Colon possessed the very contents he claims the SCA prevented him from obtaining, and his suggestion that there could have been additional exculpatory material in the *** [content] is purely speculative."

#Miscellaneous

#Trial Related

#Social Media

United States v. Pineda-Moreno, 591 F.3d 121 (9th Cir. 2010), *vacated*, 565 U.S. 1189 (2012)

The Government installed mobile tracking devices on the defendant's vehicle while it was parked on a public street, in a public parking lot, and his driveway. The government used the information to track the defendant from a marijuana field. The defendant entered a conditional guilty plea to manufacturing marijuana after the district court denied his motion to suppress. On appeal, the defendant argued that his Fourth Amendment rights were violated. The Court of Appeals held that the defendant's vehicle was within the curtilage of his home when two devices were installed. However, since he took no steps to exclude the public from the driveway, the defendant had no reasonable expectation of privacy in it. The court also held that the defendant had no reasonable expectation of privacy when his vehicle was parked in public spaces. Finally, distinguishing *Kyllo v. United States* (which considered the use of thermal imaging technology to "search" with the cartilage of a home), the court rejected the argument that the use of "new" technology to track the location of the defendant's vehicle was a impermissible search. The court took note that several state Supreme Court decisions reached the opposite conclusion under their respective state constitutions. Judgment was later vacated by the U.S. Supreme Court, and the case remanded to Ninth Circuit for further consideration in light of *United States v. Jones,* 132 S.Ct. 945 (2012).

#Fourth Amendment Warrant Required or Not

United States v. Powell, 847 F.3d 760 (6th Cir. Feb. 6, 2017)

The defendants were convicted of narcotics distribution-related offenses. They argued on appeal, among other things, that the district court had erred in denying their motions to suppress evidence derived from "(1) the collection of cellular- phone identification and location information; (2) the use of a GPS tracking device; and (3) the monitoring of video cameras installed on nearby utility poles." The Court of Appeals affirmed the denial of the motions. It held that two of the three defendants had standing to assert alleged Fourth Amendment violations based on their co-ownership of relevant cell phones and other things. A third defendant argued that he had standing to challenge his arrest as the "fruit of the poisonous tree" of evidence illegally obtained from the GPS tracking and surveillance of the other defendants but the Court of Appeals declined to address his standing because the evidence was secured legally. The Court of Appeals then held that probable cause existed for the issuance of the warrant for CSLI and rejected the defendants' argument that allegedly material information had been omitted from the supporting affidavit. The Court of Appeals then applied the good faith exception to evidence derived from warrantless tracking of a vehicle because the law enforcement reasonably relied on then-binding circuit precedent. Finally, the Court of Appeals held that the defendants had no reasonable expectation in video monitoring because there was neither physical intrusion nor violation of any reasonable expectation of privacy.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. Qadri, Cr. No. 06-00469 DAE (D. Haw. Mar. 9, 2010)

One defendant moved (a second time) to dismiss the indictment and superseding indictment for violation of the Speedy Trial Act. The defendant had been charged with, among other things, wire fraud. The indictments came nearly three years apart. ESI from other thirty hard drives and three servers was in issue. Although the Government did not respond to defense communications about production "expeditiously," the Government did produce a substantial number of documents and copied the hard drives for the defendant. There also appeared to be a problem with the defendant's ability to review the content of the servers. The defendant had consented to various continuances and had not established prejudice. The court denied the motion: "It appears that the delay in this case may be attributed at least in part to the nature of electronic discovery, the complex nature of the alleged crimes, and the necessity of

coordinating various branches of government in the investigation." The court also denied the defendant's request for an evidentiary hearing.

#Discovery Materials

United States v. Ransfer, 743 F.3d 766 (11th Cir. Jan. 28, 2014), *Opinion Revised and Superseded,* 749 F.3d 914 (11th Cir. 2014), *cert. denied*, *Hanna v. United States*, 135 S. Ct. 392 (2014)

The defendants were convicted of robberies under the Hobbs Act and other crimes. They appealed, challenging, among other things, "the admission of evidence resulting from the installation and use of a GPS tracking device without a warrant to determine the location of a Ford Expedition that was used in the commission of several robberies." An informant led the police to several of the defendants and the investigation established the use of the vehicle in the robberies.

The Court of Appeals affirmed. Prior to *United States v. Jones,* binding precedent in the Eleventh Circuit established that the warrantless installation of an electronic tracking device on a vehicle did not violate the Fourth Amendment when the police had reasonable suspicion. "There is no doubt of reasonable suspicion *** based on the thorough police investigation ***. Accordingly, it was reasonable for the police to rely on this long-standing, clear precedent ***."

#Fourth Amendment Good Faith Exception

***United States v. Raymond,* 2009 U.S. Dist. LEXIS (N.D. Okla. Sept. 16, 2009)**

In this child pornography prosecution, the court denied the defendant's request for access to images on a seized computer. The Government had mirror-imaged the hard drive and made the mirror image available to the defendant's expert. The expert contended that he could not locate all of the allegedly illegal images from among the 14.000 in total on the mirror image. The court held that the Adam Walsh Act superseded Fed. R. Crim. P. 16 and barred the Government from reproducing child pornography in response to a discovery request as long as materials were made "reasonably available" to a defendant. Here, the allegedly illegal images were made available for inspection by defense counsel. The court rejected the expert's suggestion that the mirror image had been stripped of metadata. The Government agreed to make available to the expert on CDs the "missing" images, although these remained in the possession of the Government. Finally, the court directed the parties to confer about Government production of redacted images for use by the defendant in subpoenaing information from Web site owners.

#Discovery Materials

United States v. Rarick, 636 F. App'x 911 (6th Cir.), *cert. denied,* 136 S. Ct. 2403 (2016)

The defendant moved to suppress evidence of child pornography found on his cell phone that was searched pursuant to a warrant after his arrest for obstructing official business and driving on a suspended license. The district court denied the motion and the defendant pled guilty but reserved his right to appeal. He argued on appeal that the warrant violated the Particularity Requirement because it was overbroad as it did not specify what electronic evidence was sought and the particular crime to which the evidence was connected. The court of appeals upheld the denial of the motion to suppress. "Certain portions of the warrant, such as the portion authorizing seizure of 'images' and 'videos,' were specifically targeted to what the officers had probable cause to search." Moreover, "[n]o evidence offered against Rarick was seized pursuant to the overbroad portions of the warrant." The court also rejected the argument that the manner of the search was unconstitutional: "we will not get involved in the minutiae of demonstrating specifically what methodologies should be taken, but will rather examine whether the search executed under the facts of this case was reasonable."

#Fourth Amendment Particularity Requirement

United States v. Rigmaiden, No. CR 08-814-PHX-DGC (D. Ariz. May 8, 2013), *reconsideration denied*, (D. Ariz. Aug. 27, 2013)

The defendant was indicted for, among other things, mail and wire fraud. He was located and arrested, in part, by tracking the location of an aircard connected to a laptop computer allegedly used to perpetrate the crimes. Having found the location, the Government secured a search warrant for a computer located there. The defendant, proceeding *pro se,* moved to suppress. The court denied the motion, concluding, among other things: (1) The defendant secured the aircard, purchased the computer and rented the location through fraud and hence could not have a objectively reasonable expectation of privacy in any of these; (2) assuming that the SCA had been violated by the Government in some way, suppression was not an available remedy any such violation; (3) historical cell-site records could be obtained under the SCA; (4) the reasoning of *United States v. Jones* did not support suppression because making calculations from cell-site data was not analogous to attaching a GPS device to a vehicle; (5) the defendant had no reasonable expectation of privacy in addresses of email messages sent from the computer that were conveyed to a third party provider; and (6) the warrant for the aircard tracking satisfied the particularity requirement of the Fourth Amendment. The district court also rejected the argument made to the defendant (and an intervenor) that, "because cell-site simulators are a new and potentially invasive technology, the government was required to

include a more detailed description in the warrant application."

#Fourth Amendment Warrant Required or Not

United States v. Riley, 858 F.3d 1012 (6th Cir. 2017) (*per curiam*)

The defendant pled guilty to being a felon in possession of a firearm but reserved his right to appeal the denial of his motion to suppress a pistol found in his hotel room. The Government had secured an order under various federal laws, including the SCA, compelling AT&T to disclose "call metadata such as inbound and outbound phone numbers and cell-site location *** data, as well as real-time tracking or 'pinging' of the latitude and longitude of Riley's phone." The tracking occurred over a seven-hour period and the defendant was arrested after a hotel clerk provided the defendant's room number. The Sixth Circuit affirmed. Relying on *United States v. Skinner* (*q.v.*), the court held that, "using seven hours of GPS location data to determine an individual's location (or a cell phone's location), so long as the tracking does not reveal information within the home (or hotel room), does not cross the sacred threshold of the home, and thus cannot amount to a Fourth Amendment search." The court observed that, if the defendant wanted to avoid detection "he could have chosen not to carry a call phone at all, or to *turn it off*." The concurring judge would have affirmed on different grounds: The defendant's Fourth Amendment argument failed because he was a fugitive subject to a valid arrest warrant and the officers had reasonable suspicion that he was in possession on the phone they were tracking.

#Fourth Amendment Warrant Required or Not

#Miscellaneous

United States v. Robinson, 781 F.3d 453 (8th Cir.), *cert. denied*, 136 S. Ct. 596 (2015).

The defendant was convicted of wire fraud and federal program theft. On appeal, he challenged, among other things, the warrantless installation of a GPS device on his vehicle in 2010. The Court of Appeals affirmed the denial of his motion. The device was installed in 2010, before *United States v. Jones* (*q.v.*) was decided. Evidence derived from the device was admissible pre-*Jones* based on then-binding Supreme Court precedent. The agents who installed the transmitter acted in objectively reasonable reliance on that precedent. The good faith exception to the Warrant Requirement applied.

#Fourth Amendment Good Faith Exception

United States v. Rubin/Chambers, Dunhill Ins. Servs., 825 F. Supp. 2d 451 (S.D.N.Y. 2011)

The defendants were indicted for crimes arising out of an alleged conspiracy to fix bids. The Government disclosed to defendants lists of transactions which it intended to use at trial as "overt acts." The Government produced ESI during discovery in searchable format and with searchable metadata. The defendants, citing *Brady,* moved to compel the Government to reproduce the ESI in categorized bunches that related to the transactions. The court denied the motion: "Here, there is no allegation of prosecutorial bad faith or that the Government has deliberately hid what it knowingly identified as Brady needles in the evidentiary haystacks of its disclosures to Defendants." Distinguishing *United States v. Salyer* (*q.v.*), the court observed that, among other things, the materials were electronic and searchable and the Government had "undertaken many additional steps to relieve some of the burden of its 'voluminous' disclosure."

#Discovery Materials

***United States v. Russian,* 848 F.3d 1239 (10th Cir. Feb. 21, 2017)**

The defendant was convicted of drug- and gun-related offenses. On appeal, he challenged, among other things, the denial of his motion to suppress evidence derived from the search of two cell phones seized at the time of his arrest. The Court of Appeals held that the warrant was invalid because it lacked particularity and was facially deficient: "Although the application requested authorization to search the two Samsung cell phones law enforcement had seized at the time of Russian's arrest and certain data that might be found on them, the warrant itself merely authorized a search of Russian's arrest and certain data that might be found on them, the warrant itself merely authorized a search of Russian's residence and seizure of any cell phones found inside. The warrant did not identify either of the phones that were already in law enforcement's custody, nor did it specify what materials *** law enforcement was authorized to seize." However, the Court of Appeals held that the good faith exception to the exclusionary rule applied because the officer who conducted the search acted in objectively reasonable reliance on the warrant and that, in any event, any error was harmless beyond a reasonable doubt. The Court of Appeals also rejected the defendant's suggestion that it should require law enforcement to specify an *ex ante* search protocol: "we note that, like other circuits, we have previously declined to require a search protocol for computer searches, since courts are better able to assess the reasonableness of search protocols ex post ***."

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Good Faith Exception

#Fourth Amendment Particularity Requirement

United States v. Saboonchi, 990 F. Supp. 2d 536 (D. Md. 2014), *reconsideration denied*, 48 F. Supp. 3d 815 (D. Md. 2014)

The defendant was indicted for unlawful export to an embargoed country and conspiracy. The defendant and his wife had been stopped in New York State on their return from a day trip to Canada. Electronic devices were seized and later imaged by the Government. The images were "forensically searched using specialized software" in Maryland while the devices were returned. The defendant moved to suppress, arguing that the warrantless border search and the later forensic search were unconstitutional. The court denied the motion, reasoning that, although "a forensic search of an electronic device seized at the border cannot be performed absent reasonable, articulated suspicion," and the Government made such a showing.

The defendant moved for reconsideration after *Riley v. California* was decided. The court denied that motion by Memorandum Opinion filed July 28, 2014, because the "border search exception" to the Warrant Requirement remained viable after *Riley*.

#Fourth Amendment Warrant Required or Not

United States v. Salyer, Cr. No. S-10-0061 LKK [GGH] (E.D. Cal. Apr. 18, 2011), *adopting report and rec.*, No. CR. S-10-061 LKK (E.D. Cal. May 12, 2011)

In this white-collar prosecution, where the Government collected gigabytes of ESI and storage containers full of paper over a five-year period, the court exercised its case management powers to require the Government to identify *Brady* and *Giglio* materials. On a motion for reconsideration, the court rejected the Government's argument that identification would compel disclosure of protected work product. The court also rejected the Government's "open file" argument, as the defendant was a detained individual, had a "relatively small defense team," and did not have access to "corporate assistance" in searching the voluminous information, although the defendant did have an obligation to "help himself in ascertaining information favorable to himself." The court did, however, modify the "logistics of implementation" based on a burden argument raised by the Government.

#Discovery Materials

United States v. Schesso, 730 F.3d 1040 (9th Cir. 2013)

This was an interlocutory appeal from an order suppressing evidence derived from a search of

the defendant's computer equipment and digital storage devices. The defendant was charged with various federal child pornography-related crimes. The warrant had been issued by a Washington State judge based on an affidavit from a Vancouver detective and was executed at the defendant's home in Washington. In granting the relief sought, the district judge emphasized that, "the warrant application failed to include any of the protocols for searching electronic records suggesting by the concurring opinion" in *United States v. ComprehensiveDrug Testing, Inc.,* 621 F.3d 1162 (9th Cir. 2010) (*en banc*). A Ninth Circuit panel reversed.

After concluding that probable cause existed for the issuance of the warrant, the court addressed whether, "the electronic data search guidelines laid out in the *CDT* cases affect the outcome here." The court distinguished the facts before it from those in *CDT* and *United States v. Tamara,* 694 F.2d 591 (9th Cir. 1982):

"Schesso's situation is unlike *CDT III* and *Tamura* in that the government properly executed the warrant, seizing only the devices covered by the warrant and for which it had shown probable cause. Based on the evidence that Schesso possessed and distributed a child pornography video on a peer-to-peer file-sharing network, law enforcement agents had probable cause to believe that Schesso was a child pornography collector and thus to search Schesso's computer system for any evidence of possession of or dealing in child pornography. In other words, Schesso's entire computer system and all his digital storage devices were suspect.

Tellingly, the search did not involve an over-seizure of data that could expose sensitive information about other individuals not implicated in any criminal activity—a key concern in both the per curiam and concurring opinions of *CDT III*—nor did it expose sensitive information about Schesso other than his possession of and dealing in child pornography. Indeed, inclusion of the search protocols recommended in the *CDT III* concurrence would have made little difference for Schesso. For example, the concurrence recommends that the government forswear reliance on the plain view doctrine, or have an independent third party segregate seizable from non-seizable data.

***. Here, officers never relied on the plain view doctrine; they had probable cause to search for child pornography, and that is precisely what they found. The seized electronic data was reviewed by Investigator Holbrook, a specialized computer expert, rather than Detective Kennedy, the case agent, and Schesso does not assert that Holbrook disclosed to Kennedy 'any information other than that which [was] the target of the warrant.' ***. Additionally, unlike the concern articulated in the concurrence in *CDT III,* which stated that the affidavit created the false impression that the data would be lost if not seized at once, here the affidavit explained that individuals who possess, distribute, or trade in child pornography 'go to great lengths to conceal and protect from discovery their collection of sexually explicit images of minors'

[footnotes and citations omitted]."

The Court of Appeals did, however, offer further "guidance" on protocols:

"Although we conclude that the exercise of 'greater vigilance' did not require invoking the *CDT III* search protocols in Schesso's case, judges may consider such protocols or a variation on those protocols as appropriate in electronic searches. We also note that Rule 41 of the Federal Rules of Criminal Procedure sets forth guidance for officers seeking electronically stored information. Ultimately, the proper balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures of electronic data must be determined on a case-by-case basis. The more scrupulous law enforcement agents and judicial officers are in applying for and issuing warrants, the less likely it is that those warrants will end up being scrutinized by the court of appeals [footnote 119

omitted]."

Finally, the court that, "[e]ven if the warrant were deficient, the officers' reliance on it was objectively reasonable and the 'good faith' exception to the exclusionary rule applies. The Court of Appeals deferred to the state judge's probable cause determination and the objectively reasonable reliance of law enforcement on the warrant. Further, its analysis was not affected by the decision to seek a warrant from a State, rather than a federal judge.

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Good Faith Exception

***United States v. SDI Future Health Inc*., 568 F.3d 684 (9th Cir. 2009)**

On this appeal from an order granting a motion to suppress evidence seized pursuant to a search warrant, the Court of Appeals addressed when employees have standing to challenge searches of corporate premises: "except in the case of a small, family-run business over which an individual exercises daily management and control, an individual challenging a search of workplace areas beyond his own internal office must generally show some personal connection to the places searched and the materials seized." The Court of Appeals remanded for further fact-finding. Turning to the corporation's challenge to the warrant, the Court of Appeals held that the warrant had incorporated the supporting affidavit by reference, that the affidavit "accompanied" the search, and that the warrant satisfied the particularity requirement. The court did, however, sustain the invalidity of the warrant on overbreadth grounds as to, among other things email: There was no limitation placed on the email to be searched. The court also rejected the Government's reliance on "good faith" and held that the district court should have

severed the unconstitutional portions of the warrant and allowed only partial suppression.

#Fourth Amendment Particularity Requirement

United States v. Sember, 170 F. Supp. 3d 1049 (S.D. Ohio 2016)

The defendant had been found not guilty of theft of government property. The government sought leave to destroy and dispose of an external hard drive and four notebooks seized from the defendant's home. Ownership of the drive and "its alleged 'contraband' nature" was in dispute. The defendant objected to destruction of the drive. Since the defendant "indicated that the data on the ***drive might be relevant to future litigation, the Government is not permitted to destroy it." The court ordered that the drive "in its current condition" be transferred to the clerk of the court until further order to forestall additional disputes should the data be altered while in the government's possession.

#Discovery Materials

#Preservation and Spoliation

United States v. Serrano, 16-cr-00169-WHP (S.D.N.Y. July 18, 2017)

The defendant was involved in a physical assault in an apartment after which State law enforcement seized ammunition and a bullet vest from that apartment. Months later, he was arrested on federal charges of being a felon in possession of ammunition and a violent felon in possession of body armor. Thereafter, the defendant turned over his cell phone and identified the apartment as his residence. The Government then secured an order under the SCA that directed the defendant's cell service provider to turn over historical CSLI for a *period beginning ten months before the assault and through the date of the order*. He moved to suppress, arguing that his Fourth Amendment rights had been violated. The district court denied the motion, finding that the defendant voluntarily provided his location to the provider and had no legitimate expectation of privacy in it. The court also relied on the fact that there was no disclosure of content of any conversation and that the CSLI only disclosed location information. The court rejected the defendant's argument that the time period of the order was overbroad because the defendant had made an "apparent attempt to disassociate himself from the location" such that the Government's request to ascertain his location prior to the assault was proper.

#Fourth Amendment Warrant Required or Not

#SCA

United States v. Shah, **No. 5:13-CR-328-FL (E.D.N.C. Jan. 6, 2015)**

The defendant was indicted for intentional damage to a protected computer. He moved to suppress evidence of cell phone location secured from AT&T, user location from Facebook, and email and associated data from Google. The "location" evidence was secured pursuant to 2703(d) orders and the Google evidence pursuant to a search warrant. The district court found that the defendant had no reasonable expectation of privacy in the location evidence. As to the Google-derived evidence, the court agreed with the defendant that "the warrant's terms failed to provide the necessary particularity because they failed to state the particular crime for which the evidence was being sought. Nevertheless, the evidence is admissible because officers 'acted in good faith' in relying on the *** warrant." The court also found that the "two-step" procedure described in the warrant for the search of email was constitutional and that there was no basis to impose a "minimization" procedure on the search of the Google email and data.

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Good Faith Exception

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

#Social Media

United States v. Sharp, **No. 1:14-CR-227-TCB (N.D. Ga. Aug. 4, 2015)**

The defendant moved to suppress evidence derived from the search of the mirror image of a hard drive. He consented to the search but revoked his consent after the Government had begun its review. The court denied the motion, holding that the defendant had no reasonable expectation of privacy in the mirror image once it had been obtained.

#Fourth Amendment Warrant Required or Not

United States v. Sivilla, **714 F.3d 1168 (9th Cir. 2015)**

The defendant was arrested after an inspection of his vehicle at a border crossing from Mexico revealed heroin inside the engine manifold. An agent took poor quality photographs of the engine area and the cocaine and preserved the latter but despite a preservation order the vehicle was sold at auction and stripped for parts. Moreover, a person to whom the defendant

had loaned the vehicle shortly before had been murdered. The district court denied the defendant's motion to dismiss or for a jury instruction but allowed defense counsel to "explore the facts regarding the failure to preserve the vehicle during trial." The jury returned a guilty verdict. The Court of Appeals held that the exculpatory value of the vehicle was not apparent and the Government had not acted in bad faith. Hence, there had been no constitutional violation. However, the district court abused its discretion when it rejected an adverse inference instruction because "the quality of the government's conduct was poor" and there was significant prejudice to the defendant. The case was remanded for a new trial with a remedial instruction to be given.

#Preservation and Spoliation

United States v. Skilling, 554 F.3d 529 (5th Cir. 2009), aff'd in part, vacated in part, and remanded, 561 U.S. 358 (2010)

In this appeal from a conviction for, among other things, tax fraud, the defendant argued that the Government "dumped" an enormous volume of electronic information (several hundred million pages) on him in an attempt to conceal *Brady* material. The Government had provided the defendant with an "open file [that] was electronic and searchable." It also provided a list of "hot documents," created indices, and gave the defendant access to databases. Moreover, the case was complex and there was no evidence of wrongful conduct. Under these circumstances, the court held that the use of the open file did not violate *Brady.*

#Discovery Materials

***United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), *cert. denied*, 133 S. Ct. 2851 (2013).**

The defendant was convicted of drug trafficking and conspiracy. On appeal, he challenged, among other things, the denial of his motion to suppress evidence obtained from the search of his vehicle. The DEA had secured an order that authorized a telephone company to release GPS information that was used to track the defendant. The Court of Appeals affirmed. The court held that the defendant had no reasonable expectation of privacy "in the data given off by his voluntarily procured pay-as-you go cell phone." The court relied on *United States v. Knotts,* 460 U.S. 276 (1983), and distinguished the facts before it from those in *United States v. Jones* (*q.v.*): Unlike *Jones,* there was no "physical intrusion" of the defendant's vehicle and the defendant was tracked for only three days.

#Fourth Amendment Warrant Required or Not

***United States v. Sparks,* 711 F.3d 58 (1st Cir.), *cert. denied*, 134 S. Ct. 204 (2013)**

The defendant was suspected of committing bank robberies. To track the defendant, the FBI placed a GPS device in his vehicle, tracked the vehicle to the scene of a bank robbery, and used the device to locate the vehicle. The defendant moved to suppress the fruits of the warrantless search, relying on *United States v. Jones.* The trial court denied the motion. Declining to address *Jones,* which was decided after the trial court had ruled, the Court of Appeals held that the good faith exception applied: "at the time of the GPS surveillance in this case, settled, binding precedent *** authorized the agents' conduct."

[Note this observation: The "good-faith exception is not a license for law enforcement to forge ahead with new investigative methods in the face of uncertainty as to their constitutionality. 'The justifications for the good-faith exception do not extend to situations in which police officers have interpreted ambiguous precedent or relied on their own extrapolations from existing caselaw'" (citation omitted)].

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

United States v. Sparks, 806 F.3d 1323 (11th Cir. 2015), *cert. denied*, 136 S. Ct. 2009 (2016).

The defendants pled guilty to possession of child pornography but reserved their rights to appeal the denial of motions to suppress evidence derived from searches of their cell phone. The Eleventh Circuit affirmed:

Defendants-Appellants['] *** day did not start well for them. They left their cell phone at a Walmart store. But this wasn't just any cell phone; Johnson and Sparks's phone stored hundreds of images and videos of child pornography that they had made using Sparks's friend's four-year-old child—and Johnson was already a registered sex offender. So Defendants must have felt pretty relieved when they learned that Linda Vo, an employee of the Walmart where Defendants left their phone, had found it and that she agreed to return it.

But Vo decided to look at the contents of the phone, which were not password-protected, after speaking with Sparks and before actually meeting her. Upon discovering the images of child pornography, Vo resolved not to return the phone. Instead, unbeknownst to Defendants, she arranged for it to be turned over to law enforcement.

When Vo failed to meet Sparks with the phone as the two had previously agreed, Defendants knew how to find Vo to get their phone back. But Defendants did not return to their Walmart store and look for Vo. Nor did they ask for Walmart's assistance in obtaining their phone, found in its store, by its employee. They also did not file a report with Walmart or the police complaining that Vo would not return their phone, despite their requests. Instead, they made a conscious decision to stop pursuing the phone, even though they knew how to get it back with reasonable effort.

That decision—whether because Defendants hoped that Vo would not report them if they did not continue to seek the phone or because Defendants simply thought recovery of the phone was not worth their reasonable effort—can be viewed only as a deliberate decision to abandon the phone. Because Defendants abandoned their phone within three days of having lost it, they lack standing to challenge law enforcement's 23-day delay between recovering the phone and obtaining a search warrant to search it.

As for searches conducted within the three-day period before Defendants abandoned their interest in the phone, we find no reversible error in the district court's denials of Defendants' suppression motion. ***.

#Fourth Amendment Warrant Required or Not

***United States v. Stagliano*, 693 F. Supp. 2d 25 (D.D.C. 2010)**

The defendants were indicted for various obscenity-related offenses arising out of the use of an "interactive computer service." They challenged the statutes under which they were indicted on constitutional grounds. Rejecting the challenges, the court held, among other things, that the use of "community standards" did not render the statutes substantially overbroad. In so doing, the court declined to follow *United States v. Kilbride.* The court also rejected that the argument that the defendants had a right to "publish" (rather than merely possess) obscene materials.

#Miscellaneous

***United States v. Stanley*, 753 F.3d 114 (3d Cir.), *cert. denied*, 135 S. Ct. 507 (2014)**

A police investigator discovered a computer on a peer-to-peer network sharing files that he suspected contained child pornography. The investigator secured the computer's IP address as well as subscriber information. The investigator executed a search warrant on the subscriber's home but found no child pornography. The investigator surmised that "the computer sharing child pornography was connecting wirelessly to the *** [subscriber's] router from a nearly

location without the ***[subscriber's] knowledge or permission." Thereafter, the investigator used a "MoocherHunter" device to trace the other computer to the interior of the defendant's home. He secured a search warrant for the home and seized a computer containing image of child pornography. The defendant was indicted and moved to suppress the evidence secured from his home, arguing that the investigator "conducted a warrantless search under *Kyllo v. United States* *** when he used the MoocherHunter to obtain information about the interior of his home that was unavailable through visual surveillance." The district court denied the motion and the defendant pled guilty. On appeal, he challenged the denial of his motion.

The Court of Appeals affirmed: "Stanley made no effort to confine his conduct to the interior of his home. In fact, his conduct—sharing child pornography with other Internet users via a stranger's Internet connection—was deliberately projected *outside* of his home, as it required interactions with persons and objects beyond the threshold of his residence. In effect, Stanley opened his window and extended an invisible, virtual arm across the street ***. In so doing, Stanley deliberately ventured beyond the privacy protections of the home, and thus, beyond the safe harbor provided by *Kyllo."*

#Fourth Amendment Warrant Required or Not

***United States v. Stephens,* 764 F.3d 327 (4th Cir. 2014), *cert. denied*, 136 S. Ct. 43 (2015)**

In the course of an investigation, a Baltimore police officer, who had been deputized as a federal agent attached a GPS device to the defendant's vehicle and tracked him for several weeks in 2011 without a warrant. The vehicle was tracked to a particular location, the defendant was subjected to a pat-down, and the vehicle searched after a dog alerted to a weapon. *United States v. Jones* was decided while the action was pending in the district court. The defendant moved to suppress on the basis of *Jones*. The motion was denied and the defendant entered a conditional guilty plea. On appeal, he challenged the denial of his motion. The Court of Appeals affirmed. It accepted the district court's ruling that the warrantless use of the GPS was a Fourth Amendment violation. It also held that the good-faith exception to the Warrant Requirement applied given federal and Maryland case law in 2011.

The dissent objected to the majority's conclusion because, in its view, there was no binding appellate precedent in 2011, the law was unsettled, and no exigent circumstances existed.

#Fourth Amendment Good Faith Exception

***United States v. Stimler,* 864 F.3d 253 (3d Cir. July 7, 2017)**

The defendants were convicted of conspiracy to commit kidnapping. One argued on appeal, among other things, that the trial court had erred in denying his motion to suppress evidence derived from an order issued under Section 2703(d) of the SCA that compelled AT&T to turn over historical CSLI generated by his phone over a 57-day period. The Third Circuit began its discussion by reference to *In re Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government,* 620 F.3d 304 (3d Cir. 2010), in which the court "rejected the applicability of the third-party doctrine to CSLI, holding that the transmission of CSLI was not truly voluntary" but held that "the SCA's disclosure regime did not violate the Fourth Amendment because individuals lack a reasonable expectation of privacy." Both the Government and the defendant argued that the Court of Appeals was not bound by this binding precedent because "intervening legal developments have undercut the decisional rationale" of *In re Application.* The panel disagreed, rejecting, among other things, the defendant's reliance on *Jones v. United States* (*q.v.*) and *Riley v. California* (*q.v*.). *Riley* addressed the protection of content, which is not acquired by CSLI, and J*ones* addressed GPS tracking, which is more intrusive on privacy rights given that its accuracy is greater than CSLI. One judge disagreed, concluding that the "shadow majority" in *Jones* was a sufficient intervening development and that the distinction between GPS and CSLI had "nearly disappeared" since *in re Application* was decided.

#Fourth Amendment Warrant Required or Not

#SCA

#Third-Party Doctrine

United States v. Stratton, 229 F.Supp.3d 1230 (D. Kan. Jan. 17, 2017)

The defendant alleged that Sony Computer Entertainment America, LLC ("Sony"), violated his Fourth Amendment rights when it searched information on his PlayStation3 gaming device and reporting its findings of suspected child pornography to the National Center for Missing and Exploited Children and law enforcement, which led to searches of his electronic communications and his residence. He moved to suppress evidence derived from the searches, arguing that Sony "acted as a government agent" when it conducted the searches. The court denied the motion. First, "[n]othing in the evidence suggests that Sony was acting to pursue anything other than its own interests when it *** sent information to the NCMEC." Second, "[n]o evidence suggests that NCMEC exceeded the scope of Sony's private search." Third, the defendant had no reasonable expectation of privacy in any communications he made once these were received by other users of the gaming device or in images he had downloaded because Sony's terms of service authorized it to monitor online activity and cautioned users that Sony might turn over evidence of illegal activity to law enforcement. Finally, the court

found that the good faith exception to the exclusionary rule applied even if there had been a Fourth Amendment violation.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. Suarez, Criminal Action No. 09-932 (JLL) (D.N.J. Oct. 21, 2010)

Ruling on the defendants' motion to suppress or for an adverse inference instruction, the court found that the Government had failed to issue a litigation hold, as a result of which certain text messages between a cooperating witness and FBI agents had been deleted. The court also found that the deleted messages *could* have constituted Jencks Act material and should have been preserved. The court held that suppression of related evidence was unwarranted, as the Government had not acted in bad faith and there was no evidence that the deleted messages "clearly contained exculpatory material." The court did, however, agree to issue an adverse inference instruction and, to do so, "consult[ed] the more thoroughly developed civil case law on the subject." Applying a four-part test articulated in *Mosaid Tech. Inc. v. Samsung Elec. Co.,* 348 F. Supp. 2d 332 (D.N.J. 2004), the court found that the Government had "control" over the messages, that there was "actual suppression or withholding" of the messages, that the deleted messages were relevant, and that it was reasonably foreseeable that the messages would be discoverable. The court also relied on *Pension Comm. v. Banc of America Sec.,* 685 F.Supp.2d 456 (S.D.N.Y. 2010), in framing the instruction.

#Discovery Materials

United States v. Swartz, 945 F.Supp.2d 216 (D. Mass. 2013)

The defendant in this criminal action had been indicted for allegedly attempting to download certain archived materials through a MIT computer network. He committed suicide and the charges were dismissed. Between the indictment and the dismissal, the district court barred the defendant from disclosing documents discoverable under Criminal Rule 16 to anyone other than potential witnesses. After the suicide, media interest "escalated" and a congressional investigation commenced. Threats and harassing incidents, including hacking, occurred. The defendant's estate moved to modify the protective order pursuant to Criminal Rule 16(d) to allow it to release documents to Congress and the public. The victims of the defendant's alleged crimes intervened to oppose modification. The Government, the estate, and the victims agreed that some modification was appropriate, but disputed whether names and identifying information of certain individuals, including law enforcement personnel, should be disclosed.

The district court held that, (1) it was "appropriate to analyze the 'good cause' requirement to [modify a protective order] under the criminal rules in light of precedent analyzing protective orders in civil cases," (2) the interests of the third-party victims bore "particular emphasis," and (3) the presumptive right of access did not attach to criminal discovery materials. Applying the "good cause" test, the district court found that, "the estate's interest in disclosing the identity of individuals named in the production, as it relates to enhancing the public's understanding of the investigation and prosecution ***, is substantially outweighed by the interest of the government and the victims in shielding their employees from potential retaliation." The district court also allowed MIT to redact information related to weaknesses in its computer network and modified the order so that the estate could "disclose discovery materials in its possession after redaction of the identity of individuals and sensitive network information."

#Trial Related

United States v. Szymuszkiewicz, 622 F.3d 701 (7th Cir. 2010)

The defendant had modified a "rule" on his supervisor's email account so that copies of email sent to her were automatically sent to the defendant. On an appeal from his conviction under the Wiretap Act, the Court of Appeals affirmed. First, the Court of Appeals rejected the defendant's argument that he should have been charged under the SCA: "It is risky to defend against one crime by admitting another." The Court of Appeals then discussed the concept of "package switching" (by which email is routed from sender to recipient) and concluded that there had been an "interception" under the Wiretap Act. The Court of Appeals also held that the interception in issue was contemporaneous with the email, but rejected the incorporation of a "contemporaneous" requirement into the Wiretap Act that had been adopted by other Courts of Appeals.

#Miscellaneous

United States v. Thielemann, 575 F.3d 265 (3d Cir. 2009), *cert. denied*, 558 U.S. 1133 (2010)

The Court of Appeals affirmed the imposition of special conditions on a convicted child pornographer. The conditions banned the defendant from possessing or viewing adult sexually explicit material and also restricted him from owning or operating a personal computer with Internet access anywhere without permission.

#Miscellaneous

United States v. Thomas, 818 F.3d 1230 (11th Cir.), *cert. denied,* 137 S. Ct. 171 (2016)

On appeal, the Eleventh Circuit agreed with the district court that third-party consent by the defendant's wife was valid because it was obtained before the defendant objected. Additionally, the couple shared the password to access the computer. Therefore, the wife had apparent control and authority over the computer. The court also found that the evidence would have been validly obtained, absent consent, under the independent source doctrine. The officers observed incriminating evidence in plain view on the computer.

#Preservation and Spoilation

#Fourth Amendment Warrant Required or Not

United States v. Thomas, Nos. 5:12-cr-37, 5:12-cr-44, 5:12-cr-97 (D. Vt. Nov. 8, 2013), *aff'd,* 788 F.3d 345 (2nd Cir. 2015), *cert. denied*, 136 S. Ct. 848 (2016)

The defendants were charged with possession of child pornography. They moved to suppress all evidence derived from searches of their residences, arguing that the search warrant applications contained inaccuracies and omitted facts and that the warrants were derived from warrantless automated searches of private information. After an evidentiary hearing, the district court denied the motions, finding that the defendants had no reasonable expectation of privacy in files shared on peer-to-peer sites:

"The affidavits state that a law enforcement officer performed an investigation of peer-to-peer file sharing using automated software to determine whether IP addresses in his or her jurisdiction had offered to share files indicative of child pornography. Defendants argue that the software actually has the ability to access private information which Defendants did not make available for sharing. After a lengthy evidentiary hearing, there is no factual support for this claim. Instead, the evidence overwhelming demonstrates that the only information accessed was made publicly available by the IP address or the software it was using. Accordingly, either intentionally or inadvertently, through the use of peer-to-peer file sharing software, Defendants exposed to the public the information they now claim was private."

The court undertook an analysis under *Franks v. Delaware,* 438 U.S. 154 (1978), directed to technology-related statements included in (or omitted from) the search warrant applications and found that, as to a few statements that required further analysis, (1) "there is ample evidence of subjective and objective good faith and reasonableness" and, (2) even discounting any erroneous information or correcting material omissions, there was ample evidence to support the existence of probable cause. The court also found that, in any event, the good cause exception to the exclusionary rule would apply.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

United States v. Thomas, 788 F.3d 345 (2d Cir. 2015)

Law enforcement personnel were investigating possible child pornography committed through peer-to-peer file-sharing software. To do so officers automated the process of canvassing the peer-to-peer networks and officers were trained on the process. The defendant was located through the process. The affidavit submitted in support of a warrant described the process only in general terms. The defendant was indicted for production of child pornography and, after his motions to suppress were denied, entered a conditional plea. "The question presented is whether a search warrant affidavit that relied upon evidence generated by an automated software program provided a substantial basis for a magistrate judge's conclusion that there was probable cause that child pornography would be found on the defendant's computer." The Court of Appeals affirmed. The affidavit sufficiently described the software and found no error in the district court's finding that the software was reliable. The Court of Appeals also rejected the argument that law enforcement must secure a second warrant to search a specific computer within an otherwise searchable area.

#Fourth Amendment Warrant Required or Not

United States v. Thomas, No. 3:15CR80 (E.D. Va. Oct. 13, 2015)

The defendant was indicted for conspiracy to conduct robberies in violation of the Hobbs Act. Evidence against him included CSLI obtained over a 133-day period pursuant to a Section 2703(d) order. The defendant moved to suppress, arguing that the order violated his Fourth Amendment rights. The court was bound by *United States v. Graham,* 796 F.3d 332 (4th Cir. 2015), which held that long-term collection of CSLI was unreasonable under the Fourth Amendment, However, the court did not determine whether the collection at issue was unreasonable because the good faith exception to the Warrant Requirement applied: The officers relied on a statute which, at the time, "had not been found, in binding appellate precedent," to be unconstitutional. They also relied on an order that was not facially deficient and had been issued by a "neutral and detached" magistrate judge.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. Ulbricht, 858 F.3d 71 (2d Cir. May 31, 2017)

The defendant was convicted of drug trafficking and other crimes arising out of his creation and operation of Silk Road, an online marketplace whose users primarily purchased and sold illegal goods and services. He argued on appeal, among other things, that the trial court had erred in denying his motion to suppress evidence allegedly obtained in violation of the Fourth Amendment. The Government had secured five pen/trap orders that authorized law enforcement to collect IP address data for Internet traffic to and from the defendant's home wireless router and other devices regularly connected to the router. The orders did not permit access to any content. On the day of his arrest the Government secured a warrant allowing him to search his laptop. The Second Circuit held that collecting IP address information without content was "precisely analogous to the capture of telephone numbers in *Smith* [*v. Maryland*]" because the defendant had no legitimate privacy issue. It also rejected his arguments that the orders might allow access to content by tracking metadata and allowed impermissible monitoring activity in his home. The Second Circuit also rejected the defendant's argument violated the Particularity Requirement:

> The fundamental flaw in Ulbricht's *** argument is that it confuses a warrant's breadth with a lack of particularity. As noted above, breadth and particularity are related but distinct concepts. A warrant may be broad, in that it authorizes the government to search an identified location or object for a wide range of potentially relevant material, without violating the particularity requirement. For example, a warrant may allow the government to search a suspected drug dealer's entire home where there is probable cause to believe that evidence relevant to that activity may be found anywhere in the residence. Similarly, '[w]hen the criminal activity pervades [an] entire business, seizure of all records of the business is appropriate, and broad language used in warrants will not offend the particularity requirements.' ***. Ulbricht used his laptop to commit the charged offenses by creating and continuing to operate Silk Road. Thus, a broad warrant allowing the government to search his laptop for potentially extensive evidence of those crimes does not offend the Fourth Amendment, as long as that warrant meets the three particularity criteria outlined above.

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

United States v. Valas, 822 F.3d 228 (5th Cir. 2016)

Defendant appealed his conviction for engaging in a commercial sex act with a minor in violation of 18 U.S.C. 1591. The Fifth Circuit concluded that the district court properly instructed the jury on §1591's scienter requirements and did not abuse its discretion in denying defendant's motion for a mistrial because the court found no Brady violation. Additionally, the

district court did not abuse its discretion in denying an alibi instruction or in denying defendant's request for a spoliation instruction. The court rejected defendant's claims regarding the admissibility of rebuttal evidence regarding government statements during closing arguments; and concluded that there is no cumulative error.

#Trial Related

#Preservation and Spoilation

#Miscellaneous

United States v. Valle, 807 F.3d 508 (2d Cir. 2015)

The defendant, a NYPD officer, was convicted of violating the Computer Fraud and Abuse Act. He used his access to NYPD databases for addresses and other personal information for his violent sexual fantasies. On appeal, the defendant's conviction was reversed because he had authorized access rights to the databases and the statutory phrase, "exceeding authorized access," was inapplicable to him.

#Miscellaneous

NOTE: THIS DECISION WIDENS CIRCUIT SPLIT ON INTERPRETATION OF "EXCEEDING AUTHORIZED ACCESS" IN COMPUTER FRAUD AND ABUSE ACT.

United States v. Vaughn, No. CR 14-23 (JLL) (D.N.J. Nov. 10, 2015)

The defendant moved to dismiss the Indictment because the Government failed to certain preserve text messages. The Government conceded that it had a duty to preserve and failed to do so but contested the remedy. The court declined to dismiss the indictment but precluded the Government from using *any* text messages in its case: "Precluding only the text messages between law enforcement and the CW ***, provides an inadequate incentive for the Government to exercise appropriate diligence in the future, both in complying with preservation polices [*sic*] and in making representations to the Court and following its orders (footnote omitted)." The court also reserved to trial whether it would give an adverse inference instruction.

#Preservation and Spoliation

#Trial-Related

United States v. Voneida, 337 F. App'x. 246 (3d Cir. 2009)

The defendant was convicted of transmitting a threatening communication in interstate commerce after posting statements on his Myspace page. In affirming the conviction, the Court of Appeals rejected the defendant's argument that the statements had not been transmitted "because his postings were more like a hand-written diary." The court also rejected the argument that his postings were protected speech and that the prosecutor's reference to the Virginia Tech shootings (which happened several days before the postings) was *unduly* prejudicial.

#Trial Related

United States v. Vosburgh, 602 F.3d 512 (3d Cir. 2010), *cert. denied*, 563 U.S. 905 (2011)

This was an appeal from a conviction for possession of child pornography. At its center was an "underground Internet message board." The board did not host child pornography but, instead, directed users to where child pornography could be found on the Internet. Access to the board was relatively difficult: "It is highly unlikely that an innocent user of the Internet would stumble across ... [the site] through an unfortunate Google search." During a sting operation for users of the board, law enforcement came across an IP address that was traced to an ISP. In response to a subpoena, the ISP identified the defendant. When agents attempted to execute a search warrant at the defendant's residence, he destroyed various electronic media. Thereafter, agents secured a second warrant for a hard drive that they had inadvertently failed to seize the first time. "Thumbnail" images on the hard drive were introduced at trial. These images could not be accessed by the defendant. However, the Government argued that the thumbnails demonstrated that the defendant had possessed full-sized child pornographic images at some point. The Court of Appeals held that, given the unique nature of IP addresses, there was a fair probability that evidence of criminal activity would be found in the residence. The court also held that the application was not "stale," although there was a four month gap between the application and attempts to access the site, observing that computers have long memories and that those interested in child pornography "tend to hoard their materials and retain them for a long time." The court also held that the Government's reliance on the thumbnail images did not constitute an impermissible amendment of the indictment and that there was sufficient evidence to support the conviction (the defendant argued on appeal that his expert had "definitively disproved" the Government's case).

#Miscellaneous

United States v. Wallace, 866 F.3d 605 (5th Cir. May 22, 2017)

The defendant, a member of a Texas crime syndicate, was convicted of five violent felonies. He appealed from, among other things, the denial of his motion to suppress evidence obtained at the time of his arrest. The defendant had been located through a "Ping Order" issued pursuant to the federal pen-trap statute (Section 2703(d) of the Stored Communications Act) and State law that allowed law enforcement to obtain *prospective* CSLI for his cell phone and locate the defendant. The Court of Appeals affirmed. It held that suppression was not an available remedy under either federal or Texas law. The Court of Appeals also held that the defendant had no reasonable expectation of privacy in prospective CSLI. The appellate court had previously held that historical CSLI was a business record collected for business purposes by a third party and that there was no reasonable expectation of privacy in it. Because the Fifth Circuit found, in prior history, "little distinction between historical and prospective cell site data" the business record concept applied to both. In any event, suppression would be unwarranted under the good faith exception to the Warrant Requirement.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

#SCA

#Third-Party Doctrine

United States v. Warshak, 631 F.3d 266 (6th Cir. 2010)

In this appeal from convictions arising out of a "massive scheme to defraud," the Court of Appeals held that a defendant had a reasonable expectation of privacy in the content of email held by an commercial Internet Service Provider (drawing an analogy to post offices and telephone companies) and that the Government violated the defendant's Fourth Amendment rights when it secured the email from the ISP by subpoena under Section 2703(b) and *ex parte* order under Section 2703(d) of the SCA. However, the Court of Appeals concluded that an exclusionary remedy was inappropriate as the securing agents had relied in good faith on the constitutionality of the Act. The Court of Appeals observed, however, that "after today's decision, the good-faith calculus has changed, and a reasonable officer may no longer assume that the Constitution permits warrantless searches of private emails." The Government had failed to give the defendant notice of the subpoena or order, as required by Section 2703(b)(1)(B). However, the Court of Appeals rejected the defendant's argument that this weighed against good faith, as the issue was reasonable reliance in *obtaining* the email. Likewise, the Court of Appeals rejected the defendant's argument that the Government's

demand pursuant to Section 2703(f) that the ISP preserve his email *prospectively* violated the Act (although this was a subject of the concurrence). The Court of Appeals held, among other things, that the Government had acted properly in making large amounts of ESI available to the defendant. Rejecting the analogy to the Federal Rules of Civil Procedure made in *United States v. O'Keefe,* the Court of Appeals held that the Criminal Rules did not require the Government to produce ESI in a particular form, that much of the ESI was taken from computers that the defendants could access, that the defendants had an expert who could search the ESI, and the Government had given the defendants a "guide" to the ESI. The Court of Appeals also held that the Government had no obligation to "sift fastidiously" through the ESI to satisfy the Government's *Brady* obligations. Reviewing the counts on which the defendants were convicted, the Court of Appeals held, among other things, that there was sufficient evidence to conclude that a defendant had committed access-device fraud when he charged monies to customers' credit card accounts without consent. Although access to the monies in the accounts may have been "ephemeral" (the monies were credited back immediately), the defendant did "receive" the monies and that was sufficient for conviction. The Court of Appeals did reverse the convictions under several counts and remanded for resentencing on others.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009)

The Government moved to compel an ISP to comply with a subpoena and produce the contents of email sent or received by the defendant, accused of child pornography. Interpreting the SCA, the court held that, for email less than 181 days old, an ISP must comply with a subpoena if email is "held or maintained solely to provide the customer storage of computer processing services." Disagreeing with a Ninth Circuit decision, and relying on a distinction between Web-bases and other email systems," the court also held Web-based email that is *opened* and then stored is not "in storage" under the Act. Under the facts *sub judice*, the court granted the motion.

#Discovery Materials

United States v. Welch, 291 F. App'x 193 (10th Cir. 2008)

The defendant, convicted on child pornography charges, appealed the denial of motions to suppress evidence. The Government had begun drug investigations, which had "stalled" twice. In the interim, the Government learned that the defendant had operated a child pornography Website. The Government then secured a search warrant for rental premises owned by the defendant, located boxes containing drug-manufacturing materials, and made a warrantless

arrest of the defendant. The Government then secured a search warrant for the defendant's residence to search for evidence of drug manufacturing. During execution of the warrant, the Government seized *non- networked* computer equipment. During a search of the electronic information on the seized items, the Government discovered child pornography on the unallocated space on a hard drive. The Government then secured a warrant to search for child pornography. The Court of Appeals held that there was no probable cause to believe that there was evidence of a drug crime at the rental premises, because, among other things, the supporting information was "stale." However, since all the known facts could have led to a reasonable belief that the evidence might be present and there was no police misconduct, the court applied the "good faith" exception. The court then rejected the defendant's argument that the second search warrant was overbroad: The warrant allowed computers to be searched for evidence of drug manufacturing, the Government could not identify what types of computer equipment it would encounter during the search, and the Government halted the search and applied for another warrant when it found child pornography. The court also rejected a "fruit of the poisonous tree argument."

#Fourth Amendment Particularity Requirement

United States v. Williams, No. 13-cr-00764-WHO-1 (N.D. Ca. Feb. 9, 2016), *appeal filed,* No. 16-10109 (9th Cir. Mar. 11, 2016)

The government is correct that "the filing of a notice of appeal is an event of jurisdictional significance," but that event only "divests the district court of its control over those aspects of the case involved in the appeal." The government has not identified any other pending pretrial issues similar enough to those on appeal to risk this Court and the Ninth Circuit, "from stepping on each other's toes."

#Trial Related

#Miscellaneous

United States v. Wigginton, Criminal No. 6:15-cr-5-GFVT-HAI-1 (E.D. Ky. Dec. 10, 2015)

The defendant was charged with bank robbery. His debit card transactions (which placed him in the vicinity of two robberies) had been tracked over thirteen days and his real-time CSLI (used to locate and arrest him) for less than 24 hours. He moved to suppress evidence derived from this tracking. The defendant attempted to distinguish *Smith v. Maryland* because it "concerned hard copies of checks, deposit slips, and the like, none of which were able to convey the defendant's real-time location." The court rejected the attempt. The court also distinguished *United States v. Jones* because there was no physical trespass and the duration of the tracking was short-term.

#Fourth Amendment Warrant Required or Not

United States v. Williams, 592 F.3d 511 (4th Cir.), *cert. denied*, 562 U.S. 1044 (2010)

The defendant was tried on stipulated facts and found guilty of possession of an unregistered machine gun, an unregistered silence, and child pornography. He appealed from the denial of his motion to suppress evidence. The State of Virginia had secured a warrant to search for and seize evidence of threats to bodily harm and harassment by computer. During execution of the search on various media, child pornography was found. The Court of Appeals rejected the defendant's argument that the scope of the warrant was exceeded: Evidence of child pornography was relevant to the offenses for which the warrant had been issued. Moreover, evidence of child pornography fell within the plain view doctrine as the warrant authorized the *search* of the media and the subsequent *seizure* of the contraband. The court also upheld the search of a lockbox containing the machine gum and the silencer, noting that the officers were entitled to inspect these items during their search for media that could have been inside the box.

#Fourth Amendment Particularity Requirement

United States v. Winn, 79 F. Supp. 3d 904 (S.D. Ill. 2015)

The defendant used his cell phone to record teenage girls at a pool and he rubbed his genitals while doing so. Local police undertook an investigation, seized the defendant's phone with his consent, and conducted interviews. Nine days later, a detective used a template to prepare an affidavit for a warrant to search the phone. However, the warrant mistakenly identified the crime being investigated as disorderly conduct. Data was extracted from the phone that did not contain images of the girls at the pool but did contain images of child pornography. The defendant was charged with State offenses. A detective then preformed a manual search of the phone for other images of girls at the pool. The prosecution was referred to the United States Attorney and the defendant indicted on child-pornography related offenses. The defendant moved to suppress. The district court concluded: (1) The nine-day delay was "avoidable but not unreasonable;" (2) the mistaken listing of the relevant offense did not violate the Fourth Amendment as there was probable cause to search for evidence of that offense; (3) the warrant was overbroad and lacked particularity because it authorized the seizure of "any and all files" and because no time frame was specified. The district court declined to apply the good faith exception because of the general nature of the warrant and suppressed all evidence from the phone.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Particularity Requirement

Fourth Amendment Warrant Required or Not

United States v. Woerner, 709 F.3d 527 (5th Cir. 2013), *cert. denied,* 134 S. Ct. 146 2013 (2013), *rehearing denied,* 134 S. Ct. 990 (2014)

In this appeal from a conviction for possession of child pornography, the defendant challenged the denial of his motion to suppress evidence derived from an illegal search and seizure. A police officer in Illinois had been "patrolling" an Internet peer-to-peer sharing network. He located a possible suspect based on the suspect's online profile, secured access to files containing child pornography, located a physical address in Texas, and gave the information to law enforcement in Texas, which secured a warrant for the address. Although they were aware that the warrant had expired, local officers executed it, found incriminating evidence, and arrested the defendant.

During the same time period, the FBI independently secured similar information, secured a federal search warrant, and searched the address after the local police advised of the search and the arrest.

Incriminating evidence was found. While the defendant was in local custody, the FBI "mirandized" the defendant and interviewed him. He made incriminating statements which led the FBI to a minor with whom the defendant had a sexual relationship. An interview with the minor led to the issuance of a second federal search warrant for the address. More incriminating evidence was seized. Then, based on statements by the defendant and others that the defendant used various email addresses to access child pornography, a third federal search warrant was issued to third-party Internet providers. The application for this third warrant included statements made by the defendant during the FBI interview. That warrant led to the discovery of multiple images and video of child pornography.

The defendant moved to suppress everything as being the tainted "fruit" of the evidence seized during the execution of the expired local warrant. The trial court granted the motion in part and suppressed the evidence derived from the statements made to the FBI as well as the evidence seized from the first federal warrant search. The motion was denied as to statements made by the minor and his family and evidence secured through the other warrants. The trial court relied on the good faith exception to the exclusionary rule in denying the motion in part.

The Court of Appeals affirmed: (1) "The evidence at issue was obtained pursuant to a search warrant, so we begin by evaluating whether the good faith exception to the exclusionary rule applies," (2) After describing four situations where the good faith exception would not apply,

the court observed that, "this case calls upon us to answer whether the good faith exception applies in a fifth situation: when the magistrate's probable cause finding is based on evidence that was the product of an illegal search or seizure," (3) inclusion of the defendant's suppressed statements in the application for the third warrant were, "the result of negligence of more or more law enforcement officers," (4) the affiant for the third federal search warrant could not have known the statements would later be suppressed, and (5) "[u]nder these facts, involving state and federal investigations that were parallels, suppression is not justified."

#Fourth Amendment Good Faith Exception

United States v. Workman, 863 F.3d 1313 (10th Cir. July 21, 2017)

This was another appeal from an order suppressing evidence derived from a search pursuant to a warrant issued by a magistrate judge that exceeded her jurisdiction (see *United States v. Horton* above). The defendant was found by the FBI in his Colorado home in the act of downloading child pornography. The Court of Appeals assumed that an unconstitutional search had occurred. However, the court reversed, concluding that the good faith exception to the Warrant Requirement was applicable because the agents acted with an objectively reasonable belief that the warrant was valid. Among other things, the court relied on the fact that other courts had found that the warrant in issue complied with federal law. [NOTE THAT THIS DECISION INCLUDES A GRAPHIC ON HOW THE NIT WORKED].

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

United States v. Wurie, 728 F.3d 1 (1st Cir. 2013), aff'd, Riley v. California, 134 S. Ct. 2473 (2014)

"This case requires us to decide whether the police, while seizing a cell phone from an individual's person as part of his lawful arrest, can search the phone's data without a warrant. We conclude that such a search exceeds the boundaries of the Fourth Amendment search-incident-to-arrest exception. Because the government has not argued that the search here was justified by exigent circumstances or any other exception to the warrant requirement ***," the denial of the defendant's motion to suppress was reversed, the conviction vacated, and the matter remanded.

#Fourth Amendment Warrant Required or Not

In re Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@gmail.com Maintained at Premises Controlled By Google, Inc., 33 F. Supp. 3d 386 (S.D.N.Y. 2014)

The court granted a search warrant application for information from a Gmail account as it was presented by the Government. In this opinion, the court explained why it issued the warrant and did not impose conditions. That explanation included the following:

(1) The SCA permits the Government to obtain the "contents" of an "electronic communication" pursuant to a search warrant.

(2) "In the case of electronic evidence, which typically consists of enormous amounts of undifferentiated information and documents, courts have recognized that a search for documents or files responsive to a warrant cannot possibly be accomplished during an on-site search."

(3) *Fed. R. Crim. P.* 41(e)(2)(B) was amended in 2009 to provide a two- step procedure for seizure, followed by review, of electronically stored information.

(4) Caselaw "supports the Government's ability to access an entire email account in order to conduct a search for emails within the limited categories contained in the warrant."

(5)"It is unrealistic to believe that Google *** could be expected to produce the materials responsible to categories**" because (a) "the burden on Google would be enormous because duplicating the

Government's efforts might require it to examine every email," (b) "Google employees would not be able to interpret the significance of particular emails without having been trained in the investigation" and (c) "[p]lacing the responsibility for performing these searches on the email host would also put the host's employees in the position of appearing to act as agents of the Government vis-a-vis their customers."

(6) "Judging the reasonableness of the execution of a warrant *ex ante* *** is not required by Supreme Court precedent."

(7) "If the Government acts improperly in its retention of the materials, our judicial system provides remedies, including suppression and an action for damages ***."

#Fourth Amendment Ex Ante Conditions

In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), rev'd, 829 F.3d 197 (2d Cir. 2016), cert. granted, 2017 WL 2869958 (Oct. 16, 2017)

A magistrate judge issued a warrant *under the SCA* that authorized the Government to search and seize information in a web-based e-mail account. "Microsoft complied with the search warrant to the extent of producing non-content information stored on servers in the United States. However, after it determined that the target account was hosted in Dublin [Ireland] and the content information stored there," Microsoft moved to quash as to the information stored abroad. Microsoft argued that United States courts cannot issue warrants for "extraterritorial search and seizure." The court disagreed:

(1) Although the language of the controlling statute, the SCA, is "ambiguous in at least one critical respect," the "unique structure of the SCA does not implicate principles of extraterritoriality." (The ambiguity arose from the reference in 18 U.S.C. Section 2703(a) to the Federal Rules of Criminal Procedure, which includes limitations on the territorial reach of warrants issued pursuant to Rule 41).

(2) "It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information."

(3) "In this case, no such exposure [to possible human observation] takes place until the information is reviewed in the United States, and consequently no extraterritorial search has occurred."

The court observed that to hold otherwise would raise practical concerns:

(1) "[A] party intending to engage in criminal activity could evade an SCA Warrant by the simple expedient of giving false residence information, thereby causing the ISP [internet service provider] to assign his account to a server outside the United States."

(2) "[I]f an SCA Warrant were treated like a conventional warrant, it could only be executed abroad pursuant to a Mutual Legal Assistance Treaty ('MLAT')." (3) "[A]s burdensome and uncertain as the MLAT process is, it is entirely unavailable where no treaty is in place."

Finally, the court rejected Microsoft's argument that the warrant had

extraterritorial application: "an SCA warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the

location where data are stored. At least in this instance, it places obligations only on the service provider to act within the United States."

On July 31, 2014, the magistrate judge was affirmed from the Bench by a district judge. On August 29, 2014, the district judge lifted the stay of execution she had granted on July 31st to allow Microsoft an opportunity to appeal. The district judge concluded that her order was no final and appealable.

#Miscellaneous

I/M/O Warrant to Search a Certain E-Mail Acct. Controlled and Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), rehearing en banc denied, 855 F.3d 53 (2d Cir. 2017), cert. granted, United States v. Microsoft, No. 17-2 (Oct. 16, 2017)

Microsoft appealed from orders denying its motions to quash a warrant issued under the SCA and holding it in civil contempt for failing to comply with the warrant. The warrant required Microsoft to seize and produce the content of an e-mail account it maintained for a customer as part of the government's investigation into drug trafficking. Microsoft produced non-content information stored in the United States to refused produced data stored in Ireland. The court of appeals reversed, concluding that the SCA did not have extraterritorial application. In a separate opinion one judge commented that he concurred, "but without any illusion that the result should even be regarded as a rational policy outcome, let alone celebrated as a milestone in protecting privacy."

#Miscellaneous

In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013)

"The Government has applied for a Rule 41 search and seizure warrant targeting a computer allegedly used to violate *** [federal] laws. Unknown persons are said to have committed these crimes using a particular email account via an unknown computer at an unknown location. The search would be accomplished by surreptitiously installing software designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period. In other words, the Government seeks a warrant to hack a computer suspected of criminal use."

The magistrate judge denied the application: (1) The application did not meet any of the

territorial limits imposed by Criminal Rule 41(b); (2) the application did not meet the particularity requirement of the Fourth Amendment; (3) concluding "video surveillance" was being requested and borrowing from standards set forth for wiretaps under Title III of the Omnibus Crime Control and Safe Streets Acts of 1968, the application failed to address alternative investigative methods or the steps that would be taken to minimize the surveillance.

[Note that magistrate judge's statement, among other things, that "the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance in this circuit"].

#Fourth Amendment Particularity Requirement

Waymo LLC v. Uber Technologies, Inc., **319 F.R.D. 284 (N.D. Ca. Apr. 10, 2017), petition for writ of *mandamus* denied, 2017-1904 (Fed. Cir. Apr. 25, 2017)**

This civil action arises out of the alleged theft of trade secrets and proprietary information by a non-party individual, who left his position with the plaintiff corporation to start a competing business that was acquired by defendant Uber Technologies. The individual moved to prevent the defendants from listing on a privilege log a "due diligence" report prepared by a "third party." He argued that a joint defense agreement existed between with the defendants, the agreement made the defendants' lawyers his personal lawyers, and the Fifth Amendment "somehow prohibits them from revealing any information, even on a privilege log, that would help a prosecutor connect the dots to him." The court denied the motion because no binding authority supported the individual's suggestion that his "Fifth Amendment privilege necessarily supersedes typical privilege log requirements." The Federal Circuit denied the individual's *mandamus* petition as he had not established a "clear and indisputable" right to the issuance of a writ.

#Fifth Amendment Self-Incrimination

Yates v. United States, 135 S.Ct. 1074 (2015)

The petitioner, a commercial fisherman, ordered a crew member to toss undersized fish overboard to prevent federal authorities from confirming the catch. He was prosecuted and convicted for destruction of a "tangible object" under 18 U.S.C. Sec. 1519. Interpreting the statute, which was enacted as part of the Sarbanes-Oxley Act, the court reversed:

"A fish is no doubt an object that is tangible ***. But it would cut *** 1519 loose from its

financial-fraud mooring to hold that it encompasses any and all objects, whatever their size or significance, destroyed with obstructive intent. Mindful that in Sarbanes-Oxley, Congress trained its attention on corporate and accounting deception and cover-ups, we conclude that a matching description of 150

*** 1519 is in order: A tangible object captured by *** 1519 *** must be one used to record or preserve information."

#Miscellaneous

DECISIONS – STATE

***Matter of 381 Search Warrants Directed to Facebook, Inc.*, 78 N.E.3d 141 (N.Y. 2017)**

Trial court denied Facebook's motion to quash warrants for various accounts issued in furtherance of a large-scale investigation into fraudulent Social Security claims. "This appeal raises the question of whether an online social networking service, the ubiquitous Facebook, served with a warrant for customer accounts, can litigate prior to enforcement the constitutionality of the warrant on its customers' behalf." The Appellate Division dismissed the appeal: The key role of the judicial officer in issuing a search warrant is described generally by the Fourth Amendment and more specifically by state statutes. None of these sources refer to an inherent authority for a defendant or anyone else to challenge an allegedly defective warrant before it is executed. The Court of Appeals affirmed, rejecting Facebook's argument to treat "Supreme Court's first order denying its motion to quash the warrants as an appealable order denying a motion to quash *subpoenas*." The court explained: "Despite the minor similarities between SCA warrants and subpoenas, in this post-digital world, we are not convinced that SCA warrants — which are required under the statute to obtain certain content-based information that cannot be obtained with a subpoena due to heightened privacy interests in electronic communications — should nevertheless be treated as subpoenas." "Inasmuch as there is no statutory predicate for Facebook's appeal from the order denying its motion to quash the SCA warrants that were issued in a criminal proceeding nor any other legal basis for such appeal, we must affirm the Appellate Division's dismissal of Facebook's appeal insofar as taken from that order. Supreme Court's order denying Facebook's motion to compel disclosure of the affidavit is, likewise, not appealable, although Facebook may explore other procedural avenues to raise its claim."

#Miscellaneous

#Social Media

***In re Alex C.*, 13 A.3d 347 (N.H. 2010)**

There was an appeal from a trial court ruling that a delinquency petition was "true." The juvenile had sent twenty admittedly harassing instant messages to the mother of a girl who had run away. On appeal, the delinquent argued these were not "repeated communications" under New Hampshire law. The Supreme Court affirmed. The Court viewed IM, "not necessarily as some monolithic entity-a single conversation, but as a series of discrete electronic messages between two or more individuals."

#Trial-Related

***In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012), cert. denied, 569 U.S. 994 (2013)**

In this complaint for extraordinary relief, the Vermont Supreme Court addressed whether a judicial officer had discretion to attach "ex ante or prospective conditions" to a search warrant. In the course of an identity theft investigation, law enforcement applied for a warrant to search premises and seize electronic media. The warrant was issued. However, in a separate order, the issuing judicial officer imposed conditions on the search and use of the content of any seized media. After concluding that it had jurisdiction, the Supreme Court held: (1) warrant instructions are binding and failure to follow those instructions renders a search unconstitutional; (2) "ex ante instructions are sometimes acceptable mechanisms for ensuring the particularity of a search;" (3) the issuing court did not have authority to "pick and choose which legal doctrines would apply to a particular police search" (thus invalidating a condition related to the plain use doctrine); (4) "separation and screening instructions" were an appropriate means to ensure that police could only view information for which probable cause existed; (5) limitations on search techniques and the prohibition of use of "sophisticated searching software" without prior judicial approval was appropriate; and (6) instructions with regard to copying, return, and destruction were within the judge's discretion. It should be noted that the issuing officer relied on *United States v. Comprehensive Drug Testing, Inc.*, 579 F.3d 989 (9th Cir. 2009) (en banc) ("CDT I"), which approved the imposition of conditions to a warrant. The imposition of conditions was later subsequently disapproved in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) ("super" en banc) ("CDT II"). It should also be noted that, throughout its decision, the Vermont Supreme Court emphasizes both volume of ESI and privacy concerns.

#Fourth Amendment Ex Ante Conditions

***Apple, Inc. v. Superior Court*, 151 Cal. Rptr. 3d 841 (2013)**

In this putative class action, the California Supreme Court interpreted the Song-Beverly Credit

Card Act to be inapplicable to transactions which involved the alleged collection of personal identifiers as a condition of the use of credit cards to purchase electronically downloadable products over the Internet. The court distinguished *Pineda v. Williams-Sonoma Stores, Inc.*, (*q.v.*) which also interpreted the Act, as being limited to "the purchase of a physical product at a traditional 'brick-and-mortar' business." The court did note, however, that the Legislature was free to amend the Act to reach the electronic transactions.

#Miscellaneous

***Bainbridge Island Police Guild v. City of Puyallup*, 259 P.3d 190 (Wash. 2011)**

Various citizens filed suit in various counties seeking disclosure of a criminal investigation report and an internal investigation report regarding allegations of sexual assault against a police officer. The police officer and the police union sought to enjoin disclosure, citing the state public records statute. The lower courts ruled that that the reports were statutorily exempt from disclosure as personal information. The citizens seeking the reports appealed. Upon consolidating appeals, the Washington Supreme Court reversed and remanded, instructing the state to redact the officer's identity and produce the remainder of the reports. Despite the fact that the officer failed to prevent the production of the reports to newspaper reporter, the court stated that it did not mean he was forever prohibited from protecting his right to privacy in regards to disclosure of the reports to other individuals. While the officer's name was deemed statutorily exempt from disclosure, the remainder of the investigation reports concerning the allegation was not exempt. The Court held that the public did not have a legitimate interest in the name of a police officer subject to an unsubstantiated allegation of sexual misconduct; the public did, however, have a legitimate interest in knowing how police departments responded to and investigated such allegations.

#Miscellaneous

***Bennett v. Smith Bundy Berman Britton*, PS, 291 P.3d 886 (Wash. 2013), reconsideration denied, No. 84903-0 (Apr. 30, 2013)**

In what began as a marriage dissolution action, an accounting was sued and, during discovery, produced tax records of nonparties. The parties stipulated to a confidentiality order that provided, among other things, that the tax records could be used in motions, etc., only if filed under seal. The firm moved for summary judgment and the trial court ordered that documents be filed under seal. After opposition papers were filed, but before the court had considered the motion, the action settled. After the settlement, the parties realized that the opposition papers inadvertently included materials that should have been filed under seal and agreed to file redacted and sealed versions of those papers. The plaintiffs' expert then moved to intervene, seeking access to everything filed under seal. The trial court allowed the intervention but denied

to unseal the documents. The intermediate appellate court affirmed, as did the Washington Supreme Court. Interpreting the Washington State Constitution, the Supreme Court held that "the act of filing a document does not alone transform it into a public one" and that "information does not become part of the judicial process is not governed by the open courts provision." Here, the sealed documents were not relevant to a decision and there was no presumption of public access. Instead, a five-part balancing test would govern. The Supreme Court remanded to apply that test.

#Discovery Materials

***Butler v. State,* 459 S.W.3d 595 (Tex. Crim. App. 2015)**

The defendant was convicted of the aggravated kidnapping of his girlfriend. On appeal, he challenged the authentication of incriminating text messages through the girlfriend. The Court of Criminal Appeals affirmed:

"Although *** Salas's [the girlfriend's] responses are not without ambiguity, a rational jury could conclude that Salas recognized the texts to be coming from the Appellant on this occasion (and not someone else who might have purloined his phone) because: (1) he had called her from that number on past occasions; (2) the content and context of the text messages convinced her that the messages were from him; and (3) he actually called her from that same phone number during the course of that very text message exchange."

#Trial Materials

***Clark v. State,* No. 0953 (Md. Ct. Spec. App. Dec. 3, 2009)**

After conviction, the defendant appealed from the denial of his motion for a mistrial based on juror misconduct. One juror had conducted Wikipedia research on a relevant and significant term. He had not, however, shared the results of the research with fellow jurors. The appellate court reversed, citing *Wardlaw* (see below) and concluding that the juror had done more than look up a definition: "The definition of 'a definition' is like a rubber band and can, as here, be stretched to the breaking point." By doing so, the impartiality of the entire panel had been compromised.

#Trial-Related

***Collins v. State,* 172 So. 3d 724 (Miss. 2015)**

The defendant had been convicted of murder. The evidence against him included GPS locations based on the defendant's cell phone records. Addressing a question of first impression, the

Mississippi Supreme Court distinguished between lay testimony that "simply describes the information in a cell phone record *** [or] merely informs the jury as to the location of cell towers" from testimony that "goes beyond the simple description of cell phone basics *** [and] purports to pinpoint the general area in which the cell phone user was located based on historical cellular data." The court held that the latter requires that a witness be qualified as an expert. The conviction was reversed in part because the testifying officer had not been qualified.

#Miscellaneous

#Trial Materials

***Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014)**

In the course of a murder investigation, the Commonwealth secured an order pursuant to Section 2703(d) of the SCA that gave it access to the historical CSLI of a suspect for a 14-day period. A motion judge suppressed evidence derived from the CSLI. The judge reasoned that, notwithstanding the issuance of the order, access to CSLI constituted a "search" under the Massachusetts Constitution that required a search warrant supported by probable cause. The Supreme Judicial Court affirmed. It held that the user of a cellular telephone had a reasonable expectation of privacy in historical CSLI and rejected the application of the third-party doctrine: "We agree with the defendant *** that the nature of cellular telephone technology and CSLI and the character of cellular telephone use in our current society render the third-party doctrine of [*United States v.*] *Miller* and *Smith* [*v. Maryland*] inapposite; the digital age has altered dramatically the societal landscape from the 1970s, when *Miller* and *Smith* were written."

The Court noted that, "it is likely that the duration of the period for which historical CSLI is sought will be a relevant consideration in the reasonable expectation of privacy calculus *** [b]ut there is no need to consider at this juncture what the boundaries of such a time period might be because *** the two weeks covered by the 2703(d) order at issue exceeds it *** the tracking of the defendant's movements *** for two weeks was more than sufficient to intrude upon the defendant's reasonable expectation of privacy ***."

The Court remanded for consideration of whether the affidavit submitted in support of the order demonstrated the existence of probable cause. The Court also declared that its ruling constituted a "new rule" and would apply only to cases in which a defendant's conviction was not final.

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Carter,* 52 N.E.3d 1054 (Mass. 2016)**

Defendant was indicted as a youthful offender on a charge of involuntary manslaughter.

Defendant moved in the juvenile court asserting that the evidence was insufficient for an indictment because her conduct did not extend beyond words. The juvenile court denied the motion and the Supreme Judicial Court affirmed, holding that the grand jury was justified in returning an indictment because such a conviction is punishable by imprisonment.

#Miscellaneous

***Commonwealth v. Chamberlin*, 45 N.E.3d 900 (Mass. 2016)**

Defendant appealed a conviction of armed robbery, kidnapping and armed assault, arguing that the trial court erred in denying his motion to suppress his cellular telephone records. Specifically, defendant contended that the government failed to comply with Mass. Gen. Laws ch. 271, 17B, in obtaining his telephone records. The Supreme Judicial Court affirmed, holding that Mass. Gen. Laws ch. 271, 17B, did not preclude the government from obtaining the records at issue in this case.

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Cole,* 41 N.E.3d 1073 (Mass. 2015)**

The Supreme affirmed and declined to grant relief pursuant to Mass. Gen. Laws ch. 278, 33E, holding the trial judge did not err in admitting (1) medical records and related testimony and by instructing the jury on consciousness of guilt; (2) expert testimony concerning the statistical significance of DNA evidence; and (3) the victim's T-shirt into evidence, despite a discovery violation by the Commonwealth. The court also found that the prosecutor did not commit misconduct during her opening statement or her closing argument; and the trial judge properly denied defendant's motion for required findings of not guilty.

#Discovery Materials

#Trial-Related

#Miscellaneous

***Commonwealth v. Cox,* 72 A.3d 719 (Pa. Super. Ct. 2013)**

"In this appeal, we face the question of whether comments made in an on-line forum can constitute a criminal offense." The appellant had appealed a conviction for harassment under Pennsylvania law after she posted lewd comments on Facebook. The court affirmed: "The evidence of record establishes that Cox posted a statement indicating that Victim suffered from a sexually transmitted disease on an online forum, and that this statement was viewed by

multiple people. *** this is sufficient to support a finding that Cox communicated lewd sentiments about Victim to other people, and an inference that in doing do it was here intent to harass, annoy or alarm Victim" (footnotes omitted).

#Trial-Related

#Social Media

Commonwealth v. Denison, **No. BRCR2012-0029 (Mass. Super. Ct. Oct. 7, 2015)**

"ShotSpotter is a listening and recording system that runs 24/7, attuned to the sound of gunfire. When the system hears gunfire, or what it recognizes as gunfire, it locates it, reports it, preserves the recording, and send the recording to the customer within seconds." The defendant, charged with first degree murder, moved to suppress a recording made by ShotSpotter of an verbal exchange among numerous individuals before and after the fatal gunshots. The court rejected that the argument that the defendant had a reasonable expectation of privacy under the Massachusetts Declaration of Rights because the exchange was "audible by anyone passing and was in fact heard by a crowd of neighbors and other witnesses." However, the court found that the exchange was an "oral communication" and that the recording was a prohibited "interception" under the Massachusetts Wiretap Act because the defendant had no knowledge that the exchange was being recorded. The court also found that the interception was "willful" because the police had "purposefully directed the placement of the sensors." The court granted the motion to suppress: "the continuous secret audio surveillance of selective urban neighborhoods *** is the type of surreptitious eavesdropping as an investigative tool that the Legislature sought to prohibit."

#Fourth Amendment Warrant Required or Not

#Miscellaneous

Commonwealth v. Dorelas, **43 N.E.3d 306 (Mass. 2016)**

Superior Court denied defendant's pretrial motion to suppress photographs that the police had obtained from a search, conducted pursuant to a warrant, of defendant's cell phone. The court found the search to be reasonable with probable cause that evidence of communications relating to and linking the defendant to the crimes under investigation would be found on the device, and such communications could be conveyed or stored in photographic form; and the photographs in question were properly seized as evidence linking the defendant to the crimes under investigation.

#Fourth Amendment Particularity Requirement

***Commonwealth v. Dyette,* 32 N.E.3d 906 (Mass. App. Ct. 2015)**

The defendant was convicted of firearms offenses. At the time of his arrest, an officer "took the defendant's cell phone, looked at the call log, and saw that there was an array of numbers and symbols that did not represent a telephone number." The log was also examined later when the defendant was booked. The content of the log incriminated him and was admitted into evidence. On appeal, the defendant argued, among other things, that this evidence should have been suppressed. The Appeals Court agreed and reversed the conviction: Relying on *Riley v. California,* the court observed that "[t]here was no effort to secure the telephone in any fashion or to seek a warrant and that the risk that records of calls "would be pushed out of the call log in the event of other incoming calls" could be avoided by "turning the cell phone off, placing the cell in a Faraday bag, or securing the phone and seeking a warrant for it." The court also held that "the possible degradation of the call log is not an exigent circumstance since that degradation is preventable."

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Exigent Circumstances

***Commonwealth v. Estabrook*, 38 N.E.3d 231 (Mass. 2015)**

The defendants in this murder prosecution moved to suppress evidence derived from historical CSLI. In 2012, police secured two weeks of CSLI for one defendant's cell phone pursuant to a Section 2703(d) order. That evidence placed his cell phone near the scene of the murder and, through an interview with him, led the police to the second defendant. The CSLI was reobtained pursuant to a search warrant supported by probable cause over a year later. The trial court denied the motions. Revisiting *Commonwealth v. Augustine,* the Massachusetts Supreme Judicial Court adopted a "bright-line rule that a request for historical CSLI for a period covering six hours or less does not require a search warrant." The court emphasized that "the salient consideration is the length of time for which a person's CSLI is requested, not the time covered by the person's CSLI that the Commonwealth ultimately seeks to use as evidence at trial." Thus, the Massachusetts warrant requirement applied because the police obtained two weeks of CSLI. Both defendants incriminated themselves during interviews conducted after the CSLI had been obtained. The court observed that the statements would be admissible "if they are not the fruits of the illegal search of the CSLI." The court concluded that none of the statements made by the second defendant should be suppressed because "they were sufficiently attenuated from the illegal search." However, the statements of the defendant with the cell phone were suppressed as these were made in "in close proximity to the illegality, and there were no intervening circumstances between the police questions based on the CSLI" and the defendant's responses. Finally, the court upheld the 2013 warrant. The supporting affidavit established probable cause

and contained no information obtained pursuant to the Section 2703(d) order.

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Gelfgatt,* 11 N.E.3d 605 (Mass. 2014)**

On remand from the Massachusetts Supreme Judicial Court, the Superior Court held the defendant in civil contempt. He was under a "clear and unambiguous order *** to unlock the security features of his computers and flash drives by entering his personal and self-created passwords or phrases" and failed to do so. The court found that the defendant's contention that he could not remember the passwords was "dubious."

#Fifth Amendment

***Commonwealth v. Keown*, 84 N.E.3d 820 (Mass. 2017)**

The defendant was convicted of murder in the first degree on a theory of deliberate premeditation for poisoning his wife. He argued on appeal, among other things, that that the trial judge abused her discretion in denying motions relating to (1) the defendant's use of the computer username "Kaiser Soze"; (2) the victim's statements and e-mail messages; and (3) the incriminating Google searches performed on the computer. The state Supreme Judicial Court held that the judge did not abuse her discretion in "allowing the username evidence to be admitted at trial for the limited purpose of showing the defendant's possession, custody, and control of the laptop computer." Furthermore, the victim's messages "were admitted in evidence for another permissible purpose (i.e., to show that the victim's state of mind was inconsistent with suicide), and their innocuous nature makes it unlikely that they would (or could) have been used improperly by the jury." Finally, the judge did not abuse her discretion in admitting evidence of the incriminating searches performed on the computer using Google prior to the victim's death. Although there "was no evidence offered on who conducted these searches," a jury "could reasonably infer that it was the defendant who conducted the searches."

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Mauricio*, 80 N.E.3d 318 (Mass. 2017)**

The defendant was convicted of carrying a firearm without a license and receiving stolen property with a value in excess of $250. The convictions stem from a search of the defendant's backpack after he was arrested for possession of a controlled substance and breaking and entering a residence. During the course of the inventory search, the police discovered a digital camera, a ring, and other items. The inventory officer turned on the camera and retrieved images

depicting the defendant next to firearms later determined to have been stolen. The receiving stolen property conviction was based on the ring discovered in the defendant's backpack. On appeal, the defendant argued that the judge wrongly denied the motion to suppress the images recovered from the warrantless search of the digital camera because the search did not fall within the purview of the search incident to arrest exception to the warrant requirement and exceeded the scope of a valid inventory search. The court reversed the decision of the lower court holding that under the Massachusetts Declaration of Rights, digital cameras may be seized incident to arrest, but that the search of data contained in a camera exceeds the scope of the search incident to arrest exception to the warrant requirement. The court applied the same reasoning utilized by the Supreme Court in *Riley v California* explaining that threat of harm to officers and destruction of evidence were not present with regard to the data on a digital camera. Furthermore, the court found that the search of the digital camera exceeded the bounds of the inventory search exception to the warrant requirement because it was "investigatory in nature." Therefore, the search "exceeded the scope of and was inconsistent with the purposes underlying the inventory search exception to the warrant requirement." However, the court disagreed with the defendant's argument that the ring should have been suppressed under the "fruit of the poisonous tree" doctrine. The court explained that the connection between "the ring and the illegality—the unlawful search of the camera—is so tenuous," that the "application of the fruit of the poisonous tree doctrine would risk untethering it from its underlying principles."

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Rousseau*, 990 N.E.2d 543 (Mass. 2013)**

The two appellants were convicted of criminal acts arising out of the burning and vandalizing of four properties. Suspecting their involvement, the police secured a warrant allowing the installation of a GPS device on a vehicle owned by one defendant and in which the other was a passenger. The vehicle was tracked for thirty days and the tracking "tied" the defendants to four criminal acts. They were arrested and subsequent searches yielded incriminating materials. The Massachusetts Supreme Court, on a direct appeal, affirmed the convictions: (1) Relying on *Commonwealth v. Connolly,* 454 Mass. 808 (2009) and *United States v. Jones,* 132 S. Ct. 945 (2012), the court concluded that the appellant owner of the vehicle had a possessory interest sufficient for standing purposes, (2) the other appellant, although a "mere passenger having no possessory interest" in the vehicle, had standing under the Massachusetts Constitution given the facts of the case, and (3) probable cause existed for the issuance of the warrant given, among other things, the appellants' extensive criminal histories and statements made by a cooperating witness, even assuming that certain information was excised from the warrant application.

The court did modify a probationary condition for one appellant. Both appellants had been barred from *any* access to a computer while in prison. Although the court agreed that some

restriction was appropriate given that the appellants had sought to publicize their criminal acts, the court concluded that, "given that the Department of Correction had digitized its law library, *** the breadth of the probationary condition would have the practical effect of denying Rousseau access to the courts" and permitted him to "use the prison library computers for the limited purpose of conducting legal research and other activity related to his case."

#Fourth Amendment Warrant Required or Not

#Miscellaneous

***Commonwealth v. Stem*, 96 A.3d 407 (Pa. Super. Ct. 2014)**

In this post-*Riley* decision, the Superior Court of Pennsylvania affirmed the trial court's suppression of evidence derived from the warrantless search of the defendant's cell phone and "the fruits derived therefrom." The defendant had been arrested and his phone searched on August 14, 2012. The trial court ruled on July 13, 2013. Interestingly, the Superior Court did not consider *any* exception to the warrant requirement!

#Fourth Amendment Warrant Required or Not

***Commonwealth v. Tarjick,* 30 N.E.3d 125 (Mass. App. Ct. 2015), *appeal denied,* 40 N.E.3d 552 (Mass. 2015)**

"This matter involves the interplay between twenty-first century technology and twentieth century search and seizure principles. We hold that the police, while executing a search warrant for nude images of the defendant's thirteen year old stepdaughter on a video camera, cellular telephone ***, and computer, were justified in seizing three memory cards from digital cameras they came upon." The police secured a warrant that did not include the memory cards as items to seize. However, they searched the contents only after having secured a second warrant. On appeal from his conviction for child abuse, the defendant argued that evidence derived from the cards should have been suppressed. The Appeals Court held that the cards were "plausibly related to the victim's allegations and were properly seized under the plain view doctrine." Moreover, "[o]n discovery of the memory cards, the officers were also justified in recognizing the possibility that any evidence contained in them could be at risk of erasure or destruction, making it reasonable for the officers to seize the cards to preserve the evidence while applying for the second warrant." The convictions were affirmed.

#Fourth Amendment Particularity Requirement

***Cunningham v. N.Y. State Dep't of Labor*, 997 N.E.2d 468 (N.Y. 2013)**

The petitioner, a former New York State employee, appealed from his discharge for submitting false time reports. To investigate his conduct, the State attached a GPS device to the petitioner's car. The GPS device and two replacements tracked the car for a month, "including evenings, weekends and several days when petitioner was on vacation in Massachusetts. The Court of Appeals reversed: (1) There is a workplace exception to the warrant requirement, (2) "when an employee chooses to use his car during the business day, GPS tracking of the car may be considered a workplace search," and (3) reasonable suspicion of employee misconduct existed to justify the attachment of the device. However, the search was unreasonable because it was excessively intrusive.

#Fourth Amendment Warrant Required or Not

***Demby v. State,* 118 A.3d 890 (Md. 2015)**

"We are called upon *** to decide whether Petitioner *** was entitled, by application of the rule established in *Riley* [*v. California*], to suppression of evidence obtained as the result of the search of a cell phone incident to his arrest in 2012." At the time of the petitioner's arrest, binding precedent in Maryland allowed a warrantless search. Therefore, suppression was unwarranted by application of the good faith doctrine.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

***In re the Detention of H.N.,* 355 P.3d 294 (Wash. Ct. App. 2015), *rev. denied,* 366 P.3d 1244 (Wash. 2016)**

The detainee was committed for involuntary treatment on findings that she suffered from a mental disorder and posed a likelihood of serious harm to herself. She argued on appeal that the trial court had erred when it admitted as substantive evidence "e-mailed screen shots of text messages" relied on by the State's psychologist. The purported messages were made between the detainee and her boyfriend on an evening when she had been found unconscious and lying in a pool of her own vomit after ingesting liquor and a medication. The Washington Court of Appeals held that the State had made a sufficient *prima facie* showing:

"The record establishes that the emailed screenshots of text messages were authored by H.N. Likewise, they were sent from the cell number associated with H.N. Finally, they were sent from the cell number associated with H.N. Finally, the distinctive characteristics of the messages, taken in conjunction with the circumstances are sufficient to support authentication."

#Trial Materials

***Devega v. State*, 689 S.E.2d 293 (Ga. 2010)**

After being convicted of murder and other offenses, the defendant sought a new trial. He argued, among other things, that his trial attorney should have challenged on Fourth Amendment grounds the warrantless "ping" of his cell phone. The police used the phone to monitor the location of the phone from a public road, distinguishing *United States v. Karo* (which addressed the monitoring of a beeper from a private residence). The court found that the defendant had no reasonable expectation of privacy while traveling in public places.

#Fourth Amendment Warrant Required or Not

***Facebook, Inc. v. Superior Court,* No. A144315 (Cal. Ct. App. Sept. 8, 2015), *rev. pending,* 195 Cal. Rptr. 3d 789 (2015)**

Three social media providers moved to quash subpoenas for public and private content from user accounts of a murder victim and a witness. The subpoenas were served by two defendants who were indicted and awaiting trial on various charges related to the murder. The providers moved to quash, contending that disclosure of content was barred by the Stored Communications Act. The trial court denied the motion and ordered *in camera* review. The providers appealed. The defendants argued that, regardless of the SCA, the materials were needed to "ensure their right to present a complete defense to the charges against them, and that their Fifth Amendment guarantee of due process and Sixth Amendment right to compulsory process are implicated." The Court of Appeal disagreed and ordered that the motions be granted: "[W]e find no support for the trial court's order for pretrial production of information otherwise subject to the SCA's protections. The court left open the possibility that the defendants might seek content *at trial*, "where the trial court would be far better equipped to balance the Defendants need for effective cross- examination and the policies the SCA is intended to serve." In *dicta,* the court questioned the constitutionality of the SCA should it be construed to bar a *trial* subpoena by a defendant.

#Discovery Materials

#Trial-Related

#Social Media

***Freeman v. Mississippi*, 121 So.3d 888 (Miss. 2013)**

The defendant was arrested for DUI. The stop was recorded on video. The defendant was then transported to a police station, where a blood alcohol test was administered. The defendant subpoenaed the arresting officer for the video tape. There was no response. The video was played at trial. The defendant argued that the video was inconsistent with testimony offered by

the officer. After being convicted, the defendant appealed for a trial *de novo.* The defendant secured a preservation order. Thereafter, the defendant learned that the tape had been destroyed. The trial court denied a motion to dismiss but inferred that the video would have been favorable to the defendant. "At trial, the facts were hotly contested." The defendant was again convicted. After an appellate court affirmed the conviction, the Mississippi Supreme Court reversed: (1) "[T]he State was under an affirmative duty via a court order to preserve the video," (2) "the loss of the video while the State was under a court order to preserve the video clearly impaired Freeman's defense," (3) preservation would not have imposed "unreasonable requirements on the police to employ guesswork as to what should be preserved, or to preserve an unreasonable quantity of evidence," and (4) the destruction of the tape "undermines the confidence in the outcome of the trial."

In ruling, the court made this observation in footnote 4: "We note that video evidence is different from biological evidence such as DNA samples in that it is much easier to preserve and/or produce to the defense. It need not be subject to testing or preserved using specialized scientific processes. The State offers no excuse as to why it did not comply with the discovery requests and the court order, other than that Officer Patrick did not think he had the software on his computer with which to copy the video. There is no evidence that such software would be difficult to obtain and utilize, especially given the nearly fourteen months that elapsed between the first request for the video and the assertion that the video was destroyed. In making this distinction, we do not suggest that the loss or destruction of biological or like evidence is any less egregious than the destruction of video evidence. We merely note that video evidence is likely to be even easier for the State to produce to defendants."

#Preservation and Spoliation

***Galloway v. Town of Hartford*, 57 A.3d 684 (Vt. 2012)**

A journalist requested records relating to the police's response to a possible burglary in progress. The police used considerable force in restraining the suspect, who turned out to be the homeowner. The police chief and town manager denied the request, claiming the records related to a criminal investigation, and thus, were protected from disclosure under "exemption five" of the state's public records act. The journalist filed an action against the town to compel production of the records. The trial court concluded that the records created by police were exempt from disclosure under the state's public records act "because they were created *during* the course of an investigation into suspected criminal activity." Because the investigation was terminated without any resulting criminal charges, however, the court held that "any records created *after* the decision that there would be no criminal charges had to be disclosed." The trial court reasoned that "the records revealing the outcome of an investigation are not records 'of the investigation,' but are its product." The journalist objected to this decision on the grounds that it

contravened the purposes of the public records act, and that the criminal investigation ended when the handcuffs were removed from the suspect. The trial court declined to modify its decision and the journalist appealed. The state Supreme Court reversed, holding that the homeowner was subjected to a de facto "arrest," requiring the disclosure of "all records considered by the trial court that were identified by the police as being generated as a result of the incident." The Court found "exemption five" inapplicable because the town failed to demonstrate that disclosure "pose[d] a concrete harm to law enforcement interests." In weighing the competing interests in determining whether the records were public, the Court also noted that "many other states are guided by statutory criteria that provide police and courts with a far better and more defined framework in making decisions about disclosure of this type of record." Two of the Justices concurred in the result but stating that the reason why the records did not fall within the exemption was because "there was no crime." One dissenting justice found that the plain language of the exemption clearly evidenced a legislative intent "to withhold information on criminal investigations and investigative detentions not resulting in charges, while mandating disclosure of arrests accompanied by a formal criminal charge." The dissenting judge criticized the majority opinion for ignoring the plain language of the statute, and instead, "impos[ing] a variable, or floating, test for public access of police records, requiring a determination of "whether the temporary detention of a suspect amounts to an arrest for purposes of Fourth Amendment protection, even when, as here, no such claim of unconstitutional invasion is at issue. As a result of this "floating" test, the dissenting judge believed that custodians of police records "must now puzzle over "de facto" arrest versus investigative detention not amounting to arrest—a moving target worthy of countless and diverse court decisions."

#Miscellaneous

***Garnett v. Commonwealth,* No. 1573-15-2 (Va. Ct. App. Dec. 20, 2016)**

The appellant was the driver of a vehicle that had been stopped at a checkpoint. When an officer approached the car, she smelled a strong marijuana odor and asked the defendant to exit. The defendant consented to a personal search. The officer then searched the vehicle and found a cell phone as well as marijuana. The appellant stated that the vehicle belonged to his sister and that he had borrowed it. At trial, the officer could not recall whether she found the phone in the center console or on the appellant's person. The police secured a warrant for the phone and obtained text messages related to drug sales. The appellant was convicted of possession with intent to distribute. He challenged the admission of the messages, among other things, on appeal. The appellate court held that the trial court erred in admitting the messages as these had not been authenticated: "the Commonwealth relied on circumstantial evidence to prove that appellant owned the cell phone and authored the text messages. The Commonwealth argued that appellant was the only person in the car, so the cell phone had to belong to him. However,

Madeline [the officer] could not recall where she found the cell phone, and proximity to the cell phone is insufficient to prove that appellant owned the cell phone and authored the text messages." Moreover, the Commonwealth did not offer business records to demonstrate ownership, the appellant made no statements about ownership, and no evidence was presented "from other people who may have sent or received text messages from appellant and could recognize his text messages." The court concluded that the error in admitting the messages was not harmless and remanded for a new trial.

#Admissibility

#Trial-Related

***Gary v. State,* 790 S.E.2d 150 (Ga. Ct. App. 2016), *cert. denied,* No. S17C0068 (Ga. Apr. 17, 2017)**

The defendant was convicted of criminal invasion of privacy under Georgia law after he "aimed his cell-phone camera underneath the skirt of the victim and recorded video" in a store. He argued on appeal that his conduct did not violate the statute under which he was charged. The Georgia Court of Appeals reversed the conviction, concluding that the conduct did not occur in a "private place" as required by the law.

#Miscellaneous

***In re Gee,* 956 N.E.2d 460 (Ill. App. Ct. 2010), *appeal denied,* 356 Ill. Dec. 797 (2011)**

During the prosecution of a murder, newspapers petitioned to intervene and gain access to a sealed search warrant file. The district court granted the petitions to intervene, but ordered the affidavit supporting the search warrant and the inventory to remain sealed. The newspapers appealed. The Court of Appeals affirmed, holding the presumption of public access in criminal proceedings did not attach to sealed-search warrant affidavit and inventory, either under the First Amendment, common law, or state law. The Court noted that federal circuit courts were split over the issue, but emphasized that the warrant application process had not been historically open to the public. Further, even assuming that a qualified right of access applied, the Court found that the generalized public interest was far outweighed by the substantial probability of compromising and interfering with an ongoing investigation. The Court stated that a warrant application involved no public or adversary proceedings.

#Trial-Related

***Gill v. State*, 300 S.W.3d 225 (Mo. 2010), *cert. denied,* 562 U.S. 861 (2010)**

The defendant, sentenced to death for first-degree murder, sought post-conviction relief, arguing that he was denied effective assistance of counsel. Trial counsel had been given a report about the contents of the murder victim's computer, which had been found in the defendant's car. The good character of the victim had been put in issue in the death penalty phase of the defendant's trial and, if counsel had investigated the computer, they would have found child pornography, with which they could have attacked the victim's character. Reserving the court below, the Supreme Court held that trial counsel's failure to investigate the contents constituted ineffective assistance of counsel and remanded for retrial of the penalty phase. The Supreme Court rejected a *Brady* challenge, noting that the report had been made available to trial counsel.

#Trial-Related

***In re Globe Newspaper Co., Inc.*, 958 N.E.2d 822 (Mass. 2011)**

After a woman was indicted by a grand jury with the murder of her brother, a newspaper filed a motion to inspect and copy the inquest report and transcript of the inquest proceedings. The judge denied the newspaper's motion and ordered the inquest report and transcript to be impounded until further order of the court. The newspaper challenged the denial of its motion, claiming that the judge erred in concluding that the impoundment was governed by the common-law principles in *Kennedy v. Justice of the District Court of Dukes County*, 356 Mass. 367, 252 N.E.2d 201 (1969) (*Kennedy*), rather than the statute addressing inquest reports enacted after the *Kennedy* decision. The Massachusetts Supreme Court held that the report and transcript became presumptively public documents once the district attorney filed a notice, which indicated that the grand jury returned an indictment, with the superior court stating. The case was remanded with instructions to vacate the judge's denial of the motion.

#Trial-Related

***Griffin v. State*, 19 A.3d 415 (Md. 2011), *cert. denied,* 96 A.3d 145 (Md. 2014)**

In this appeal of a second-degree murder conviction where a woman was shot seven times in a bathroom bar, the appellant argued that that court erred in allowing the state to introduce a printout of a witness' MySpace profile page that said "I HAVE 2 BEAUTIFUL KIDS.... FREE BOOZY!!!! JUST REMEMBER, SNITCHES GET STITCHES!! U KNOW WHO YOU ARE!!" without proper authentication. The court noted that it saw "no reason why social media profiles may not be circumstantially authenticated in the same manner as other electronic communication - by their content." The court held that the evidence was authentic because the MySpace page identified the user's birth date, discussed her boyfriend, Boozy, and displayed her photograph within the MySpace page.

#Trial-Related

#Social Media

***J.B. v. N.J. State Parole Bd.,* 79 A.3d 467 (N.J. Super. Ct. App. Div. 2013), *cert. denied,* B.M. v. N.J. State Parole Bd., 88 A.3d 192 (N.J. 2014)**

The appellants, who were convicted of sex offenses, challenged terms of post-incarceration supervision that restricted their access to "social media web sites on the Internet" on, among other things, First Amendment and due process grounds. The Appellate Division rejected the *per se* challenge: "The manifest objective of the Internet restrictions in the authorizing statute and the Parole Board's regulations is not to eliminate the ability of released offenders *** to access the Internet in its entirety. Instead, the provisions are legitimately aimed at restricting such offenders from participating in unwholesome interactive discussions on the Internet with children or strangers who might fall prey to their potential recidivist behavior." The court did, however, "urge the Parole Board to be amenable to fine-tuning the Internet regulations as technology advances and the nomenclature and uses of cyberspace continue to evolve."

#Miscellaneous

***Kelly v. State,* 82 A.3d 205 (2013), *cert. denied*, 135 S. Ct. 401 (2014)**

Over an eleven-day period in 2010, police conducted warrantless tracking of the defendant's vehicle via a GPS device attached to it. The tracking led to the issuance of search warrants for various properties and charges being filed against the defendant for burglary. The defendant moved to suppress evidence, arguing that the placement of the device violated the Fourth Amendment. The motions were denied. The defendant was convicted and appealed. *United States v. Jones* was decided while the appeal was pending. The Maryland Court of Special Appeals affirmed: Pre-*Jones* law in Maryland permitted warrantless tracking and, because the police had acted in "objectively reasonable reliance" on "binding appellate precedent," suppression was not appropriate.

#Fourth Amendment Good Faith Exception

***Kobman v. Commonwealth,* 777 S.E.2d 565 (Va. Ct. App. 2015)**

The defendant was convicted on multiple counts of possession of child pornography. The Commonwealth had secured a warrant to search the defendant's residence for evidence of child pornography. In response to a statement he made, the Commonwealth seized various devices and media. Images were found in the recycle bin and unallocated space of seized computers. The images were retrievable by the defendant from recycle bins but those in allocated space were "invisible" and required specialized software to retrieve. The Virginia Court of Appeals held that there was no evidence that the defendant was "aware of, or exercised dominion and control"

over the images in the unallocated space and reversed his convictions as to those images. As to the images in the recycle bin, the court held that there was sufficient evidence that the defendant "was aware of the presence of the *** illicit photographs *** and exercised dominion and control over the contraband."

#Trial-Related

#Miscellaneous

***Long v. State,* No. PD-0984-15 (Tex. Crim. App. June 28, 2017)**

The defendant's daughter made a "surreptitious recording" of speeches made by a public high school basketball coach in a locker room of a public high school. The appellant was convicted under the Texas wiretap statute of procuring the recording and disclosing it to an assistant principal. The statute required that the speaker have a reasonable expectation of privacy in making the oral communication. The Court of Appeals reversed the lower court's decision that the coach had no reasonable expectation of privacy. The court explained that the coach "had a subjective expectation of privacy that society is prepared to regard as objectively reasonable when he uttered that communication within the girls' locker room."

#Fourth Amendment Warrant Required or Not

***Love v. State,* No. AP-77, 024 (Tex. Ct. Crim. App. Dec. 7, 2016)**

The defendant moved during trial to suppress evidence of text messages offered against him, arguing that the messages were inadmissible because these were secured without a warrant. The State argued that the messages had been properly obtained through a court order compelling production of cell phone records from the defendant's service provider pursuant to Section 2703(d) of the SCA. The trial court overruled the objection and the defendant was convicted of capital murder. He challenged the ruling on appeal. The Court of Criminal Appeals held that text messages were analogous to "regular mail and email communications" such that content was distinguishable from routing information and that, since service providers had no business purpose for keeping content, the defendant had a reasonable expectation of privacy in the content. Accordingly, the third-party doctrine did not apply and a warrant supported by probable cause was required. The court then held that, as there was no warrant and no showing of probable cause, a statutory good faith exception to the exclusionary rule did not apply and the messages should have been suppressed. The court reversed and remanded for a new trial because it could not conclude that the admission of the text messages was harmless.

#Admissibility

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

#Third-Party Doctrine

***Lowe v. Mississippi,* 127 So.3d 178 (Miss. 2013)**

"The State indicted *** Lowe on five counts of exploitation of a minor, alleging that he had downloaded sexually explicit images and videos of children via the Internet to his laptop computer. Because the State had no direct evidence ***, its case depended on the opinions of its expert witnesses." The defendant's request for funds to retain his own expert was denied and he was convicted. The Mississippi Supreme Court reversed: "Because the trial court's denial of Lowe's requested expert funds denied him the opportunity to prepare an adequate defense, the decision rendered Lowe's trial fundamentally unfair." The court rejected the State's argument that there was overwhelming evidence against the defendant because that evidence "primarily consists of opinions provided by the State's expert."

#Trial-Related

***In re M.C.,* No. 64839 (Nev. Feb. 26, 2015)**

The appellant was adjudicated a delinquent based on a threatening Facebook posting. His post was discovered by a police officer who "monitored the Facebook activity of approximately 130 individuals by befriending them under a fictitious name." Affirming the adjudication, the Nevada Supreme Court held that the officer's monitoring did not violate the Fourth Amendment: "As soon as he released the post to a third party—specifically, his Facebook friends—M.C. lost any objectively reasonable expectation of privacy." The court also held that the posting had been properly authenticated through the officer's testimony: "he admitted making the *** post, subsequent communications referred back to that post, and there is no indication that someone else accessed his Facebook account." Moreover, the officer's testimony was not hearsay because the content of the post were party admissions.

#Fourth Amendment Warrant Required or Not

#Trial Materials

#Social Media

***McCaleb v. Commonwealth*, No. 2016-CA-000433-MR (Ky. Ct. App. Nov. 3, 2017)**

The defendant was indicted for burglary and theft. He appealed from a trial order granting the Commonwealth's motion to forfeit all the pictures of the various items of clothing seized from him. The Court of Appeals affirmed the trial court's decision: "It is undisputed that the undergarments themselves constituted "property held in violation" of Kentucky law. Defendant stole the items not for their innate market value but to satisfy his sexual fetish. The "mere fact that defendant converted these highly personal items to a digital platform" should not shield these images from forfeiture. "Under the unique facts of this case, allowing McCaleb to retain the images would in effect allow him to retain the fruits of his crime for the purpose for which he intended them." The Court also dismissed the defendant's argument "that some of the photographs in question are not of items relating to his convictions" as the issue was not raised before the trial court.

#Trial related

#Miscellaneous

***In re Maine Today Media Inc.*, 59 A.3d 499 (Me. 2013)**

The trial court in this criminal case initiated jury selection through a process regularly used in Maine courts that provided for extensive individual voir dire, with the practical effect that the public was excluded from the voir dire process. After jury selection had begun, the trial court received a letter from counsel for a media company asserting a greater right to public access. The court initially agreed to open the process to the public upon the defendant's agreement. After considering his options and consultation with his attorney, however, the defendant expressed concerns about the ability to draw an impartial jury if the process used by the court was changed. The court then agreed to continue with the individual voir dire process. After jury selection had begun, the media company filed a motion to intervene. Given the lateness of the request and a concern that juror candor would be reduced, the trial court denied the motion. The media company filed an interlocutory appeal. The Supreme Court of Maine held that, although the trial court exercises substantial discretion over the mode and conduct of voir dire, the trial court's generalized concern that juror candor might be reduced if voir dire was conducted in public was insufficient to bar the public or media from the entirety of the process. Accordingly, the matter was remanded for the trial court "to conduct the remaining voir dire in a presumptively public manner, exercising its considerable discretion to prevent the dissemination of sensitive juror information." The Supreme Court stated that public's access to the jury selection that already occurred could be "addressed, at the court's discretion, by the release of appropriately redacted transcripts.

#Trial-Related

***In re Malik J.*, 193 Cal. Rptr. 3d 370 (Ct. App. 2015)**

A minor had been adjudicated a delinquent and conditions of probation imposed on him. After he admitted violating the conditions by committing robberies that might have been furthered through the use of electronic devices, additional terms were imposed, including that he and his family "provide all passwords and submit to searches of electronic devices and social media sites." The Court of Appeal modified the conditions to omit the reference to the minor's family as well as the requirement that the minor turn over passwords to social media accounts. The conditions were also modified to restrict searches to devices found in his custody or control as these might be stolen property.

#Miscellaneous

***In re Mike H.,* No. D069391 (Cal. Ct. App. Mar. 30, 2017)**

The juvenile in this matter was adjudged a ward of the State after admitting to sodomy of a minor. He appealed from various conditions of probation imposed on him that, among other things, "limit and facilitate searches of his Internet and computer activity." Among other things, the Court of Appeal struck broad conditions that restricted the juvenile's Internet and computer use because these were "unrelated to the offense, do not involve conduct that is itself criminal, and bear no reasonable relationship to preventing future criminality." The Court of Appeal affirmed conditions that barred the juvenile from "anonymizing his presence on the Internet" because those were reasonably related to "deter future criminality by preventing further contact with the victim" and did not violate the juvenile's First Amendment rights because the conditions were narrowly tailored to "serve the compelling state interest of assisting Mike's reformation and rehabilitation." The Court of Appeal vacated as being constitutionally overbroad a condition that prohibited the juvenile from knowingly using or possessing an electronic device with encryption "because, if read literally, it would prohibit him from using the Internet or possessing a modern smartphone" given the "ubiquity of encryption technology." It remanded and invited modification to narrow the condition.

#Encryption #Probation and Supervised Release

#Social Media

***Moats v. State,* 148 A.3d 51 (Md. Ct. Spec. App. 2016), *aff'd,* No. 89 (Md. Aug. 31, 2017)**

The defendant was convicted of possession of child pornography. He argued on appeal that the court below erred in denying his pretrial motion to suppress. Law enforcement had arrested the defendant on drug offenses and for sexual assault. His cell phone was seized incident to arrest and retained by law enforcement after the defendant was released from custody. Law

enforcement thereafter secured a warrant to search the phone for evidence of the crimes with which the defendant had been charged. Sexually explicit photos and a video of a young woman were discovered during the search. The court affirmed the denial of the motion. It concluded that law enforcement had probable cause to seize the phone for the time necessary to obtain a warrant. The record supported these findings.

#Trial-Related

#Miscellaneous

***In re P.O.,* 200 Cal. Rptr. 3d 841 (Ct. App. 2016)**

A juvenile was declared a ward of the court and put on probation after he admitted to a misdemeanor count of public intoxication. He challenged on appeal a condition of probation that required him to submit to warrantless searches of his "electronics including passwords." The appellate court concluded that the condition was overbroad because it was "not narrowly tailored to its purpose of furthering his rehabilitation." The court modified the condition to "limit authorization of warrantless searches of P.O.'s cell phone data and electronic accounts to media of communication reasonably likely to reveal whether he is boasting about drug use or otherwise involved with drugs." The court also required the juvenile to disclose passwords only to such accounts.

#Miscellaneous

#Social Media

***People v. Austin*, No. 97 (N.Y. October 19, 2017)**

The defendant was convicted of third-degree burglary and fourth-degree criminal mischief. On appeal, he argued that his Sixth Amendment right to confrontation was violated by the introduction of DNA evidence through witness testimony. The Court of Appeals reversed the lower court's order denying defendant's request that the jury be given an adverse inference charge based on the unavailability of blood evidence at trial: "defendant was entitled to cross-examine the analyst who either performed, witnessed or supervised the generation of the critical numerical DNA profile" or who "used his or her independent analysis on the raw data." "The criminalist's testimony was nothing more than a parroting of hearsay statements, made by other analysts and of which he had no personal knowledge. There is no question that his testimony as to the findings and conclusions of the nontestifying witnesses was elicited in order to prove the truth of those extrajudicial assertions — primarily, identifying defendant as the burglar."

#Sixth Amendment Right of Confrontation

***People v. Badalamenti,* 54 N.E.3d 32 (N.Y. 2016)**

The defendant was convicted of various offenses arising out of child abuse. He lived with his girlfriend and her five-year old child. The child's father had visitation rights and became concerned for the child's safety. While attempting to reach the mother on her cell phone, he recorded defendant threatening the child. Later, the defendant was arrested for beating the child and the recording was introduced into evidence at trial over the defendant's objection that it was "eavesdropping" prohibited by State law. New York law prohibited "intentional overhearing or recording of a telephonic *** communication by a person other than a sender or receiver thereof, without the consent of either the sender or receiver." The Appellate Division affirmed. Thereafter, the Court of Appeals held that the father gave "vicarious consent" to the recording on behalf of his child: "the record supports the conclusion of the courts below that the People have sufficiently demonstrated that the father had a good faith, objectively reasonable basis to believe that it was necessary for the welfare of his son to record the violent conversation he found himself listening to." It did so over a dissent that the majority disregarded principles of statutory interpretation in allowing vicarious consent when the controlling statute was silent on the subject.

#Miscellaneous

***People v. Barnes*, 157 Cal. Rptr. 3d 853 (Ct. App. 2013), *rev. denied,* No. A135131 (Cal. Sep. 18, 2013)**

The defendant entered a conditional plea to, among other things, armed robbery after his motion to suppress was denied. The defendant had stolen a wallet which contained a cell phone. Law enforcement, with the consent of the owner of the stolen phone, used GPS data to locate the defendant. Affirming the denial of the motion, the Court of Appeals held that the defendant had no reasonable expectation of privacy in data generated from a stolen phone. The court also rejected the argument that the data could not be "verified."

[Note that the court here distinguished *United States v. Jones* on various grounds].

#Fourth Amendment Warrant Required or Not

***People v. Bryant,* 215 Cal. Rptr. 3d 740 (Ct. App. 2017), *rev. granted,* 219 Cal. Rptr. 3d 473 (2017)**

The defendant was convicted of possessing a concealed, loaded, unregistered firearm in a vehicle. The court imposed a two-year sentence, some of which was to be served under mandatory supervision. The defendant was required to submit to searches of "any text messages,

emails, and photographs on any cellular phone or other electronic device in his possession or residence. The Court of Appeal held that the condition was invalid under controlling precedent because the condition was not "reasonably related to preventing future criminality." Among other things, there was no showing of a connection between the defendant's use of a cell phone and any criminality or how the condition would reasonably prevent future crime.

#Probation and Supervised Release

***People v. Diaz*, 153 Cal. Rptr. 3d 90 (Ct. App. 2013), *rev. denied,* No. S209134 (Cal. Apr. 17, 2013)**

The defendant appealed her conviction for involuntary manslaughter and vehicular manslaughter while intoxicated. The defendant contended that, "the admission of evidence obtained through the warrantless seizure of the sensing diagnostic module (SDM) from her previously impounded vehicle and the downloading of data from the device violated her Fourth Amendment rights." The data seized pertained to the vehicle's speed and braking immediately before a deadly impact and the vehicle had been impounded. The Court of Appeal affirmed.

Addressing an issue of first impression in California, the court held: (1) The "automobile exception" to the warrant requirement was applicable, (2) probable cause existed for the search of the SDM, and (3) the scope of the warrantless search was not unreasonable. The court also held that the warrantless search was valid because the vehicle was itself evidence of the crime.

The Court of Appeal rejected the defendant's reliance on *United States v. Jones*: "Here, the trespass theory underlying Jones has no relevance and *** the purpose of the SDM was not to obtain information for the police."

#Fourth Amendment Exigent Circumstances

***People v. Diaz,* 119 Cal. Rptr. 3d 105 (2011), *cert. denied*, 132 S. Ct. 94 (2011)**

The defendant pled guilty to transportation of a controlled substance. On appeal, he challenged the denial of his motion to suppress evidence derived from the warrantless search of the contents of his cell phone. The contents had been searched some 90 minutes after the defendant had been arrested. Over a strong dissent, the California Supreme Court affirmed, holding that the search was incident to the defendant's lawful arrest. The court analogized the cell phone to clothing worn by an arrestee or a cigarette case taken from the arrestee's person. The court also rejected the argument that the validity of a search incident to arrest should depend on the "nature and character" of the item seized.

The majority closed by noting that it was bound by decisions of the United States Supreme Court

and that, if "the wisdom of the high court's decisions 'must be newly evaluated' in light of modern technology ..., then that reevaluation must be undertaken by the high court itself."

#Fourth Amendment Warrant Required or Not

***People v. Durant,* 44 N.E.3d 173 (N.Y. 2015)**

The defendant was convicted of robbery. On appeal, he challenged the trial court's failure to give a permissive adverse instruction because the police did not electronically record his custodial interrogation. The Appellate Division affirmed, as did the Court of Appeals: "defendant's proposed jury instruction was neither required as a penalty for governmental misfeasance nor akin to a missing witness charge ***." Although the Court of Appeals declined to adopt a categorical rule that adverse inference instructions should be given whenever an interrogation was not recorded it did "recognize the broad consensus that electronic recording of interrogations has tremendous value" and noted the "commendable efforts of various groups to address the question.

#Miscellaneous

#Preservation and Spoliation

***People v. Goldsmith,* 172 Cal. Rptr. 3d 637 (2014), *cert. denied*, 135 S. Ct. 763 (2014)**

The defendant was found guilty of failing to stop at a traffic light at an intersection based on evidence generated by an "automated traffic enforcement system (ATES)" that was introduced into evidence by an officer. She argued on appeal that the evidence had not been properly authenticated and constituted hearsay. The California Supreme Court affirmed the conviction. *Permissive* statutory presumptions supported the finding that the evidence was accurate representations of data stored in the ATES. The officer's testimony was sufficient to support a finding that the evidence was genuine. The Supreme Court rejected the argument that testimony from someone with "special expertise" was necessary because digital images were involved. Further, the court held that the evidence was not a "statement of a person" and was therefore not hearsay.

#Trial Materials

***People v. Harris,* No. F072865 (Cal. Ct. App. Dec. 29, 2016)**

The defendant and his victim had been in a "on-and-off dating relationship." Among other things, he struck the victim with brooms and thereafter pled no contest to assault with a deadly weapon. He was granted probation with a number of conditions, including one that required him to submit

"electronic and cellular devices" to warrantless search and seizure. He appealed from the condition, arguing that it was invalid. The Court of Appeal held that the condition was reasonably related to preventing future criminality. "Defendant is subject to a criminal protective order and a probation condition prohibiting him from contacting the victim in any way, including electronically," and the condition enabled the probation officer to monitor the defendant's compliance. However, the court held the condition overbroad as it applied to *all* of the defendant's electronic data, struck the condition, and remanded for the trial court to fashion a more tailored one.

#Miscellaneous

***People v. Harris*, N.Y.S.2d 590 (Crim. Ct. 2012), *appeal dismissed,* 988 N.Y.S.2d 524 (App. Div. 2014)**

After the defendant was charged with disorderly conduct, the government sent subpoena duces tecum to third-party online social networking service provider Twitter, seeking to obtain the defendant's user information and Twitter postings ("tweets") during a relevant period. The defendant's motion to quash was denied for lack of standing. The provider then moved to quash. The court stated that it was a case of first impression, "distinctive because it is a criminal case rather than a civil case, and the movant is the corporate entity (Twitter) and not an individual." In denying Twitter's motion, the court rejected its arguments that the defendant had standing to challenge the subpoena, a Fourth Amendment privacy interest, and that the subpoena and order violated the SCA. The court noted there was no physical intrusion into the defendant's personal property -- the Twitter account -- because defendant "had purposely broadcast to the entire world into a server 3,000 miles away." Further, there was no reasonable expectation of privacy in the tweets because "If you post a tweet, just like if you scream it out the window." The court distinguished a tweet from a "private email, a private direct message, a private chat, or any of the other readily available ways to have a private conversation via the internet that now exist." To access those private dialogues, the court said, a warrant based on probable cause was required. The court found no unreasonable burden to Twitter, "as it does not take much to search and provide the data to the court." The court added: "[s]o long as the third party is in possession of the materials, the court may issue an order for the materials from the third party when the materials are relevant and evidentiary."

#Trial-Related

#Social Media

***People v. Holmes,* Case No. 12CR1522 (Colo. Dist. Ct. Nov. 7, 2013)**

The defendant moved to suppress records obtained by law enforcement from two Internet

dating sites. The motion was denied: "Part of the motion is moot because the prosecution does not intend to introduce into evidence records containing any communications between the defendant and other members of the websites. The rest of the motion fails because the defendant did not meet his burden of demonstrating a constitutionally protected expectation of privacy in the profile records and subscription records." As to the latter ruling, the court reasoned that the defendant had no reasonable expectation of privacy under the Colorado or United States constitutions because he "posted his profiles with the intent to make them accessible and, because, before law enforcement had sought the records, the profiles had been published. As to the subscription records, the court drew an analogy between voluntarily submitting information to an internet site administrator and submitting voluntarily information to third-parties such as telephone companies (*citing Smith v. Maryland,* 442 U.S. 735 (1979)), and found that the defendant had no reasonable expectation of privacy under the Fourth Amendment. The court also distinguished prior Colorado rulings and held there was no reasonable expectation under Colorado law.

#Fourth Amendment Warrant Required or Not

***People v. John,* 52 N.E.3d 1114 (N.Y. 2016)**

The defendant was convicted of criminal possession of a weapon and menacing. Evidence offered against him included reports which asserted that the defendant's "DNA profile" matched DNA found on a weapon and a DNA sample. The State did not present any witness who "conducted, witnessed or supervised the laboratory's generation of the DNA profile from the gun or defendant's exemplar." Following *Bullcoming v. New Mexico,* 564 U.S. 647 (2011) and prior New York case law, the Court of Appeals held that the defendant's Sixth Amendment right of confrontation had been violated, reversed the conviction, and remanded for a new trial."

#Trial-Related

#Miscellaneous

***People v. Kent*, 910 N.Y.S.2d 78 (App. Div. 2010), *aff'd as modified,* 19 N.Y.3d 290 (2012)**

The defendant, a college professor, had been convicted of child pornography-related offenses after an employee of the college had run a virus scan on the defendant's office computer and found files of young girls, after which the college turned the hard drive over to police along with a "Consent to Search" form. In affirming the judgment of conviction, the Appellate Division addressed questions of first impression in New York. Among other things, the court held that "the mere existence of an image automatically stored in the cache, standing alone, is legally insufficient to prove either knowing procurement or knowing possession of child pornography." However, there was sufficient evidence to support the defendant's conviction. The court also

rejected an ineffective assistance argument based on the failure of defense counsel to move to suppress the evidence collected from the hard drive. The defendant had no reasonable expectation of privacy in any personal files stored on his office computer because the computer was the property of the college and, therefore, there was a legitimate explanation for counsel's conduct.

#Miscellaneous

***People v. Klapper,* 902 N.Y.S.2d 305 (Crim Ct. 2010)**

The defendant was charged with unauthorized use of a computer under New York law. The defendant was alleged to have installed keystroke tracking software on a computer in his office and to have used that software to access the personal email account of an employee. On a motion to dismiss, the court held the allegations did not establish that the access was "without authorization." The defendant's ownership of, and authority over, the computer were of central importance. Moreover, the employee had a diminished expectation of privacy in the email communications. Absent allegations that the defendant had exceeded his right of access or that there was some restriction on that right, the motion was granted.

#Miscellaneous

***People v. Lewis,* 12 N.E.3d 1091 (N.Y. 2014)**

The defendant was convicted of various offenses arising out of his use of forged credit cards in Manhattan. His phones were tapped pursuant to a warrant. He was under visual surveillance. However, because of traffic congestion in Manhattan, investigators installed a GPS tracking device on his vehicle without a warrant. After his conviction, the defendant challenged (among other things) the warrantless installation. The Court of Appeals affirmed. The Court acknowledged that the warrantless installation was unconstitutional under *United States v. Jones.* However, "the use of the GPS device, although amounting to a constitutional violation, was nonetheless harmless because it provided information redundant to that which investigators had already obtained legally. The People also presented overwhelming evidence of defendant's guilt ***."

#Fourth Amendment Warrant Required or Not

#Miscellaneous

***People v. Lopez,* No. H041713 (Cal. Ct. App. Jan. 25, 2016), *rev. denied,* No. S232792 (Cal. April 27, 2016)**

The appellant, a juvenile, pled guilty to vehicle theft with a prior criminal conviction. He challenged two conditions of probation on appeal, one of which required him to give his probation officer passwords to any "social media sites." The appellate court affirmed the imposition of the condition, rejecting the appellant's argument that the term was unconstitutionally vague given, among other things, clarification by the judge who imposed the condition. The appellate court also rejected the argument that the condition was unconstitutionally overbroad given that "the state's interest in preventing the defendant from continuing to associate with gangs and participate in gang activities outweighed the minimal invasion of his privacy."

#Miscellaneous

#Social Media

***People v. Nakai*, 107 Cal. Rptr. 3d 402 (Ct. App. 2010), *rev. denied,* No. S182558 (Cal. July 21, 2010)**

The defendant was found guilty under California law of attempting to send harmful material to a minor with intent to seduce. On appeal, the conviction was affirmed. Although the defendant wanted a Yahoo! dialogue with someone posing as a minor to be confidential, he had no reasonable expectation of privacy. Among other things, the defendant was on notice that dialogues might be shared in the investigation of illegal conduct and that others might have access to the dialogue.

#Trial-Related

***People v. Pakeman,* No. A148084, A146013 (Cal. Ct. App. Jan. 24, 2017), *rev. denied,* No. S239740 (Cal. Mar. 29, 2017)**

The defendant was convicted of pimping, pandering, and domestic violence. He argued on appeal, among other things, that the State's production shortly before trial of some 6,800 pages downloaded from his cell phone violated his rights to due process and effective assistance of counsel. The Court of Appeal affirmed. After the defendant rejected the final plea offer, the prosecutor provided defense counsel with a thumb drive that contained the pages. Thereafter, at the urging of the trial court, the prosecutor agreed to seek to admit only 200 pages at trial. The defendant insisted on his right to a speedy trial and there was no evidence that defense counsel was unprepared. The court also rejected the defendant's argument that his counsel had been ineffective because counsel failed to move to suppress the data stored on the cell phone. The warrant authorized the search and seizure of the pages admitted into evidence, the pages were "clearly" admissible, and there was overwhelming proof of the defendant's guilt.

#Discovery Materials

#Miscellaneous

#Trial-Related

***People v. Price,* 80 N.E.3d 1005 (N.Y. 2017)**

The defendant was convicted of robbery. A witness to the robbery testified at trial that he had seen someone holding a gun but never saw the gunman's face and was unable to identify the defendant as a robber. The People then offered a photo "'found on the internet,' which purportedly depicted defendant holding a handgun." Over the defendant's objection the trial court ruled the photo admissible. It was shown to the victim, who testified that the gun in the photo was "similar" to the one used in the robbery but that he could not identify the gun as being the one used by the robber. The photo was taken by a detective who used the defendant's surname to search the Internet and found a public profile that contained photographs of the defendant holding a gun. There was no testimony that the content of the profile matched the defendant's pedigree information and there was no testimony surrounding the taking of the photo. On leave to appeal, the Court of Appeals reversed and remanded for a new trial. The court described various means to identify a photo and held that the photo in issue had not been authenticated at trial because the victim was unable to identify the weapon used in the robbery and no witness testified that the photo was a fair and accurate depiction. The court also rejected the People's argument that, even assuming that the photo might have been authenticated through the defendant's connection to the profile, there was an insufficient foundation to tie the defendant to it. The majority of the Court of Appeals disagreed with the opinion of a concurring judge, who proposed adoption of a controlling test for authentication in all cases "involving authentication of photographs found on a social media network web page," and concluded that it would be "more prudent to proceed with caution in a new and unsettled area of the law such as this."

#Admissibility

#Trial-Related

***People v. R.D.,* No. 14CA1800 (Colo. Ct. App. Dec. 29, 2016), *cert. granted,* No. 17SC116 (Colo. Sep. 5, 2017)**

The appellant was adjudicated a delinquent based on conduct that if committed by an adult

would constitute the crime of harassment. The conduct consisted of multiple tweets the juvenile made to a student in a different school. The Court of Appeals reversed, concluding that the tweets were neither true threats nor fighting words such that, as applied, the statute under which he was charged violated the juvenile's First Amendment rights. Among other things, the court differentiated tweets posted on a public forum (as before it) from "e-mails and other social media messages, which are sent directly – and usually privately – to a person or specified group of people." The court also held that "close physical proximity to the recipient" was required for the tweets to be fighting words and that there was no such proximity.

#Miscellaneous

#Social Media

***People v. Relerford,* 56 N.E.3d 489 (Ill. App. Ct. 2016), *appeal pending*, 65 N.E.3d 845 (Ill. Nov. 23, 2016)**

The defendant was convicted of stalking and cyberstalking under Illinois law. After the defendant was convicted the United States Supreme Court decided *Elonis v. United States,* 135 S. Ct. 2001 (2015) (*q.v.*), which held that a defendant's due process right was violated when he was convicted under a federal stalking statute that premised a defendant's guilt on how a reasonable person would understand the posts there in issue. Applying *Elonis,* the Illinois appellate court vacated the defendant's conviction because the statutes under which he was convicted similarly lacked a *mens rea* requirement.

#Miscellaneous

#Social Media

***People v. Sandee*, 222 Cal. Rptr. 3d 858 (Ca. Ct. App. 2017)**

After a denial of probationer's motion to suppress evidence obtained from the search of her cell phone in trial court, she brought this appeal contending that although she was subject to a general search condition of her "property" and "personal effects" without a warrant, the scope of the search did not extend to her cell phone. Sandee also argued that under the Electronic Communications Privacy Act (ECPA), the search was illegal because she did not consent to the search of her cell phone. Here, the court reasoned that "a reasonable person at the time the search was conducted would understand the terms "property" and "personal effects" to include [her] cell phone and the data it contained. However, the Court refused to apply the ECPA because it came into effect *after* the search was conducted. Thus, the Court adhered to California precedent focusing only *at the time of the search*, and rejected Sandee's ECPA argument.

#Fourth Amendment Warrant Required or Not

#ECPA

***People v. Smith,* No. 1-14-1814 (Ill. App. Ct. Mar. 1, 2017), *appeal denied,* No. 122199, (Ill. Sep. 27, 2017)**

"Trial counsel was ineffective for failing to challenge the State's failure to provide a proper foundation for the admission of lay opinion testimony regarding sophisticated surveillance technology used by the police to track and arrest the defendant. Absent a proper foundation, the remainder of the State's evidence was vacant of any probable cause or reasonable suspicion to arrest the defendant. As a result, there is a reasonable probability that absent counsel's failure to object to the admission of the improperly introduced lay opinion testimony, the defendant's motion to quash would have been granted, and the State would have been without any evidence with which to proceed against the defendant at trial. Accordingly, the cause is reversed and remanded for a new motion to quash and suppress hearing and the defendant is appointed new counsel."

#Admissibility

#Miscellaneous

#Sixth Amendment Assistance of Counsel

#Trial-Related

***People v. Superior Court (Chubbs*), No. B258569 (Cal. Ct. App. Jan. 9, 2015)**

In 2011, as part of a "cold case investigation," a DNA test was conducted on vaginal swabs from the victim of a 1977 murder. In 2012, the defendant was arrested for an unrelated reason and his DNA was found to match that taken from the victim. The defendant was charged with the murder. Thereafter, a lab conducted further testing of the victim's DNA through the use of its "TrueAllele software" and issued a report that further incriminated the defendant. The defendant moved to compel production of the source codes for the software. After a series of procedural "meanderings" the trial court ordered that the source codes be disclosed. The People took an interlocutory appeal which the Court of Appeal granted. The parties did not dispute that the source code was a trade secret. The Court of Appeal held that the holder of a trade secret could not be compelled to disclose it under California law, "even subject to a protective order and the closing of certain proceedings, without a showing that the trade secret is relevant and necessary to the defense." On the facts before it, Chubbs [the defendant] has received extensive

information regarding TrueAlelle's methodology and underlying assumptions, but he has not demonstrated how TrueAlelle's source code is necessary to his ability to test the reliability of its results. We therefore conclude that Chubbs has not made a prima facie showing of the particularized need for TrueAlelle's source code. The Court of Appeal also rejected the defendant's argument that his right of confrontation required that the source code be disclosed because the right did not apply to *pretrial* discovery of privileged information.

#Discovery Materials

#Trial-Related

***People v. Valdez*, 135 Cal. Rptr. 3d 628 (Ct. App. 2011), *rev denied,* No. S199558 (Cal. Mar. 28, 2012)**

The defendant was convicted of two counts of attempted murder, four counts of assault with a firearm, and two counts of street terrorism. On appeal, the defendant contended the trial court erroneously admitted pages from his MySpace social networking site that included his gang moniker ("Yums"), a photograph of him making a gang hand signal, and written notations including "T.L.F.," "YUM $ YUM," "T.L.F.'s '63 Impala," "T.L.F., The Most Wanted Krew by the Cops and Ladiez," and "Yums You Don't Wanna F wit[h] this Guy." The MySpace page included the following under "Groups": "CO 2006, Thug *****Life/Club Bounce. O.C.'s Most Wanted G's. Viva Los Jews. Screaming Thug Life" and, in an interests section, stated: "Mob[b]ing the streets and hustling, chilling with homies, and spending time with my mom." An investigator from the district attorney's office testified he printed out the web pages a year *before* the shootings, after accessing them as part of his internet search using the terms "T.L.F. Santa Ana. The gang expert relied on the MySpace page and other evidence as a basis for his opinion that the defendant was an active T.L.F. gang member. The defendant objected to admission of the MySpace evidence based on lack of authentication, hearsay, and that it was more prejudicial than probative. The trial court admitted the MySpace printouts for specified purposes and not for the truth of any express or implied assertions. In particular, the court instructed the jury to consider the MySpace evidence for the limited purposes of (1) corroborating a victim's statement to investigators shortly after the first shooting that the victim recognized the defendant from the MySpace site, and (2) as foundation for the gang expert's testimony. The appellate court affirmed, finding the MySpace evidence sufficiently authenticated, not improper hearsay evidence, and not unduly prejudicial.

#Trial-Related

***People v. Weissman*, 997 N.Y.S.2d 602 (Crim. Ct. 2014)**

In this post-*Riley* trial court decision, the defendant had been charged with two counts of criminal

contempt for using his cell phone inside a courthouse to take pictures in violation of a rule. The defendant was observed inside a courtroom with his phone apparently turned on, although there was no proof that he had used the phone to take pictures. The defendant was similarly observed in a corridor. A court officer in the corridor directed the defendant to show images on the phone to the officer, one of which appeared to be that of a witness. An officer inside the courtroom then did the same and observed an image of a witness. The defendant moved to suppress and the motion was granted. Although the court acknowledged that the defendant had a diminishing expectation of privacy in a courthouse, the judge found that the defendant had been coerced in giving the officers access to the images.

#Fourth Amendment Warrant Required or Not

***Restrepo v. Carrera,* 189 So. 3d 1033 (Fla. Dist. Ct. App. 2016)**

The defendant in this civil action sought *certiorari* relief from an order requiring her to "provide cell phone numbers and/or names of providers used" during six-hour periods before and after a crash. The appellate court quashing the order, concluded that compelling the information sought while her criminal case was pending would violate the petitioner's Fifth Amendment rights. However, the court expressed no opinion on the "status of the petitioner's Fifth Amendment rights once her criminal case has concluded."

#Fifth Amendment Self-Incrimination

***Rutland Herald v. Vermont State Police*, 49 A.3d 91 (Vt. 2012)**

The plaintiffs made a public records request to the state police relating to a criminal investigation into the possession of child pornography by employees at a state police academy. The State refused, citing statutory provisions permitting the withholding of records dealing with the detection and investigation of crime. The plaintiffs filed suit and the trial court granted summary judgment in favor of the state. The appellate court affirmed and held that the legislative intent of the state public records act was that criminal investigative records be permanently exempt, citing the omission of temporal language in this area that pervades other areas of the PRA.

#Trial-Related

***Sinclair v. State,* 118 A.3d 872 (Md. 2015)**

After conviction on carjacking-related charges, the petitioner appealed from the denial of his motion to suppress incriminatory images taken from his flip phone seized and searched incident to arrest. Between the conviction and the acceptance of the appeal the United States Supreme Court decided *Riley v. California*. Although the Maryland Court of Appeals held that the Petitioner

had waived his right to move to suppress, it nevertheless held that one image was of a screen saver "readily apparent" to the arresting officer and was admissible under the plain view doctrine:

Under the categorical approach favored by the Supreme Court in *Riley,* an officer who seizes a flip cell phone incident to an arrest may physically inspect and secure the phone, which would include an examination of the phone and its case for weapons, powering off the phone, and removing its batteries. Such actions would inevitably involve physically opening a flip phone, although they would not entail a search of its data. Thus, physically opening a cell phone would not be an unlawful search under *Riley*. And a photograph of a screen server image in plain view when the phone is physically opened—an image that the investigator immediately recognized as the stolen item under investigation—would not be subject to suppression. The officer found two other images in his warrantless search. The Court of Appeals held that admission (one being identical to the screen server image) was harmless error.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Plain View

***Smallwood v. State*, 113 So. 3d 724 (Fla. 2013)**

The defendant was arrested for, among other things, armed robbery. His cell phone was seized during a search incident to arrest. After the defendant had been secured, the arresting officer accessed and searched the content of the phone. The officer saw five images relevant to the crime. Thereafter, the prosecutor obtained a search warrant and viewed the images. Over the defendant's objection, the trial court allowed the images into evidence. On appeal, the intermediate appellate court affirmed the defendant's convictions but certified a question to the Supreme Court with regard to the search incident to arrest. Distinguishing *United States v. Robinson,* 414 U.S. 218 (1973), the Florida Supreme Court held that, "the electronic devices that operate as cell phones of today are materially distinguishable from the static, limited-capacity cigarette pack in *Robinson,"* and that, under the facts before it, a warrant was required to search the phone: "In our view, allowing law enforcement to search an arrestee's cell phone without a warrant is akin to providing law enforcement with a key to access the home of the arrestee." The court rejected the State's attempt to rely on the good faith exception to the warrant requirement and reversed the convictions, concluding that the admissions of the images were not harmless error.

#Trial-Related

#Fourth Amendment Warrant Required or Not

***Smith v. State*, 136 So. 3d 424 (Miss. 2014)**

The defendant was convicted of capital murder in the death of a seventeen-month-old child. On appeal, he challenged, among other things, the admissibility of several Facebook messages. The Court of Appeals affirmed, holding the messages had been properly authenticated. The Mississippi Supreme Court granted *certiorari* to address the admissibility issue and affirmed the conviction but held that the Court of Appeals had erred on authentication.

The State had introduced at trial two Facebook messages and an email notification containing a Facebook message. However, the Supreme Court held that the State "failed to make a prima facie case that the Facebook profile whence the messages came belonged to Smith, as the only information tying the Facebook account to Smith is that the messages purport to be from a 'Scott Smith' and are accompanied by a very small, grainy, low-quality photograph that we can only assume purports to be Smith." Moreover, there was no *prima facie* showing that any messages were actually sent by the defendant. However, the defendant's conviction was affirmed as the evidence of his guilt was overwhelming. **[Note that the Court's analysis relies on, among other decisions, *Griffin v. State,* 419 Md. 343, 19 A.3d 415 (2011)].**

#Fourth Amendment Warrant Required or Not

#Social Media

***Spence v. State,* 118 A.3d 864 (Md. 2015)**

The petitioner sought to suppress evidence derived from his cell phone, the contents of which were searched without a warrant incident to his arrest. The Maryland Court of Appeals affirmed the denial of the motion based on the arresting officer's good faith reliance on pre-*Riley v. California* binding precedent.

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

***S.S.S. v. M.A.G.*, No. A-1623-09T2 (N.J. Super. Ct. App. Div. Oct. 14, 2010) (*per curiam*)**

This is a domestic violence action arising out of a failed relationship and an alleged assault. The trial judge granted relief to the plaintiff. In doing so, the trial judge refused to admit into evidence as hearsay records of the defendant's E-Z Pass use, which the defendant offered to show that he could not have been at the scene of the assault. The Appellate Division reversed. The records qualified as a "business record," were thus admissible as a hearsay exception, and exclusion was prejudicial in this "classic 'he said-she said' dispute."

#Trial-Related

***State v. Andrews,* 134 A.3d 324 (Md. Ct. Spec. App. 2016)**

"This case presents a Fourth Amendment issue of first impression in this State: whether a cell phone—a piece of technology so ubiquitous as to be on the person of practically every citizen—may be transformed into a real-time tracking device by the government without a warrant." Police used a cell site simulator known as "Hailstorm" to locate the defendant, who was wanted for attempted murder. The police secured a pen register/trap & trace order based on what the appellate court characterized to be a misleading application because the resulting order did not support the use of the stimulator. The defendant was found inside a residence and, after his arrest, the police secured a warrant to search the premises and found a weapon. A trial court found the warrantless use of the Hailstorm device to be an unreasonable search and suppressed all evidence obtained by the police as "fruit of the poisonous tree." On an interlocutory appeal, the appellate court concluded that "people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement *** and that people have an objectively reasonable expectation of privacy in real-time cell phone location information." Thus, a "valid search warrant, or an order satisfying the constitutional requisites of a warrant" was required for use of a simulator "unless an established exception to the warrant requirement applies." The court rejected the State's argument that the *Leon* good faith exception applied because of misleading application was misleading and "without the antecedent Fourth Amendment violation the nexus between the residence to be searched and the alleged criminal activity could not have been established."

There is a lot in this decision. Among other things, it addressed the admissibility of testimony about the stimulator, the effect of a nondisclosure agreement entered into by the State, and the distinction between historical and real-time CLSI, and the third-party doctrine. Also, note that the decision relied to some degree on the panel decision in *United States v. Graham* which was reversed *en banc* (*q.v.*).

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant required or Not

#Trial-Related

***State v. Ates*, 86 A.3d 710 (N.J. 2014), *cert. denied*, 135 S. Ct. 377 (2014)**

In the course of a murder investigation, law enforcement officials secured New Jersey court orders pursuant to the New Jersey Wiretap Act that allowed them to intercept communications over various phones. Intercepted communications included conversations between speakers in

Florida and Louisiana, including the defendant, a Florida resident, who was convicted of the murder. The defendant appealed, contending, among other things, that the Wiretap Act "should be declared unconstitutional because it permits New Jersey authorities to act outside their jurisdiction and wiretap individuals with no connection to New Jersey." The New Jersey Supreme Court rejected the argument: (1) Two findings that a judge must make under the Act "require a direct link to New Jersey;" (2) the "point of interception" as defined in the Act is a "listening post" in New Jersey.

#Miscellaneous

***State v. Bailey,* 989 A.2d 716 (Me. 2010)**

After conviction of various child pornography-related offenses, the defendant appealed from the denial of his motion to suppress evidence. Police had been led to the defendant's apartment through their investigation of a peer-to-peer networking program. After a search of a nearby home, the police learned that someone was using an unsecured wireless router to access the network and disseminate child pornography. After turning off the router, a detective gained access to the apartment by telling the defendant that he was canvassing the neighborhood to see if anyone had a problem with computers being wrongfully accessed. The detective then gained access to the defendant's computer with the defendant's consent and searched it for files containing child pornography. The detective found, but did not open, the files. The defendant then acknowledged having a "problem" with child pornography and consented to a physical search, which yielded tapes that further implicated the defendant and adverse witnesses. On appeal, the Supreme Judicial Court reversed. The court concluded that the defendant had standing to challenge the search of his computer: He had a reasonable expectation of privacy in the computer and its contents when not being accessed through the network. Next, the court held that the defendant had consented to the initial search of the computer. Under the circumstances, the detective's deception was not such as to vitiate the consent. However, the detective exceeded the scope of the consent when "he ran a general search for *all* of the video files" (emphasis in original). Suppressing the evidence secured through that search, the court remanded for consideration of an issue not on appeal: Whether other evidence should be suppressed as "the fruits of the poisonous tree."

#Fourth Amendment Warrant Required or Not

***State v. Bates,* No. CR-2016-370-2 (Ark. Cir. Ct. Mar. 6, 2017) ("Stipulation and Consent Order")**

Amazon had moved on First Amendment grounds to quash a warrant for production of "any audio recording created as a result of interactions with an Amazon Echo device owned by the defendant and located in his residence" over a 48-hour period. The warrant was issued as part of

a murder investigation. After the motion was filed the defendant consented to production and Amazon complied with the warrant, thus making the motion moot.

Information about this matter is available at, among other sites,

http://au.pcmag.com/consumer-electronics-reviews-ratings/46662/news/amazon-drops-fight-over-alexa-data-in-murder-case

#Miscellaneous

***State v. Bray,* 383 P.3d 883 (Or. Ct. App. 2016), *rev. granted,* 397 P.3d 30 (Or. 2017)**

The defendant was convicted of various sexual assault-related crimes. On appeal, he argued that the trial court erred in refusing to compel the prosecution to secure electronic data from Google that federal law permitted Google to turn over to the prosecution but not the defense. He also argued that the trial court erred in denying his motion to compel the victim to comply with a subpoena to turn over her computer for in camera inspection. The Oregon Court of Appeals rejected the first argument, concluding that Oregon law did not require the prosecution to secure data that was not within its control. However, the appellate court vacated the convictions and remanded because, under Oregon law, the defendant had a "broad right" to compel the production of evidence and the subpoena was not overbroad.

#Discovery

#Miscellaneous

***State v. Brereton,* 826 N.W.2d 369 (Wis. 2013), *cert. denied*, 134 S. Ct. 93 (2013)**

The defendant was a suspect in a string of burglaries. After visually monitoring the defendant's vehicle, law enforcement conducted a stop based on non-criminal vehicular violations. The vehicle was towed to an impound lot where a GPS device was installed after an order was obtained. The vehicle was then returned to the defendant. Using data from the GPS, the defendant was tied to a crime and arrested. The defendant appealed the denial of his motion to suppress evidence obtained through the monitoring of a GPS device installed on his vehicle. The installation and monitoring had been done through a warrant. The defendant argued that law enforcement "lacked probable cause to seize his vehicle and move it to another location where a GPS device could be safely installed" and that, "the GPS tracking utilized more advanced technology than was contemplated under the warrant, thereby effecting an unreasonable search through execution of the warrant." The Wisconsin Supreme Court affirmed the denial of the motion: (1) "[T]he seizure of Brereton's vehicle was supported by probable cause that the vehicle was, or contained, evidence of a crime, and was therefore permissible under the Fourth

Amendment," (2) "the three-hour seizure of Brereton's vehicle, whereby officers were able to install the GPS device, did not constitute an unreasonable seizure under the Fourth Amendment, as applied to automobiles," and (3) "the technology used in conducting the GPS search did not exceed the scope of the warrant."

#Fourth Amendment Warrant Required or Not

***State v. Buhl,* 138 A.3d 868 (Conn. 2016)**

The defendant had been convicted of breach of the peace and harassment as a result of entries she posted on Facebook through a fictitious profile and an anonymous mailing. An appellate court reversed the conviction for breach of the peace in the absence of expert testimony that the postings were "publicly exhibited," an element of the offense under State law. Testimony was offered about Facebook settings by the victim. Among other things, the Supreme Court held that expert testimony was not required because concepts related to Facebook were "simple." The court also held that the evidence and reasonable inferences supported the finding that the defendant created the profile and made the postings and reinstated the conviction for breach of the peace.

#Trial-Related

#Social Media

State v. Carlson*, 778 N.W.2d 171 (Wis. Ct. App. 2009) (*per curiam)

The defendant appealed from a conviction for possession of child pornography. Central to the trial was the defendant's allegation that he did not knowingly download the pornographic images but that, instead, he visited the Web sites accidentally or a computer virus involuntarily took him to those sites. The defendant argued on appeal that he was denied effective assistance of counsel because the computer expert selected by counsel was not "sufficiently knowledgeable." The court rejected the argument: "Counsel did not perform deficiently simply because the expert she located did not provide as much helpful testimony" as a new, post-verdict expert could have. Moreover, the evidence presented demonstrated a high probability of the defendant's guilt.

#Trial-Related

***State v. Combest*, 350 P.3d 222 (Or. Ct. App. 2015), *rev. denied,* 363 P.3d 501 (Or. 2015)**

The defendant was convicted of multiple courts related to child sexual abuse. "[W]e must determine whether the officers' use of Shareaza LE to seek out and download files from defendant on a peer-to-peer network—and to obtain the IP address, GUID, and hash value

associated with those files" invaded the defendant's protected privacy interest and constituted a "search" under the Oregon Constitution. The Oregon Court of Appeals held that there had not been a search: (1) The information obtained was available to other network users; (2) the police engaged in limited observation of particular conduct rather than "pervasive surveillance" of the defendant's life. "And the fact that technology has created efficiencies in police practice does not mean that police conduct a 'search' when they use it."

#Fourth Amendment Warrant Required or Not

***State v. Dabas*, 71 A.3d 814 (N.J. 2013)**

A jury found the defendant guilty of murder and attempting to leave the scene of a fatal motor vehicle accident. His conviction was based largely on statements he made. An investigator's handwritten notes of the interview during which the statements were made were purposefully destroyed in violation of a court rule. The trial court declined to give an adverse inference instruction. The Appellate Division reversed because the instruction should have been given. The State appealed.

The New Jersey Supreme Court affirmed the Appellate Division: (1) The destruction of the notes violated a court rule, (2) the notes should have been turned over to the defendant in post-indictment discovery under New Jersey's "open file" policy, (3) the notes were critical to testing the credibility of the investigator, who testified at trial, and (4) an adverse inference instruction was a permissible remedy for the spoliation that took place.

#Preservation and Spoliation

***State v. Decker,* No. A16-0830 (Minn. Ct. App. May 8, 2017), rev. granted, No. A16-0830, (Minn. July 18, 2017)**

The defendant was convicted of criminal sexual conduct and indecent exposure after he sent a photograph of his erect penis to a minor via Facebook Messenger. He argued on appeal he had not engaged in conduct "in the presence of a minor" as required by the statute under which he had been convicted. The Court of Appeals affirmed. It concluded that the minor's "online presence" was sufficient to meet the statutory requirement. The court also concluded that the defendant's conduct of sending digital images was sufficient for his conviction of indecent exposure.

#Trial-Related

***State v. Diamond,* 890 N.W.2d 143 (Minn. Ct. App. 2017), *rev. granted,* No. A15-2075 (Minn. Mar. 28, 2017)**

The defendant was convicted of burglary and other offenses. On appeal, among other things, he challenged on Fifth Amendment grounds an order compelling him to provide his fingerprint so that the police could search his cell phone. The Court of Appeals affirmed the conviction. The police secured a warrant to search the phone but could not do so because they were unable to unlock the phone. The defendant refused to comply with the order and was found in civil contempt. He then provided the fingerprint. The court held that the act of providing a fingerprint was not a testimonial communication because the defendant was not required to "disclose any knowledge he might have or to speak his guilt."

#Fifth Amendment Self-Incrimination

***State v. Dingman*, 202 P.3d 388 (Wash. Ct. App. 2009), *rev. denied,* 217 P.3d 783 (Wash. 2009)**

The defendant appealed from a conviction for theft and money laundering. The trial court had denied the defendant's requests for access to computer information in a format other than that used by the State. Noting the State's obligation to provide meaningful access to hard drive copies, the Court of Appeals reversed the conviction. The defense was entitled to use its own systems in analyzing the computer information.

#Miscellaneous

***State v. Earls*, 70 A.3d 630 (N.J. 2013)**

The police were investigating a series of burglaries. The defendant was identified as the perpetrator and a warrant issued for his arrest. In an effort to locate the defendant and his girlfriend (who, it was feared, might be harmed by the defendant), the police obtained cell-phone location information from a service provider without a court order or warrant on three occasions. The defendant was arrested and indicted. He pled guilty after his motion to suppress was denied by the trial under the "emergency aid" exception to the warrant requirement. The defendant appealed his sentence. The Appellate Division affirmed, concluding that the defendant did not have a reasonable expectation of privacy in his location information.

The New Jersey Supreme Court reversed. It held: "The New Jersey Constitution protects an individual's privacy interest in the location of his or her cell phone. Users are reasonably entitled to expect confidentiality in the ever-increasing level of detail that cell phones can reveal about their lives. Because of the nature of the intrusion, and the corresponding, legitimate privacy interest at stake, we hold today that police must obtain a warrant based on a shoeing of probable cause, or qualify for an exception to the warrant requirement, to obtain tracking information

through the use of a cell phone." The court applied this new rule to the case before it and to future cases and remanded to the Appellate Division to consider the applicability of the emergency aid 201 doctrine.

#Fourth Amendment Warrant Required or Not

***State v. Edwards,* 156 A.3d 506 (Conn. 2017)**

The defendant was convicted of home invasion and related offenses. He argued on appeal, among other things, that the trial court improperly admitted into evidence certain testimony by a police officer. The officer had taken cell phone data provided by Verizon and created maps derived from a computer program to depict cell towers that were used in cell phone calls made by the defendant and that connected him to the crime. Undertaking a *Daubert* analysis, the Supreme Court held that the officer's testimony was expert in nature and that the trial court had erred by not "qualifying him as an expert and conducting a *** hearing in order to ensure that his testimony was based on reliable scientific methodology." However, the Supreme Court affirmed, concluding that the error in admitting the testimony was harmless given, among other things, the overwhelming evidence of the defendant's guilt.

#Admissibility

#Trial-Related

***State v. Esarey*, 67 A.3d 1001 (Conn. 2013)**

The defendant was convicted of, among other things, promoting a minor in an obscene performance. On appeal, he challenged the denial of his motion to suppress the fruits of the search of his Google e-mail account, arguing that the court lacked authority to "issue an extraterritorial *** warrant *** for evidence contained in e-mail servers in another state [California]." Declining to address the issue, the Supreme Court held that, given "that mountain of other evidence" against the defendant, "any impropriety in the issuance and execution of the Gmail warrant was, beyond a reasonable doubt, harmless error that did not affect the verdict ***."

[Note the following: "given the increasing significance of electronically stored communications to the investigation and adjudication of criminal cases, we urge our legislature to undertake a review of Connecticut's relevant statutory scheme to ensure its consistency with federal and sister state provisions authorizing service providers to honor and facilitate the service of warrants issued by-out-of state judges *** "].

#Fourth Amendment Good Faith Exception

***State v. Estrella*, 286 P.3d 150 (Ariz. Ct. App. 2012), *cert. denied*, 133 S. Ct. 2803 (2013)**

The defendant was convicted of, among other things, transportation of marijuana for sale. During an investigation, law enforcement attached a GPS device to a van owned by the defendant's employer and used by the defendant to transport the marijuana. The device was attached in a public parking lot and GPS data was observed over several days. The defendant moved to suppress evidence derived from the data, relying on *United States v. Jones.* The trial court denied the motion. The Court of Appeals affirmed the conviction: (1) The court declined to address whether the warrantless use of the GPS was a search under the trespass analysis of *Jones*; (2) the defendant had no reasonable expectation of privacy in the placement of the device and the monitoring of the van's movement; and (3) the court declined to address whether extended surveillance might intrude on a reasonable expectation of privacy.

#Fourth Amendment Warrant Required or Not

***State v. Feliciano,* 132 A.3d 1245 (N.J. 2016)**

"This case raises a novel question about the constitutionality of the roving wiretap provision of the State's wiretap law. As a general rule, law enforcement must follow a strict set of procedures and get court approval before they intercept communications over a telephone facility. Among other requirements, the State must identify in advance the specific facility it seeks to intercept."

"If a suspect purposefully switches telephone facilities to thwart detection, though, he may effectively avoid being intercepted. To address that situation, both federal and state law contain a "roving wiretap" provision that allows the police, under certain circumstances, to intercept communications on a newly discovered facility used by the target, without first returning to a judge."

The defendant was arrested as part of a drug trafficking conspiracy. Evidence against him was derived from roving wiretaps. His motion to suppress was denied by the trial court. The defendant pled guilty and appealed the denial of his motion to suppress, among other things. The Appellate Division affirmed his convictions.

The Supreme Court rejected, among other things, the defendant's argument that the wiretap order in issue violated the Particularity Requirement of the Fourth Amendment and the New Jersey Constitution. The Supreme Court held that that, given that a judge had found probable cause to monitor a particular facility and that a particular target intended to thwart interception by changing facilities, the requirement had been satisfied under the New Jersey Constitution, which afforded heightened protections than did the Fourth Amendment. However, the court imposed conditions on roving wiretap orders in the future to address constitutional concerns.

#Fourth Amendment Particularity Requirement

***State v. Gray*, No. 93609-9 (*en banc*) (Wash. Sup. Ct. Sept. 14, 2017)**

Defendant was charged and convicted of second degree dealing in depictions of a minor engaged in sexually explicit conduct, for sending a picture of his own penis to a woman. Gray sent two text messages where one of them contained a picture of an erect penis with the words "Eric Gray" written under it. He argued that the statute that he was charged under is constitutionally vague and overbroad entrenching upon his First Amendment rights and that the state legislature, when enacting the law, did not intend to include minors from taking and distributing sexually explicit photos of themselves. The court rejected his argument and upon appeal, affirmed the decision.

#Miscellaneous

***State v. Hamlin,* 776 S.E.2d 364 (N.C. Ct. App. 2015), *rev. denied,* 778 S.E.2d 88 (N.C. 2015)**

The defendant was convicted of felony larceny after breaking and entering. The evidence against him consisted of gift cards that had been stolen from a church. The director of security for the issuer of the gift was permitted, over the defendant's hearsay objection, to testify about ownership and use of the cards based on printouts of electronic records maintained and accessed by the issuer and stored on a third-party secured server. The North Carolina Court of Appeals affirmed.

Testimony about the cards was admissible under the business records exception to the hearsay rule. The court held that the cards had been sufficiently authenticated by the director although he did not himself create the data pertaining to the cards. He testified that he understood how the data was created, collected and transmitted. This was sufficient for admissibility.

#Trial Materials

***State v. Hannah,* 151 A.3d 99 (N.J. Super. Ct. App. Div. 2016)**

The defendant was convicted of simple assault. She argued on appeal, among other things, that a Twitter posting had been improperly admitted into evidence, "citing a Maryland case [*Griffin v. State* (*q.v.*)] requiring that social media postings must be subjected to a greater level of authentication." The Appellate Division disagreed and affirmed. The victim testified that she recognized the tweet as being from the defendant because it displayed the defendant's picture and the victim was familiar with the defendant's Twitter handle. The witness also testified that the tweet was posted in response to events related to the assault and that she and the defendant

had been tweeting back and forth. Moreover, the victim testified that she saw the tweet on the defendant's Twitter page and captured it as a screenshot. The Appellate Division rejected *Griffin,* concluding that "[t]he simple fact that a tweet is created on the Internet does not set it apart from other writings," that only a *prima facie* showing of authentication was required under the evidence rules, and that the evidence presented was sufficient for that showing.

#Admissibility

#Social Media

#Trial-Related

***State v. Hinton,* 319 P.3d 9 (Wash. 2014) (*en banc*)**

The police arrested an individual for possession of heroin and seized his iPhone. Without a warrant, an officer looked through the iPhone and read an incriminated text message. The officer arranged a meeting with the sender through a series of messages and arrested him. When the sender was being booked, a text message was received on the iPhone from the defendant, another meeting was arranged, and the defendant was consequently arrested for a drug transaction. The defendant moved to suppress, arguing that the officer's conduct violated the Washington State Constitution as well as the Fourth Amendment. The motion was denied and the defendant pled guilty, reserving his right to appeal. The intermediate appellate court affirmed. The Washington Supreme Court reversed on the basis of the State Constitution: "Just as subjecting a letter to potential interception while in transit does not extinguish a sender's privacy interest in its contents, neither does subjecting a text message to the possibility of exposure on someone else's phone." Although the defendant assumed the risk that the recipient of his text message would betray him, the recipient had not consented to the warrantless search and therefore the defendant's message remained "private."

#Fourth Amendment Warrant Required or Not

***State v. Huggett*, 783 N.W.2d 675 (Wis. 2010), *rev. denied,* 791 N.W.2d 67 (Wis. 2010)**

The defendant had been charged with second-degree murder. At the time of the murder, a police officer seized the defendant's cell phone and took the cell phone of the defendant's girlfriend. The phones allegedly contained text and voice messages from the victim that would have supported self-defense and defense of another. Although the State preserved the text messages, it did not preserve any voicemail. In affirming the dismissal of the charge with prejudice, the appellate court held that the State had created an "expectation of preservation" by taking possession of the phones, that the State had failed in its duty to preserve, and that there was a due process violation as no "comparable evidence" existed. The tone of the victim was important,

and neither text messages nor witness testimony was a replacement.

#Preservation and Spoliation

***State v. Jenkins,* 884 N.W.2d 429 (Neb. 2016)**

The defendant was convicted of robbery. Evidence offered against her included cell phone records secured through an order issued under Section 2703(d) of the SCA which enabled the police to track the defendant's use of a cell phone. She appealed from, among other things, the denial of her motion to suppress. The Supreme Court observed that the order required the production of historical information CSLI rather than content. The court affirmed the conviction, relying on the third-party doctrine to conclude that the defendant had no reasonable expectation of privacy in the information at issue.

#Fourth Amendment Warrant Required or Not

***State v. Kohonen,* 370 P.3d 16 (Wash. Ct. App. 2016)**

The appellant, a juvenile, was found guilty of cyberstalking based on two tweets sent from her Twitter account. She challenged the sufficiency of the evidence offered against her on appeal. The appellate court reversed, having concluded that there was insufficient evidence that the tweets were "true threats." A reasonable person in the appellant's position would not have foreseen that the tweets, although "admittedly mean-spirited," would be interpreted to be a "serious expression of an intent to harm."

#Miscellaneous

#Social Media

***State v. Loomis,* 881 N.W.2d 749 (Wis. 2016), *cert. denied*, 137 S. Ct. 2290 (2017)**

The defendant was convicted of various offenses arising out of a drive-by shooting. His presentence report included an evidence-based risk assessment that indicated a high risk of recidivism. On appeal, the defendant argued that consideration of the risk assessment by the sentencing judge violated his right to due process. The Supreme Court rejected the argument. However, it imposed conditions on the use of risk assessments.

#Miscellaneous

***State v. Lyons*, 9 A.3d 596 (N.J. Super. Ct. App. Div. 2010)**

The trial court granted a motion to dismiss the indictment, concluding that the defendant's "passive conduct" in possessing images of child pornography in a shared folder on a peer-to-peer network were insufficient to show intent to transfer or distribute the images to other. The Appellate Division reversed in a case of first impression in New Jersey and, in doing so, canvassed the law of other jurisdictions. The defendant was aware that his folder materials were available to others who shared the network and he acted "affirmatively" in installing the network and making these available to others.

#Miscellaneous

***State v. McDuffie,* 164 A.3d 414 (N.J. Super. Ct. App. Div. 2017)**

The defendants were convicted of various arising out of a series of home robberies and other offenses. The police had secured a warrant for the installation of a GPS tracking device on a vehicle registered to the mother of one defendant. The device was available only to law enforcement but included commercially-available components. The device was used for real-time tracking of the vehicle and, on the date of their arrests, a GPS expert confirmed the proper functioning and accurate recording of the vehicle's location through personal observation. The vehicle was then tracked to the scene of robberies and the defendants (who were both in the vehicle) arrested. On appeal, the defendants argued, among other things, that their right to a fair trial had been impeded by the failure of the trial court to suppress the GPS data and to disclose specific information about the device. The Appellate Division affirmed the convictions on the basis of the State's privilege to protect law enforcement methods. First, the defendants had not made a showing of a particularized need for disclosure of the specific information about the device. Second, the defendants had an adequate opportunity to cross-examine the State's witness on the proficiency of the user of the device and its accuracy. Third, there was collaborating visual evidence extrinsic to the device. Finally, the State had introduced sufficient technical data to enable them to secure an expert in their defense. The Appellate Division remanded, however, for resentencing.

#Admissibility

#Miscellaneous

#Trial-Related

***State v. Moser,* 884 N.W.2d 890 (Minn. Ct. App. 2016)**

"By eliminating a mistake-of-age defense and imposing strict liability, Minnesota Statutes ***, as

applied to solicitation over the Internet, involves no face-to-face contact between the solicitor and the child, and where the child represents to the solicitor that he or she is 16 or older, violates substantive due process."

#Trial-Related

#Social media

***State v. Patino,* 93 A.3d 40 (R.I. 2014), *cert. denied*, 135 S. Ct. 947 (2015)**

The defendant was indicted for the murder of the six-year-old son of his girlfriend. The girlfriend had called 911 from her apartment and reported that her son was unresponsive and not breathing. When the police arrived the defendant was in the apartment. An officer observed four cell phones in the apartment, one of which indicated that it was receiving a message. This led the officer to open the phone and to eventually read an incriminating message. This led to the discovery of additional incriminating messages on three phones. The defendant moved to suppress all evidence derived from the cell phones. The hearing judge granted the motion.

The Rhode Island Supreme Court reversed. The cell phone opened by the officer in the apartment was used exclusively by the girlfriend. "Having already sent the incriminating text messages, which were indeed delivered to *** [the girlfriend's phone], defendant no longer had any control over what became of the messages contained in that phone." Thus, the defendant had no reasonable expectation of privacy in the girlfriend's phone or the messages it contained and lacked standing to challenge the search and seizure. [**NOTE**: There is much more to this decision. This annotation focuses on only one issue].

#Fourth Amendment Warrant Required on Not

State v. Pittman*, No. A-2569-08T4 (N.J. Super. Ct. App. Div. Nov. 4, 2009) (*per curiam)

In this interlocutory appeal, the court affirmed the decision of the trial court to bar evidence derived from a GPS device installed surreptitiously on the defendant's vehicle. Expert testimony was deemed essential as to the accuracy and trustworthiness of the *particular* GPS device installed on the vehicle, and that testimony was lacking below. Moreover, the State had declined various opportunities to present sufficient proof or make a proffer.

***State v. Polk*, 415 S.W.3d 692 (Mo. Ct. App. 2013)**

The defendant was convicted of rape. On appeal, he challenged, among other things, the prosecutor's comments during trial about the case on Twitter. The trial court rejected the challenge. The Court of Appeals affirmed. It recognized that, "extraneous statements on Twitter

or other forms of social media, particularly during the time frame of the trial, can taint the jury and result in reversal of the verdict." However, because the defendant presented no evidence that the jury was, "aware of or influenced by Joyce's [the prosecutor] Twitter comments," it affirmed the denial of the defendant's motion for a new trial.

#Trial-Related

#Social Media

***State v. Purtell*, 851 N.W.2d 417 (Wis. 2014)**

In this post-*Riley* decision, the defendant had moved to suppress evidence derived from the warrantless search of his personal computer by a probation officer. The trial court denied the motion. The Court of Appeals reversed. The Washington Supreme Court reinstated the conviction: "A probation agent's search of a probationer's property satisfies the reasonableness requirement of the Fourth Amendment if the probation agent has 'reasonable grounds' to believe the probationer's property contains contraband. *** The record demonstrates that the probation agent had reasonable grounds to believe Purtell's computer, which Purtell knowingly possessed in violation of the conditions of his probation, contained contraband."

The dissent challenged the majority opinion for failing to distinguish between the seizure of the computer (which was contraband under the defendant's terms of probation) and the subsequent warrantless search of the content of the computer. "By ignoring precedent and suggesting that once property is seized it can be searched, the majority greatly reduces not only the property rights of probationers, but the privacy rights of the millions of people who own cellphones, computers, and similar electronic devices."

#Fourth Amendment Warrant Required or Not

***State v. Reid,* 945 A.2d 26 (N.J. 2008)**

The State appealed from the suppression of evidence secured through a defective municipal court subpoena. The defendant had been indicted for computer theft after allegedly accessing a supplier's website and changing her employer's password and shipping address. In a case of first impression, the New Jersey Supreme Court held that Internet subscribers had a reasonable expectation of privacy in their IP addresses under the State Constitution. The court also held that disclosure of such addresses to third-party service providers did not vitiate the privacy interest and that the address be sought through an *ex parte* grand jury subpoena. Of interest, the court noted: "Should that reality [the existence of websites which reveal service providers but not individual users] change over time, the reasonableness of the expectation of privacy in Internet subscriber information might change as well."

#Miscellaneous

***State v. Riley*, 841 N.W.2d 431 (S.D. 2013), *cert. denied,* 134 S. Ct. 2667 (2014)**

The defendant was convicted by a jury of possession of child pornography. On appeal, he argued that there was insufficient evidence to establish "knowing" possession. The South Dakota Supreme Court affirmed the conviction. The State had no direct evidence. Instead, it relied on circumstantial evidence: "(1) the reinstallation of the operating system, the deletion of numerous other files, and Riley's past employment with IBM together with Riley's knowledge that the police were coming to search his computer, (2) Riley's admission that he used LimeWire and 'glanced at' child pornography, (3) his statement that 'it's gone' in regards to the 79 video files containing child pornography, (4) the text strings suggesting child pornography, and (5) the evidence that he was the only user of the computer at issue on an IP address that was downloading child pornography." The court found this evidence sufficient to support a rational jury verdict.

#Trial-Related

***State v. Rivera,* No. CA2008-12-308 (Ohio. Ct. App. Feb. 1, 2010), *appeal denied,* 927 N.E.2d 12 (Ohio 2010), *cert. denied,* 131 S. Ct. 478 (2010)**

The defendant appealed from his conviction for compelling prostitution. Law enforcement had secured the defendant's cell phone number from minors he had solicited to perform sexual acts and had also secured the defendant's text messages with the minors from his cell phone service provider. Thereafter, a search warrant was issued and the defendant confessed. On appeal, the conviction was affirmed. First, although the SCA had been violated when law enforcement secured the messages by order rather that warrant and had not given the defendant notice, the Act did not provide a suppression remedy for violation of its terms. Moreover, the defendant did not demonstrate a privacy right in the messages.

#Fourth Amendment Warrant Required or Not

***State v. Scoles,* 69 A.3d 559 (N.J. 2013)**

The defendant was charged with endangering the welfare of a child based on allegations of email transmission of child pornography. He moved to compel discovery after the State refused to provide computer images to his attorney. The trial court denied the motion but entered a protective order that allowed access to the images at a State facility and only within 48 hours of making a request for inspection. The Supreme Court granted leave to appeal: "The discovery issue that we consider *** has become a recurring one as prosecutions involving child pornography have become more frequent." The Supreme Court declined to adopt the "prophylactic controls" of the Adam Walsh Act.

Instead, the court held that, consistent with the "open file" policy of the New Jersey criminal rules, a trial court had authority to issue an order that would allow for greater access within the following framework: (1) defense counsel must request access be afforded within their offices; (2) defense counsel must, at a conference, "demonstrate the ability to comply with the terms of a *** order designed to secure the computer images from intentional and unintentional dissemination ***;"and (3) when access is only allowed at a State facility, "greater access and flexibility must be made available to the defense team as the trial date approaches."

[Note that this decision imposes an ESI-related competency requirement on defense counsel].

#Trial-Related

#Discovery Materials

***State v. Scott*, No. A-4147-05T4 (N.J. Super. Ct. App. Div. July 20, 2009) (*per curiam*)**

The defendants appealed following their convictions for various crimes. Among other things, they challenged the trial judge's substitution of a juror *after* deliberations began. The substituted juror had conducted Internet research and had shared the results with her fellow jurors. The appellate court vacated and remanded for a new trial, concluding that substitution was inappropriate: The juror did not the New Jersey rule-based "inability to continue" standard for substitution and her conduct tainted the entire jury.

#Trial-Related

***State v. Shannon*, 120 A.3d 924 (N.J. 2015), *cert. denied*, 136 S. Ct. 1657 (2016)**

A municipal court judge issued a warrant for the defendant's arrest. Thereafter, the judge vacated the warrant but it remained on a computer database and the defendant was arrested on the warrant. At the time of his arrest narcotics were found in the defendant's vehicle and he was indicted. Relying on a 1987 New Jersey Supreme Court decision that rejected the good faith exception to the Warrant Requirement under the New Jersey Constitution, lower courts determined that the arrest was unlawful and suppressed the evidence. An equally-divided (3-3) Supreme Court affirmed: "The arresting officer's good faith belief that a valid warrant for defendant's arrest was outstanding cannot render an arrest made in the absence of a valid warrant or probable cause constitutionally compliant."

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Good Faith Exception

***State v. Smith*, 920 N.E.2d 949 (Ohio 2009), *cert. denied*, 131 S. Ct. 102 (2010)**

When the defendant was arrested a cell phone was found on his person. Thereafter, without obtaining a warrant, the State searched the information in the cell phone and found incriminating information. The defendant was convicted of drug possession and trafficking after the trial court denied his motion to suppress the information. In a case of first impression, the Ohio Supreme Court reversed the conviction. The court held that, under the Fourth Amendment, the cell phone was not the equivalent of a closed container that would justify a search incident to arrest, that the defendant had a legitimate expectation of privacy in the cell phone's contents, and that the State should have secured a warrant.

#Fourth Amendment Warrant Required or Not

***State v. Sobczak*, 833 N.W.2d 59 (Wis. 2013), *cert. denied*, 134 S. Ct. 626 (2013)**

The defendant moved to suppress the fruits of the warrantless search of his home computer. The defendant had invited a guest to stay at his home over a weekend and had given her access to the computer. The guest accessed suspicious files on the computer and invited law enforcement into the defendant's home to view the files. The trial court denied the defendant's motion to suppress. The intermediate appellate court affirmed, as did the Wisconsin Supreme Court, concluding that, under the facts, the guest had authority to consent to the entry and the search.

#Fourth Amendment Warrant Required or Not

***State v. Stahl,* 206 So. 3d 124 (Fla. Dist. Ct. App. 2016)**

The defendant was charged with the felony offense of video voyeurism after having being observed holding a cellphone under a woman's skirt in a store. The defendant fled the scene but was positively identified from a surveillance video. When he was arrested, the defendant consented to the search of his phone but then withdrew the consent. A search warrant was issued but the State could not access content because the defendant refused to provide the passcode. The State's motion to compel the defendant was denied by the trial court, which found that the Fifth Amendment privilege against self-incrimination applied. The District Court of Appeal granted *certiorari* and reversed. The appellate court reasoned that the defendant would not be acknowledging that the phone contained evidence of the crime by providing his password and that providing the password would not be a testimonial act. The court also held that, in any event, the forgone conclusion doctrine applied.

#Fifth Amendment Self-Incrimination

***State v. Subdiaz-Osorio*, 849 N.W.2d 748 (Wis. 2014), *cert. denied*, 135 S. Ct. 379 (2014)**

In this post-*Riley* decision, the defendant, who was in the United States illegally, fatally stabbed his brother, borrowed a car, and fled the scene.

The police were concerned that the defendant was trying to escape to Mexico and was carrying the murder weapon. Without securing a warrant, the police tracked the defendant through his cell phone location and he was apprehended in Arkansas. The defendant moved to suppress all evidence obtained after his arrest on the grounds that, among other things, the warrantless search of his cell phone location violated the Fourth Amendment. The defendant pled guilty to reckless homicide after hid motion was denied and appealed.

"The court must decide whether law enforcement officers may contact a homicide suspect's cell phone provider to obtain the suspect's cell phone location information without first securing a court order based on probable cause." This question led to *six* separate opinions: "The court is deeply divided on these issues as evidenced by the number of separate filings." To summarize the writings:

(1) One justice, writing the "lead opinion," assumed that" people have a reasonable expectation of privacy in their cell phone location data and that when police track a cell phone's location, they are conducting a search under the Fourth Amendment." However, "the police did have probable cause for a warrant and *** the exigent circumstances of this case created an exception to the warrant requirement." Three justices agreed that exigent circumstances existed.

(2) One justice agreed with the dissent that there was a search within the meaning of the Fourth Amendment and that there were no exigent circumstances, but concluded that the denial of the motion to suppress was harmless error.

(3) One justice concluded that, "absent case-specific exceptions, such as an emergency, a warrant is required for the search of a cell phone's location," but that a good faith exception should be applied and the exclusionary rule should not be applicable.

(4) One justice agreed with the lead opinion that exigent circumstances existed but took issue with its "elaboration" of reasonable expectations of privacy.

(5) One justice cautioned that the Court had received no "briefing or argument on the broader privacy questions that are addressed in the lead opinion or in *Riley.*

(6)In dissent, one justice would hold that there was a "search," that exigent circumstances did not exist, that there was sufficient time to secure a warrant.

[Note: This is a very complicated decision. Justices joined in different opinions and some opinions include discussion of a "subjective" expectation of privacy in the context of terms of service.]

#Fourth Amendment Warrant Required or Not

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Good Faith Exception

***State v. Tate,* 849 N.W.2d 798 (Wis. 2014)**

The defendant was sought for a homicide which occurred outside a store in which he had just purchased a cell phone. Law enforcement secured an order for CSLI and, using that information as well as a "stingray," located the defendant in his mother's apartment and arrested him. The defendant moved to suppress all the evidence, arguing that law enforcement needed a search warrant to track his phone and that the order they secured was not the equivalent of a warrant. The motion was denied, the defendant pled to reckless homicide, and he appealed the denial. The Wisconsin Supreme Court affirmed. "[W]e assume without deciding that: (1) law enforcement's activities constituted a search ***; and (2) because the tracking led law enforcement to discover Tate's location within his mother's home, a warrant was needed. We then conclude that the search was reasonable because it was executed pursuant to a warrant ***. We also conclude that specific statutory authorization was not necessary *** to issue the order *** because the order was supported by probable cause. Nonetheless, the order did comply with the spirit of *** [statutes] which express legislative choices about procedures to employ for warrants and criminal subpoenas." **[Note that the order "functioned as a warrant for our constitutional considerations and as a criminal subpoena in regard to the information obtained from the cell service provider."]**

#Fourth Amendment Warrant Required or Not

#Miscellaneous

***Sublet v. State*, 113 A.3d 695 (Md. Ct. App. 2015)**

The Maryland Court of Appeals consolidated three cases that involved the same legal issues, those being the elucidation and implementation of our opinion in *Griffin v. State,* 419 Md. 343, 19 A.3d 425 (2011), in which we addressed the admissibility of a screenshot of a MySpace page, and its application to the authentication of messages allegedly sent through social media networking websites; in *Sublet,* via a Facebook timeline; in *Harris,* on Twitter through 'direct

messages' and public 'tweets'; and, in *Monge-Martinez*, through Facebook messages. (footnotes omitted). The court held that, in order to authenticate evidence derived from a social media networking website, the trial judge must determine that there is proof from which a reasonable juror could find that the evidence is what the proponent claims it to be. We shall hold in *Sublet* that the trial court did not err in excluding the admission of the four pages of the Facebook conversation. We shall hold in *Harris* that the trial court did not err in admitting the 'direct messages' and 'tweets' in evidence. We shall also hold in *Monge-Martinez* that the trial court did not err in admitting the Facebook messages authored by Monge-Martinez.

The court did make this observation: "We also suggested in *Griffin's* footnote thirteen that a public posting on a social networking page differs from private messages visible to specified individuals with respect to authentication. E-mails and other directed communications, for example, may present a greater opportunity for authentication by circumstantial evidence."

#Trial Materials

#Social Media

***State v. Thomas,* 376 P.3d 184 (N.M. 2016)**

The defendant was convicted of murder and kidnapping. DNA evidence was presented by the forensic analyst who had established that samples collected at the crime scene matched the defendant's DNA profile. However, as she had moved out of New Mexico, the trial court allowed her to testify though Skype. The defendant argued on appeal, among other things, that allowing such testimony violated his rights under the Confrontation Clause. The Supreme Court agreed: "A criminal defendant may not be denied a physical, face-to-face confrontation with a witness who testifies at trial unless the court has made a factual finding of necessity to further an important public policy and has ensured the presence of other confrontation elements ***." The court held the failure to make these findings was not harmless error and that since the only evidence offered against the defendant was the erroneously admitted DNA evidence the convictions must be reversed.

#Trial-Related

***State v. Worsham,* No. 4D15-2733 (Fla. Dist. Ct. App. March 29, 2017), *cert. denied.* No. 17-176 (2017)**

The defendant was the driver of a vehicle involved in a high speed accident that killed his passenger. His vehicle was impounded by the police and, without a warrant, the police downloaded data from the vehicle's "event data recorder." The defendant was charged with manslaughter and homicide. His motion to suppress the downloaded data was denied. The

District Court of Appeal reversed, holding that the defendant had a reasonable expectation of privacy in the data and relying in part on *Riley v. California*. The appellate court also rejected the argument that the third party doctrine of *Smith v. Maryland* was applicable. The dissenting judge would have held that the defendant had no such expectation.

#Fourth Amendment Warrant Required or Not

***T.H. v. C.B.,* No. A-4858-15T3 (N.J. Super. Ct. App. Div. July 13, 2017) (*per curiam*)**

The trial judge in this harassment proceeding denied the request of the plaintiff to show a video accessible from her smartphone of an encounter between the plaintiff and the defendant although the defendant did not object to her doing so. The trial judge did so because he found that no foundation had been laid and because the plaintiff was *pro se*. The Appellate Division reversed. After noting that there were no separate evidence rules for *pro se* parties, the appellate court held that the trial judge had abused his discretion when he denied admission without offering either party the opportunity to authenticate the video. The court also held that the exclusion was not harmless because the video was highly relevant and remanded for further proceedings.

#Admissibility

#Trial-Related

***Taylor v. State,* 371 P.3d 1036 (Nev. 2016), *cert. denied*, 137 S. Ct. 633 (2016)**

"This opinion addresses whether the State's warrantless access of historical cell site location data obtained from a cell phone service provider pursuant to the SCA*** violates the Fourth Amendment. We hold that it does not because a defendant does not have a reasonable expectation of privacy in this data, as it is a part of business records made, kept, and owned by cell phone providers. Thus, the 'specific and articulable facts' standard *** is sufficient to permit the access of historical cell phone information, and probable cause is not required."

#Fourth Amendment Warrant Required or Not

***Tienda v. State*, 358 S.W.3d 633 (Tex. Crim. App. 2012)**

During preparation of the state's case against defendant, the deceased's sister had provided the state with information regarding three MySpace profile pages that she believed defendant was responsible for registering and maintaining. After subpoenaing MySpace.com for the general "subscriber report" associated with each profile account, the state printed out images of each

profile page directly from the MySpace.com website, and then marked the profile pages and related content as state's exhibits for trial. Using the deceased's sister as the sponsoring witness for these accounts, and, over defendant's running objection as to the authenticity of the profile pages, the state was permitted to admit into evidence the names, account information, comments and instant messages associated with the profiles, as well as comments and photos posted on the profiles. Defendant appealed his conviction, asserting that the state had failed to prove that he was responsible for creating and maintaining the content of the MySpace pages introduced into evidence. The court of appeals affirmed his conviction, holding that the trial court had not abuse its discretion in admitting evidence from MySpace pages because there was sufficient circumstantial evidence to support a finding that the exhibits were what they purported to be.

#Trial-Related

***Wardlaw v. State*, 971 A.2d 331 (Md. Ct. Spec. App. 2009)**

After conviction, the defendant appealed from the denial of his motion for a mistrial based on juror misconduct. One juror had conducted Internet research on a relevant mental disorder and shared the results of the research with fellow jurors. The appellate court reversed, concluding that the juror had engaged in "egregious misconduct," that a presumption of prejudice arose, and that the trial court's failure to conduct a *voir dire* was an abuse of discretion.

#Trial-Related

***Wheeler v. State,* 135 A.3d 282 (Del. 2016)**

The defendant was convicted of dealing in child pornography. He argued on appeal that the trial court had erred in denying his motion to suppress evidence collected from his home and office pursuant to warrants related to witness tampering. "The challenged warrants covered Wheeler's entire digital universe and essentially had no limitations. *** the State found no evidence of witness tampering on any of the devices [seized pursuant to the warrants]. But when performing a cursory search of the data on an iMac found in Wheeler's piano room closet ***, the police discovered files containing child pornography." The Supreme Court reversed the conviction because the warrants were "general." The court also concluded that the applications violated the Particularity Requirement because, among other things, the applications failed to describe the items to be search for and seized.

#Fourth Amendment Particularity Requirement

***Zanders v. State,* 73 N.E.3d 178 (Ind. 2017), *petition for cert. filed,* No. 17-166 (Aug. 1, 2017)**

The defendant was convicted of robbery with a deadly weapon and other offenses. Evidence offered against him included historical cell site location data secured from the defendant's cell phone service provider without a warrant as well as items found in a residence pursuant to a search warrant based on the records. The defendant appealed from, among other things, the admission of this evidence over his objection. The Court of Appeals court held that suppression of historical CSLI was warranted because the third-party doctrine did not apply: a "cell phone user does not convey historical location data to his phone at all—voluntarily or otherwise—and therefore does not assume any risk of disclosure to law enforcement." The Indiana Supreme Court reversed, concluding that no search "occurred under the Fourth Amendment when police gathered historical active CSLI that defendant had already voluntarily relinquished to Sprint. Cell users are presumed to know certain facts that cellphones run on signals and that cell phone providers keep track of those signals. Thus, defendant "must know that by making and receiving calls he is "expos[ing his phone's location] to [Sprint's] equipment in the ordinary course of business."

#Admissibility

#Fourth Amendment Warrant Required or Not

#Miscellaneous

#Third-Party Doctrine

#Trial-Related

STATUTES, REGULATIONS, ETC. - FEDERAL

18 U.S.C. Sec. 2517 ("Authorization for disclosure and use on intercepted wire, oral, or electronic communications")

"(1) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(2) Any investigative or law enforcement officer who, by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication or evidence derived therefrom may use such contents to the extent such use is appropriate to the proper performance of his official duties.

(3) Any person who has received, by any means authorized by this chapter, any information

concerning a wire, oral, or electronic communication, or evidence derived therefrom intercepted in accordance with the provisions of this chapter may disclose the contents of that communication or such derivative evidence while giving testimony under oath or affirmation in any proceeding held under the authority of the United States or of any State or political subdivision thereof.

(4) No otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character." ***

#Miscellaneous

18 U.S.C. Sec. 2703(f) ("Requirement to Preserve Evidence")

Subsection 1 requires a "provider of wire or electronic communication services or a remote computer service, upon the request of a governmental agency," *** [to] take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process."

Subsection 2 provides that such records must be retained for 90 days, "which shall be extended for an additional 90-day period upon a renewed request by the governmental agency."

#Preservation & Spoliation

"The Attorney General's Guidelines for Domestic FBI Operations" (2008)

("The broad operational areas addressed by these Guidelines are the FBI's conduct of investigative and intelligence gathering activities, including cooperation and coordination with other components and agencies in such activities, and the intelligence analysis and planning functions of the FBI").

#Miscellaneous

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

#Admissibility

#Miscellaneous

#Trial-Related

"Auto Parts Executive Pleads Guilty to Obstruction of Justice," Office of Public Affairs, Department of Justice (Feb. 2, 2017), https://www.justice.gov/opa/pr/auto-parts-industry-executive-pleads-guilty-obstruction-justice

#Preservation and Spoliation

"Best Practices for Electronic Discovery in Criminal Cases," W.D. Wash. (adopted Mar. 21, 2013)

(reflecting JETWG Recommendations described below)

#Discovery Materials

Department of Justice Policy Guidance: Domestic Use of Unmanned Aircraft Systems (UAS)

Released on May 22, 2015, this Policy Guidance recognizes that drones have "emerged as a viable law enforcement tool" and sets forth principles to be applied on a "Department [of Justice]-wide" basis.

#Fourth Amendment Warrant Required or Not

#Miscellaneous

Department of Justice Policy Guidance: Use of Cell-Site Simulator Technology

Released on September 3, 2015, this Policy Guidance recognizes that the technology "provides valuable assistance in support of important public safety objectives" that must be used "in a manner that is consistent with the requirements and protections of the Constitution, including the Fourth Amendment, and applicable statutory authorities, including the Pen Register Statute." The Policy Guidance requires law enforcement agencies to seek a search warrant pursuant to *Fed. R. Crim. P.* 41 unless there are exigent circumstances or "other circumstances in which *** the law does not require a search warrant and circumstances make obtaining a warrant impracticable."

#Fourth Amendment Exigent Circumstances

#Fourth Amendment Warrant Required or Not

"General Order Regarding Best Practices for Electronic Discovery of Documentary Materials in Criminal Cases,' W.D. Okla. *General Order* 09-05 (Aug. 20, 2009)

(summarizing proposed electronic discovery practices and recognizing that, "[o]pen communications between the government and defense counsel is critical to ensure that discovery is handled and completed in a manner agreeable to all parties").

#Discovery Materials

Letter from Senator Wyden, et al., to the Attorney General seeking "more information regarding the Department's efforts to ensure that courts are adequately informed when federal prosecutors seek warrants for the use of stingrays, including how these devices adversely affect the general public" (Aug. 1, 2017), https://www.wyden.senate.gov/download/?id=CBF8211B-EE3B-4BF5-9702-43D26CCAE8E2&download=1

#Fourth Amendment Warrant Required or Not

#Miscellaneous

"Evaluation of Corporate Compliance Programs," Fraud Section, Criminal Division, U.S. Department of Justice (released Feb. 8, 2017), https://www.justice.gov/criminal-fraud/page/file/937501/download

#Miscellaneous

"Intake and Charging Policy for Computer Crime Matters" (USDOJ Sept. 11, 2014) (Released Oct. 25, 2016)

#Miscellaneous

J.R. Cantor, Acting Chief Privacy Officer, "DHS Privacy Policy Regarding Collection, Use, Retention, and Dissemination of Personally Identifiable Information") Privacy Policy Guidance Memorandum, Memorandum Number: 2017-001 (Dept. of Homeland Security: Apr. 27, 2017), https://www.dhs.gov/sites/default/files/publications/Privacy%20Policy%20Guidance%20Memo%202017-01%20-%20FINAL.pdf

#Miscellaneous

"Legislation to Permit the Secure and Privacy-Protective Exchange of Electronic Data for the Purposes of Combatting Serious Crime Including Terrorism"

(USDOJ Office of Legislative Affairs; transmitted to President of the Senate July 15, 2016)

#Miscellaneous

Letter to Senator Wyden from Internal Revenue Service

This letter, dated November 25, 2015, responded to "a question *** asked during [a] *** hearing about the use of cell-site simulator technology" by the IRS. The letter stated that the IRS would draft a policy that would mirror a DOJ Policy Guidance [*q.v.*] that required a search warrant to be secured "prior to using the technology except in exigent or exceptional circumstances."

#Fourth Amendment Warrant Required or Not

Managing Large Volumes of Discovery in Federal CJA Cases

This Memorandum, authored by James C. Duff, was issued by the Administrative Office of the United States Courts on May 14, 2015. Its purpose was to advise of "services available from the Defender Services' National Litigation Support Team (NLST)" and focused on "Coordinating Discovery Attorneys" and a "Web-hosted Document Review Platform" available through a Defender Services Office contract with AccessData.

#Discovery Materials

Preliminary Draft of Proposed Amendment to Fed. R. Crim. P. 16 to add new 16.1 (Committee on Rules of Practice and Procedure of the Judicial Conference of the United States: Aug. 2017), http://www.uscourts.gov/sites/default/files/preliminary_draft_08_2017_0.pdf

#Discovery Materials

Proposed Amendments to Federal Rule of Evidence

On August 16, 2015, the Chair of the Committee on Rules of Practice and Procedure of the Judicial Conference of the United States issued a request for public comments on proposed amendments to, among others, *Fed. R. Evid.* 803. (see "Report of the Advisory Committee on 224 Evidence Rules dated May, 7, 2015). The proposed amendments include:

1. "Abrogation of Rule 803(16), the ancient documents exception to the hearsay rule," because,

among other things, the ancient documents exception could once have been thought tolerable out of necessity (unavailability of other proof for old disputes) and by the fact that the exception has been so rarely invoked. But given the development and growth of electronically stored information, the exception has become even less justifiable and more subject to abuse. The need for an ancient document that does not qualify under any other hearsay exception has been diminished by the fact that reliable electronic information is likely to be available and will likely satisfy a reliability-based hearsay exception *** [proposed Committee Note to explain abrogation of 803(16)].

2. "Amendment of Rule 902 to add two subdivisions that would allow authentication of certain electronic evidence by way of certification by a qualified person." As explained by the Committee, [t]he first provision would allow self-authentication of machine-generated information, upon a submission of a certification prepared by a qualified person. The second proposal would provide a similar certification procedure for a copy of data taken from an electronic device, media or file. These proposals are analogous to Rules 902(11) and (12) ***, which permit a foundation witness to establish the authenticity of business records by way of certification.

The proposals have a common goal of making authentication easier for certain kinds of electronic evidence that are, under common law, likely to be authenticated under Rule 901 but only by calling a witness to testify to authenticity. The Committee has concluded that the types of electronic evidence covered by the two proposed rules are rarely the subject of a legitimate authentication dispute, but it is often the case that the proponent is nonetheless forced to produce an authentication witness, incurring expense and inconvenience – and often, at the last minute, opposing counsel ends up stipulating to authenticity in any event.

#Trial Materials

"Recommendations for Electronically Stored Information (ESI) Discovery Production in Federal Criminal Cases"

("Department of Justice (DOJ) and Administrative Office of the U.S. Courts (AO) Joint Working Group on Electronic Technology in the Criminal Justice System (JETWG)" (Feb. 2012) (setting out recommendations for "managing ESI discovery in federal criminal cases" in three documents: (1) a "general framework," (2) "technical and more particularized guidance," and (3) a one-page checklist).

#Discovery Materials

Resolution 10A
("The ABA urges the Department of Justice and the Federal Bureau of Prisons to amend their policies with respect to monitoring emails between attorneys and their incarcerated clients to permit attorneys and their incarcerated clients to communicate confidentially via email and thereby maintain the attorney-client privilege.") (Adopted by ABA House of Delegates Feb. 8, 2016)

#Discovery materials

#Miscellaneous

Security Executive Agent Directive 5, Collection, Use, and Retention of Publicly Available Social Media Information in Personnel Security Background Investigations and Adjudications (Version 5.4 – May 5, 2016; Effective May 12, 2016)

#Preservation and Spoliation

#Miscellaneous

#Social Media

"Suggested Practices Regarding Discovery in Complex [Criminal] Cases," N.D. Ca. (establishing "protocol of suggested practices regarding discovery in wiretap and other complex, document-intensive cases).

#Discovery Materials

"United States Department of Justice, Prosecuting Computer Crimes" (Computer Crime and Intellectual Property Section Criminal Division: date unknown)

("This manual examines the federal laws that relate to computer crimes. Our focus is on those crimes that use or target computer networks ***").

#Miscellaneous

United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations (Computer Crime and Intellectual Property Section Criminal Division: July 2009)

("The purpose of this publication is to provide Federal law enforcement agents and prosecutors

with systematic guidance that can help them understand the legal issues that arise when they seek electronic evidence in criminal investigations").

#Miscellaneous

STATUTES, REGULATIONS, ETC. - STATE

In re: Amendments to the Florida Evidence Code, No. SC16-181 (Feb. 16, 2017) (per curiam) (declining to adopt Daubert standard),
http://www.floridasupremecourt.org/decisions/2017/sc16-181.pdf

#Admissibility

#Trial-Related

Attorney General Law Enforcement Directive No. 2015-1

The subject of this Directive, issued by the Acting Attorney General of New Jersey on July 28, 2015, is "Law Enforcement Directive Regarding Policy Body Worn Cameras (BWCs) and Stored BWC Recording." It is intended to "provide guidance to police departments on how to make the best possible use of electronic recording technology."

#Discovery Materials

#Preservation and Spoliation

#Miscellaneous

Ch. 651, Statutes of 2015, California Electronic Communications Privacy Act (enacted Oct. 8, 2015)

#Fourth Amendment Warrant Required or Not

Formal Op. 2017-5, "An Attorney's Ethical Duties Regarding U.S. Border Searches of Electronic Devices Containing Clients' Confidential Information" (Association of the Bar of the City of New York: July 25, 2017), http://www.nycbar.org/member-and-career-services/committees/reports-listing/reports/detail/formal-opinion-2017-5-an-attorneys-ethical-duties-regarding-us-border-searches-of-electronic-devices-containing-clients-confidential-information

#Fourth Amendment Warrant Required or Not

#Miscellaneous

Minnesota S.F. No. 1740

(approved by Governor May 14, 2014) (among other things, requiring that, "[a]ny new smart phone manufactured on or after July 1, 2015, sold or purchased in Minnesota must be equipped with preloaded antitheft functionality or be capable of downloading that functionality. The functionality must be available to purchasers at no cost").

(also providing that, "[w]henever a law enforcement official *** has probable cause to believe that a wireless communications device in the possession of a wireless communications device dealer is stolen or is evidence of a crime and notifies the dealer not to see the item, the dealer shall not (1) process or sell the item, or (2) remove or allow its removal from the premises. This investigative hold must be confirmed in writing *** within 72 hours and will remain in effect for 30 days ***").

#Miscellaneous

Missouri Constitutional Amendment No. 9, amends Section 15 of Article I

"That the people shall be secure in their persons, papers, homes [and], effects, **and electronic communications and data,** from unreasonable searches and seizures; and no warrant to search any place, or seize any person or thing, **or access electronic data or communication,** shall issue without describing the place to be searched, or the person or thing to be seized, **or the data or communication to be accessed,** as nearly as may be; nor without probable cause, supported by written oath or affirmation." (added text in highlight) (approved Aug. 5, 2014).

#Miscellaneous

"Policy and Procedure Information and Updates: Public Recordings," *Memphis Police Dept.* **(**Dec. 17, 2013) (introducing policy and procedure related to public's "right to video record, photograph, and/or audio record MPD members").

#Miscellaneous

***R*. 3:9-1(b) ("Meet and Confer Requirement; Plea Offer")**

New Jersey Rules Governing Criminal Practice (requiring prosecutor and defense counsel to, "confer and attempt to reach agreement on any discovery issues, including any issues

pertaining to discovery provided through the use of CD, DVD, e-mail, internet or other electronic means").

#Discovery Materials

***R.* 13-5(c) ("Special Service Charge for Electronic Records")**

New Jersey Rules Governing Criminal Practice ("If defense counsel requests an electronic record ***, the prosecutor may charge, in addition to the actual cost of duplication, a special charge ***.")

#Discovery Materials

SB 178, enacted into law Oct. 8, 2015

This California legislation adds a new Chapter 3.6 (commencing with Section 1546) to Title 12 of Part 2 of the Penal Code ("the California Electronic Communications Privacy Act"). Generally, Section 1546 requires the government secure a search warrant to "access electronic device information by means of physical interaction or electronic communication." It also provides, among other things, that the Government must notify the target of an investigation about the information covered by a search warrant, that service providers must verify authenticity of information produced, and that service providers may voluntarily disclose communications unless otherwise prohibited by law.

#Fourth Amendment Warrant Required or Not

#Trial-Related

#Miscellaneous

TEXAS HB2268, Section 5A

(enacted into law June 14, 2013) (requiring issuance of search warrant, supported by finding of probable cause, when law enforcement seeks, "electronic customer data held in electronic storage, including the content of and records and other information related to a wire communication or electronic communication held in electronic storage, by the provider of an electronic communications service or a provider of a remote computing service ***, regardless of whether the customer data is held in this state or in a location in another state").

#Fourth Amendment Warrant Required or Not

ARTICLES

T. Alper, "Criminal Defense Attorney Confidentiality in the Age of Social Media," Vol. 31, No. 3, Criminal Justice (ABA Sec. of Crim. Justice: Fall 2016), https://www.americanbar.org/content/dam/aba/publications/criminal_justice_magazine/v31/TY_ALPER.authcheckdam.pdf

("the community of criminal defense lawyers need to be more intentional about this [social media-related ethics] training and adopt its own behavior *** and adopt a rigid rule against social media posts that have anything at all to do with client matters.")

#Discovery Materials

#Miscellaneous

#Sixth Amendment Assistance of Counsel

#Social Media

K.S. Bankston & A. Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents out of United States v. Jones, *YLJO Essay* (Jan. 9, 2014)

#Fourth Amendment Warrant Required or Not

D. Barrett, "U.S. Urges Bodycams for Local Police, but Nixes Them on Federal Teams," *Wall St. J.* A3 (Nov. 12, 2015)

#Discovery Materials

#Miscellaneous

D. Barrett, *et al.,* "In Europe's Terror Fight, Police Push to Access American Tech Firms' Data," *Wall St. J.* ___ (May 1, 2016)
("European counterterrorism officials say American laws and corporate policies are hampering their efforts to prevent the next attack ***.")

#Fourth Amendment Warrant Required or Not

#Miscellaneous

"Best Practices for Victim Response and Reporting of Cyber Incidents," Cybersecurity Unit, Computer Crime & Intellectual Property Section, *U.S. Dept. of Justice* (Version 1.0) (Apr. 2015)

#Miscellaneous

D.R. Beneman & D.L. Elm, “Extraterritorial Search Warrants Rule Change,” *Criminal Justice* 9 (Winter 2014)

#Fourth Amendment Warrant Required or Not

B. Bergstein, “What if Apple is Wrong?” *MIT Tech. Rev.* (posted Apr. 7, 2016)

(“Are we certain we want to eliminate an important source of evidence that helps not only cops and prosecutors but also judges, juries, and defense attorneys to arrive at the truth?”)

#Fifth Amendment Privilege Self-Incrimination

G. Blum & B. Wittes, “New Laws for New Threats Like Drones and Bioterrorism,” *Wall St. J.* C3 (Apr. 18-19, 2015)

#Miscellaneous

J. Bracy, “Does Stringray Use Violate Law, Target Minority Communities,” *The Privacy Advisor* (updated version posted Oct. 9, 2016)

(noting requests to FCC by civil liberties groups and senators to investigate use of cell site stimulators by law enforcement)

#Fourth Amendment Warrant Required or Not

Brennan Center for Justice, "New Analysis: Criminal Justice in President Trump's First 100 Days" (Apr. 20, 2017), https://www.brennancenter.org/press-release/new-analysis-criminal-justice-president-trump%E2%80%99s-first-100-days

#Miscellaneous

T.E. Brostoff, “Constitutional and Practical Dimensions of ESI in Federal and State Criminal Actions,” 13 *DDEE* 448 (Aug. 29, 2013)

(reporting on “discussion of topics including law enforcement’s expanding use of electronic devices, the admissibility of electronic evidence, and tools and best practices for practitioners and jurists”).

#Miscellaneous

T.E. Brostoff, "ESI in the Criminal Justice System Webinar Discusses Pre- and Post-Indictment Issues," 14 *DDEE* 152 (2014)

(reporting on two-part webinar that discussed various issues related to ESI in the investigation and prosecution of crimes).

#Fourth Amendment Ex Ante Conditions

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

#Discovery Materials

#Miscellaneous

T. Brostoff, "From Quon to Riley and Beyond: Criminal Law, eDiscovery and New Trends," 15 *DDEE* 527 (2015)

#Fourth Amendment Warrant Required or Not

#Miscellaneous

T. E. Brostoff, "Riley's Implications on Future Jurisprudence and Fourth Amendment Discussed in Webinar," 14 *DDEE* 399 (2014)

(reporting on webinar that addressed *Riley v. California* and other recent decisions and how courts might approach constitutional issues post-*Riley).*

#Fourth Amendment Warrant Required or Not

K. Burman, et al., Significant Developments in Law Enforcement Access Issues for Company Counsel," 17 DDEE 236 (2017), available from Bloomberg BNA

#Encryption

#Miscellaneous

#SCA

B. Canis & D.R. Peterman, “Black Boxes” in Passenger Vehicles: Privacy Implications (CRS: July 21, 2014)

(discussing policy implications of National Highway Traffic Safety Administration to make event data recorders mandatory on all new passenger vehicles sold in the United States).

#Miscellaneous

K. Chayka, “Somebody’s Watching: In the Age of Biometric Surveillance There is No Place to Hide,” *Newsweek* 28 (Apr. 25, 2014)

(“Today’s laws don’t protect Americans from having their webcams scanned for facial data”).

#Miscellaneous

K. Coates, "Reporting Near the Border? The ACLU has some Advice for You," Columbia J. Rev. (posted Apr. 7, 2017), https://www.cjr.org/watchdog/border-journalists-aclu-mexico.php

#Miscellaneous

D. Colarusso, “Portland’s Precrime Experiment and the Limits of Algorithms,” Lawyerist.com (posted Aug. 8, 2017), https://lawyerist.com/precrime-in-portland-a-canary-in-the-data-mine/

#Admissibility

#Miscellaneous

#Probation and Supervised Release

#Trial-Related

L. Constantin, “U.S. Drops Child Porn Case to Avoid Disclosing Tor Exploit,” IDG News Service (posted Mar. 6, 2017), https://www.computerworld.com/article/3176541/security/us-drops-child-porn-case-to-avoid-disclosing-tor-exploit.html

#Discovery Materials

#Fourth Amendment Warrant Required or Not

T. Cook, “A Message to Our Customers” (Feb. 16, 2016)

(explaining Apple's opposition to break encryption of cell phone used by shooter in San Bernardino attack)

#Fifth Amendment Privilege Self-Incrimination

J. DaSilva, "Digital Age Reshaping Privacy, Constitutional Protections," 16 *DDEE* 381 (2016) (reporting on panel discussion)

#Fourth Amendment Warrant Required or Not

L. Deutchman, "Is Cellphone Tracking Data Protected by the Fourth Amendment?" The Legal Intelligencer (posted Aug. 1, 2017) (Part One), http://www.thelegalintelligencer.com/latest-news/id=1202794122191/Is-Cellphone-Tracking-Data-Protected-by-the-Fourth-Amendment?mcode=1395262324557&curindex=36

#Fourth Amendment Warrant Required or Not

H.B. Dixon, Jr., "Another Harsh Spotlight on Forensic Sciences," Vol. 56, 37 No. 1, Judges' Journal 36 (ABA Jud. Div.: Winter 2017), https://www.americanbar.org/publications/judges_journal/2017/winter/another_harsh_spotlight_on_forensic_sciences.html

#Admissibility

#Discovery Materials

#Trial-Related

#Miscellaneous

H.B. Dixon, Jr., "Telephone Technology versus the Fourth Amendment," *Judges' Journal* 37 (ABA Judges Division: Spring, 2016)

("Predicting the direction of Fourth Amendment jurisprudence relating to telephones in increasingly difficult because of constant advancements in that technology.")

#Fourth Amendment Warrant Required or Not

Z. Elinson, "More Officers Wearing Body Cameras," *Wall St. J.* (Aug. 15, 2014)

(reporting that, "[m]ore police departments are outfitting policemen with wearable cameras that tape what officers see as they do their job, providing a record in the aftermath of incidents

like the one in Ferguson, Mo. ***").

#Miscellaneous

D.E. Elm & S. Broderick, "Third-Party Case Services and Confidentiality," *Criminal Justice* 15 (Spring 2014)

(commenting on growing trend to use third-party vendors and addressing need to maintain confidentiality when doing so).

#Miscellaneous

J.A. Engel, "Rethinking the Application of the Fifth Amendment to Passwords and Encryption in the Age of Cloud Computing," *Whittier L. Rev.*, Vol. 33, No. 3 (Summer 2012)

(addressing whether Fifth Amendment prevents government from forcing witness to provide password or encryption key).

#Fifth Amendment Self-Incrimination

C. Fariver, "FBI Would Rather Prosecutors Drop Cases Than Disclose Stingray Details," *Ars Technica* (Apr. 7, 2015)

#Fourth Amendment Warrant Required or Not

#Discovery Materials

M.L. Fox, "I Show You Exhibit E for Identification," *NYLitigator* 14 (NYSBA: Spring 2017)

#Trial-Related

#Miscellaneous

C. Friedersdorf, "The NYPD is Using Mobile X-Ray Vans to Spy on Unknown Targets," *The Atlantic* (posted Oct. 19, 2015)

#Fourth Amendment Warrant Required or Not

#Miscellaneous

D.K. Gelb & D.B. Garrie, “A Dilemma for Criminal Defense Attorneys: The Benefit of Pursing ESI Versus the Detriment of Implicating the Client,” 11 *DDEE* 339 (2011)

(addressing challenges faced by defense counsel in investigating role of ESI in criminal matters).

#Miscellaneous

D.K. Gelb, “Defending a Criminal Case from the Ground to the Cloud,” 27 *Criminal Justice,* No. 2 (2012)

(proposing guidelines for defense counsel to suppress or admit ESI at trial).

#Trial-Related

D. Gelb, “Overview of ESI Derived from a Motor Vehicle” (May 2017), available from the Editor

#Miscellaneous

A.D. Goldsmith & J. Haried, “The New Criminal ESI Discovery Protocol: What Prosecutors Need to Know,” 60 *UNITED STATES ATTORNEYS BULLETIN* 5 (Sept. 2012)

#Discovery Materials

#Trial Materials

A.D. Goldsmith, “Trends – Or Lack Thereof – In Criminal E-Discovery: A Survey of Recent Case Law,” 59 *United States Attorneys’ Bulletin* 2 (2011)

(noting that, unlike civil litigation, “a coherent body of case law on appropriate collection, management, and disclosure of ESI has yet to emerge in the criminal context”).

#Miscellaneous

J. Gershman, "Google and U.S. Fight Over Data," *Wall St. J.* B4 (Apr. 4, 2017)

#SCA

L.M. Gregory, “Teaching an Old Law New Tricks,” *Litigation News* 10 (ABA Sec. of Litigation: Summer 2016)
(discussing of expansion of government surveillance under the All Writs Act).

#Fifth Amendment Privilege Self-Incrimination

L.A. Gordon, "A Byte Out of Crime," 99 *ABA J.* ___ (Sept. 2013) (discussing constitutional concerns arising from "predictive policing")

#Miscellaneous

J. Gruenspecht, "'Reasonable' Grand Jury Subpoenas: Asking for Information in the Age of Big Data," 24 *Harvard J. L. & Tech.* 543 (2011)

(discussing constitutional and statutory limits on the scope of subpoenas and arguing that, "increasing use of digital storage technologies challenges even those limited boundaries").

#Miscellaneous

S. Gurman, "Police Tracking Social Media During Protests Stirs Concerns," *Top Tech News* (updated version posted Oct. 8, 2016)

("Increasingly common tools that allow police to conduct real-time social media surveillance during protests are drawing criticism from civil liberties advocates ***.")

#Fourth Amendment Warrant Required or Not

#Social Media

R.J. Hedges, "A Short Comment on 'Search Warrants for Cell Phones and Other Locations Where Electronically Stored Information Exists: The Requirements for Warrants Under the Fourth Amendment," 9 *Fed. Cts. L. Rev.* 31 (2016)

(arguing against imposition of *ex ante* conditions on issuance of search warrants)

#Fourth Amendment Particularity Requirement

R.J. Hedges, "Admissibility: Who Can Testify about ESI?" *Criminal Justice* 59 (ABA Sec. of Crim. Justice: Spring 2016)

(commenting on two decisions on the topic)

#Trial-Related

R.J. Hedges, "Hi Tech Obligations: The Tug of War Between the Constitution and Law Enforcement" (Vaporstream: posted Jan. 26, 2016)

(raising questions about tensions between needs of law enforcement and constitutional rights of suspects)

#Fifth Amendment Privilege Self-Incrimination

#Fourth Amendment Warrant Required or Not

R.J. Hedges, "'Hot Topics' for ESI in Criminal Matters," *Criminal Justice 43* (ABA Section of Crim. Justice: Fall 2016)

(focusing on how electronic information "fits" into various legal principles).

#Fifth Amendment Privilege Self-Incrimination

#Fourth Amendment Warrant Required or Not

R.J. Hedges & K.B. Weil, "How Will NY Courts Handle Encrypted Communications," *NYLJ 11* (Oct. 3, 2016)

(using criminal law analogy to address encryption in civil litigation)

#Fifth Amendment Privilege Self-Incrimination

R.J. Hedges, "Sentencing Guidelines, Corporate Governance and Information Management," 14 *DDEE* 238 (2014)

(discussing relationship between corporate governance and the Sentencing Guidelines).

#Miscellaneous

E. H. Holder, Jr., "In the Digital Age, Ensuring that the Department Does Justice," 41 *Geo. L.J. Ann. Rev. Crim. Proc.* iii (2012)

#Fourth Amendment Warrant Required or Not

#Miscellaneous

Hunton & Williams, "Email Privacy Act Reintroduced in Congress," (Privacy & Info. Sec. Law Blog: posted Jan. 13, 2017), https://www.huntonprivacyblog.com/2017/01/13/email-privacy-act-reintroduced-congress/

#Fourth Amendment Warrant Required or Not

G. Joseph, "Cellphone Spy Tools Have Flooded Local Police Departments," Citylab (posted Feb. 8. 2017) https://www.citylab.com/equity/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/

#Discovery Materials

#Fourth Amendment Warrant Required or Not

J. Jouvenal, "The New Way Police are Surveilling You: Calculating Your 'Threat Score," *Washington Post* (posted Jan. 10, 2016) (reporting on "software that scored the suspect's potential for violence").

#Miscellaneous

R.F. Kennedy, "Sequestration and the Impact on Access to Justice – a Growing Problem," 55 *NYSBA State Bar News* 22 (Sept./Oct. 2013)

(noting impact of sequestration in 2013 on federal courts and Legal Services Corporation).

#Trial-Related

O. Kerr, "9th Circuit Upholds Warrantless Email Surveillance of Person in the U.S. Communicating with Foreigners Abroad When the Foreigners are the 'Targets'" (Washington Post: Dec. 5, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/12/05/9th-circuit-upholds-warrantless-email-surveillance-of-person-in-the-u-s-communicating-with-foreigners-abroad-when-the-foreigners-are-the-targets/?utm_term=.a3b8842d4c3e

#Fourth Amendment Warrant Required or Not

O. Kerr, "Eleventh Circuit Deepens the Circuit Split on Applying the Private Search Doctrine to Computers," *Washington Post* (posted Dec. 2, 2015)

#Fourth Amendment Warrant Required or Not

O. Kerr, "The Fifth Amendment Limits on Forced Decryption and applying the 'Foregone Conclusion' Doctrine," *Washington Post* (posted June 7, 2016)

(commenting on application of doctrine to order requiring decryption of device)

#Fifth Amendment Privilege Self-Incrimination

O. Kerr, “Fifth Circuit Creates Split on Whether Prospective Cell-Site Collection is a Fourth Amendment ‘Search,’” The Washington Post (posted May 23, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/05/23/fifth-circuit-creates-split-on-whether-prospective-cell-site-collection-is-a-fourth-amendment-search/?utm_term=.628c71d6b509

#Fourth Amendment Warrant Required or Not

#SCA

O. Kerr, "The Fourth Amendment and Access to Automobile 'Black Boxes, " (Washington Post Mar. 30, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/30/the-fourth-amendment-and-access-to-automobile-black-boxes/?utm_term=.e860f9a26c7d

#Fourth Amendment Warrant Required or Not

O. Kerr, “The Fifth Amendment and Touch ID,” *Washington Post* (posted Oct. 21, 2016)

(commenting on application of Fifth Amendment privilege against self- incrimination to using fingerprint readers)

#Fifth Amendment Privilege Self-Incrimination

O. Kerr, “Fourth Circuit Adopts Mosaic Theory, Holds that Obtaining ‘Extended’ Cell-Site Records Requires a Warrant,” *Washington Post* (the Volokh Conspiracy) (posted Aug. 5, 2015)

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

O. Kerr, “The Geek Squad and the Fourth Amendment” (Washington Post: posted Jan. 11, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/11/the-geek-squad-and-the-fourth-amendment/?utm_term=.2e48346321bf

#Fourth Amendment Warrant Required or Not

O. Kerr, "Government 'Hacking' and the Playpen Search Warrant," *Washington Post* (posted Sept. 27, 2016)

(commenting on judicial decisions addressing "legality of a single search warrant that was used to search the computers of many visitors to a child pornography website")

#Fourth Amendment Warrant Required or Not

O. Kerr, "Judge Rejects Warrant Provision Allowing Compelled Thumbprints to Unlock iPhones" (Washington Post: posted Feb. 23, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/23/judge-rejects-warrant-provision-allowing-compelled-thumbprints-to-unlock-iphones/?utm_term=.df7610139687

#Fifth Amendment Self-incrimination

O. Kerr, "New York Court of Appeals to Hear Argument in 'In re 381 Search Warrants' Case" (Washington Post: posted Feb. 6, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/06/new-york-court-of-appeals-to-hear-argument-in-in-re-381-search-warrants-case/?utm_term=.012705fd6058

#Fourth Amendment Warrant Required or Not

O. Kerr, "Password-Sharing Case Divides Ninth Circuit in *Nosal II*," *Washington Post* (posted July 6, 2016 (commenting on 2-1 panel decision interpreting CFAA)

#Miscellaneous

O. Kerr, "The Path of Computer Crime Law," *Washington Post* (posted Oct. 13, 2016)

(commenting on changing judicial, legislative and technological changes)

#Miscellaneous

O. Kerr, "Preliminary Thoughts on the Apple iPhone Order in the San Bernardino Case," Parts 1-3, *Washington Post* (posted Feb. 18, Feb. 19 and Feb. 24, 2016)

(addressing issues raised by FBI requests for access to shooter's iPhone)

#Fifth Amendment Privilege Self-Incrimination

O. Kerr, "The Police Can't Just Share the Contents of a Seized iPhone with Other Agencies, Court Rules" (Washington Post: posted Feb. 21, 2017),

https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/21/the-police-cant-just-share-the-contents-of-a-seized-iphone-with-other-agencies-court-rules/?utm_term=.0b8797567273

#Fourth Amendment Warrant Required or Not

O. Kerr, "Relative vs. Absolute Approaches to the Content/Metadata Line," *Lawfare* (posted Aug. 25, 2016)

(addressing "apparent disagreement" in distinction between content and metadata)

#Fourth Amendment Warrant Required or Not

O. Kerr, "A Revised Approach to the Fifth Amendment and Obtaining Passwords," *Washington Post* (posted Sept. 25, 2015)

#Fifth Amendment Self-Incrimination

O. Kerr, "Remotely Accessing an IP Address Inside a Target Computer is a Search," *Washington Post* (posted Oct. 7, 2016)

(following up on earlier post "on the Playpen warrant currently being litigated in federal courts around the country")

#Fourth Amendment Warrant Required or Not

O. Kerr, "The Surprising Implications of the Microsoft/Ireland Case" (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.e1afb9448373

#Fourth Amendment Warrant Required or Not

#Miscellaneous

O. Kerr, "Third Party Rights and the Carpenter Cell-Site Case," The Washington Post (posted June 15, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/15/third-party-rights-and-the-carpenter-cell-site-case/?utm_term=.858fe1b800c4

#Fourth Amendment Warrant Required or Not

#Third Party Docrine

O. Kerr, "Thoughts on the Third Circuit's Decryption and Self- Incrimination Oral Argument," *Washington Post* (posted Sept. 9, 2016)

(commenting on oral argument in matter pending in the court)

#Fifth Amendment Privilege Self-Incrimination

O. Kerr, "United States v. Wallace is a GPS Case, Not a Cell-Site Case – Here's Why It Matters," The Washington Post (posted May 24, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/05/24/united-states-v-wallace-is-a-gps-case-not-a-cell-site-case-heres-why-it-matters/?utm_term=.348f33c57894

#Fourth Amendment Warrant Required or Not

#SCA

#Third-Party Doctrine

O. Kerr, "The Weak Main Argument in Judge Orenstein's Apple Opinion," *Washington Post* (posted Mar. 2, 2016)

(questioning opinion based on Supreme Court decisions)

#Fifth Amendment Privilege Self-Incrimination

#Miscellaneous

L. Kirchner, "Police in Florida and Other States are Building Up Private DNA Databases," *ABA Journal* (posted Sept. 14, 2016)

("collecting DNA from people who are not charged with—or even suspected of—any particular crime has become an increasing routine practice").

#Miscellaneous

J. Kosseff, "Should Tech Companies Be Subject to the Fourth Amendment," *Crunch Network* (posted Dec. 13, 2015)

#Fourth Amendment Warrant Required or Not

D.C. Kully & A.L. Fuentes, "New Criminal Charges Confirm that Companies Cannot Evade Antitrust Laws by Communicating in Increasingly High-Tech Ways," Holland & Knight Regulatory Litigation Blog (posted Aug. 9, 2017), https://www.hklaw.com/reglitblog/new-criminal-charges-confirm-that-companies-cannot-evade-antitrust-exposure-by-communicating-in-increasingly-high-tech-ways-08-09-2017/

#Admissibility

#Miscellaneous

#Trial-Related

Adam Liptak, "Sent to Prison by a Software Program's Secret Algorithms," N.Y. Times (Posted May 1, 2017), https://www.nytimes.com/2017/05/01/us/politics/sent-to-prison-by-a-software-programs-secret-algorithms.html?_r=0

#Admissibility

#Miscellaneous

#Probation and Supervised Release

#Trial-Related

A. Mackey, *et al.,* "Unreliable Informants: IP Addresses, Digital Tips and Police Raids" (EFF: Sept. 2016)

("How police and courts are misusing unreliable IP address information and what they can do to better verify electronic tips)

#Miscellaneous

S. Mahtani & D. Seetharaman, "Live Video Grows as a Platform for Violent Crime," Wall St. J. A3 (Jan. 13, 2017), https://www.wsj.com/articles/live-video-grows-as-platform-to-broadcast-violence-1484226002

#Social Media

F. Manjoo, "Police Cameras Can Shed Light, but Raise Private Concerns," *New York Times* (Aug. 20, 2014)

(reporting that, "[t]he crucial questions of when police should begin recording their work and who gets to decide which encounters should be recorded are still being worked out").

#Miscellaneous

J.P. Murphy & A. Fontecilla, "Social Media Evidence in Criminal Proceedings: A Frontier of New Legal Issues," *Richmond J. of Law and Tech.,* Vol. 19, No. 3 (2013)

(arguing that social media evidence raises unique legal challenges in criminal proceedings).

#Trial-Related

J.P. Murphy & L.K. Marion, "Riley v. California: The Dawn of a New Age of Digital Privacy," 14 *DDEE* 345 (2014)

("Recognizing the revolutionary nature of modern technologies—and it is clear that the [Supreme] Court's analysis extends well beyond cell phones-- the Court affirmed that mobile media is just *different.* With *Riley,* the Court ushers in a new age of digital privacy").

#Fourth Amendment Warrant Required or Not

#Miscellaneous

"New Contact System Makes Sure Offenders Are Never Out of Reach," *Third Branch News* (Feb. 11, 2014)

(reporting on use of "web-based Client Electronic Notification System (CENS) that will help officers maintain that contact [with individuals on pretrial release or on probation] and safeguard the community").

#Miscellaneous

M.G. Olsen, *et al.,* "Don't Panic: Making Progress on the 'Going Dark' Debate" (Berkman Center for Internet & Society at Harvard University: Feb. 1, 2016)

("A public debate unfolded alongside our meetings: the claims and questions around the government finding a landscape that is 'going dark' due to new forms of encryption introduced into mainstream consumer products and services by the companies who offer them. We have

sought to distill our conversations and some conclusions in this report.")

#Fifth Amendment Privilege Self-Incrimination

J. Palazzolo, "Defense Attorneys Demand Closer Look at Software Used to Detect Crime-Scene DNA," *Wall St. J.* A3 (Nov. 11, 2015)

#Discovery Materials

#Trial-Related

J. Palazzolo, "NSA Phone-Data Collection Program Set for Legal Challenge," *Wall St. J.* A2 (Sept. 2, 2014)

(reporting on appeals from two district court decisions on constitutionality of NSA surveillance).

#Fourth Amendment Warrant Required or Not

Peterson & E. Nakashima, "Obama Administration Explored Ways to Bypass Smartphone Encryption," *Washington Post* (posted Sept. 24, 2015)

#Fourth Amendment Warrant Required or Not

#Miscellaneous

Pillsbury Winthrop Shaw Pittman LLP, "Social Media Gets a 'Like' from SCOTUS: Comments Suggest Possible First Amendment Protection" (Social Media & Games Law Blog: posted Mar. 2, 2017), https://www.socialgameslaw.com/2017/03/scotus-social-media-first-amendment.html

#Social Media

J. Pontin, "Who Made Tim Cook King?" *MIT Tech. Review* (posted Apr. 26, 2016)

("should technology companies create black boxes, whose encryption is so strong that they cannot be unlocked without their users' consent, or treachery, even if law enforcement has a legitimate interest in seeing the boxes' contents?")

#Fifth Amendment Privilege Self-Incrimination

#Miscellaneous

Press Release, "Former Coach USA Inc. Executive Sentenced to 15 Months in Prison for

Obstruction of Justice" (Dept. of Justice Office of Pub. Affairs Mar. 23, 2017), https://www.justice.gov/opa/pr/former-coach-usa-inc-executive-sentenced-15-months-prison-obstruction-justice

#Discovery Materials

#Trial-Related

K. Robinson, "Judges Try to Read Tea Leaves; What's Next for Technology at High Court?" 15 DDEE 308 (2015)

#Fourth Amendment Warrant Required or Not

B.E. Rosenberg, "Statutory and Constitutional Limits on the Preservation of Evidence," 4 *Va. J. Crim. L.* 116 (2016)

J.S. Rubin, "Will 'Dragnet' Hacking Survive Appeals?" 17 *DDEE* 253 (2017), available from Bloomberg BNA

#Fourth Amendment Particularity Requirement

#Miscellaneous

S.A. Saltzburg, "Expert or Lay Opinion," *Criminal Justice* 45 (ABA Sec. of Crim. Justice: Fall 2016)

(discussing whether a witness offering a lay or expert opinion)

#Trial-Related

P. Shallwani, "Tablets to Help Fight Crime," *Wall St. J.* A17 (June 27, 2014)

(reporting on "potential of putting NYPD databases at officers' fingertips").

#Miscellaneous

T. Simonite, "How to Upgrade Judges with Machine Learning," MIT Tech. Rev. (posted Mar. 6, 2017), https://www.technologyreview.com/s/603763/how-to-upgrade-judges-with-machine-learning/

#Trial-Related

#Miscellaneous

D.R. Stoller, “Amazon Echo Murder Case in No Apple-FBI Encryption Battle,” 17 *DDEE* 23 (2017)

#Fourth Amendment Warrant Required or Not

D.R. Stoller, “Attorney General Sessions Favors Encryption Backdoors,” 17 *DDEE* 62 (2017)

#Fourth Amendment Warrant Required or Not

D.R. Stoller, “Senators Fail in Bid to Stop Long Distance Warrant Rule,” 16 *DDEE* 515 (2016)

#Miscellaneous

W. Stramiello, “In the Matter of 381 Search Warrants: Practical Advice for Consumers and Corporation,” 17 *DDEE* 210 (2017), available from Bloomberg BNA

#Miscellaneous

#SCA

M. Sullivan, “From Fines to Jail Time: How Apple Could be Punished for Defying FBI” (Benton Foundation: posted Feb. 24, 2016)

(discussing possible consequences of refusal to decrypt iPhone used by San Bernardino shooter)

#Fifth Amendment Privilege Self-Incrimination

J. Tashea, “Changes in Criminal Procedure Rule Could Expand the Government’s Investigative Net,” ABA Journal (posted June 1, 2017), http://www.abajournal.com/magazine/article/fed_rule41_warrant_surveillance/

#Fourth Amendment Particularity Requirement

#Fourth Amendment Warrant Required or Not

#Miscellaneous

R.M. Thompson, The Fourth Amendment Third-Party Doctrine (CRS: June 5, 2014)

("[T]his report explores the third-party doctrine, including its historical background, its legal and practical underpinnings, and its present and potential future applications").

#Fourth Amendment Warrant Required or Not

J. Valentino-Devries, "Police Snap Up Cheap Cellphone Trackers," WALL ST. J. (Aug. 19, 2015, 12:57 PM), https://www.wsj.com/articles/police-snap-up-cheap-cellphone-trackers-1439933271

#Fourth Amendment Warrant Required or Not

E. Volokh, "What Happens If You Take the Fifth in a Civil Case? An Important California Case Law Correction," *Washington Post* (the Volokh Conspiracy) (posted Aug. 30, 2015)

#Fifth Amendment

D.J. Waxse, "Search Warrants for Cell Phones and Other Locations Where Electronically Stored Information Exists: The Requirements for Warrants Under the Fourth Amendment," 9 *Fed. Cts. L. Rev.* 33 (2016)

(arguing for imposition of ex ante conditions on issuance of search warrants to satisfy Particularity Requirement)

#Fourth Amendment Particularity Requirement

"With LENS, Offender Data Quickly Reaches Officers on Beat," *Third Branch News* (Jan. 16, 2014)

#Miscellaneous

D.C. Weiss, "Murdered Woman's Fitbit Data Inconsistent with Husband's Story, Police Say," ABA Journal (posted Apr. 25, 2017), http://www.abajournal.com/news/article/murdered_womans_fitbit_data_was_inconsistent_with_husbands_story_police_say/

#Fourth Amendment Warrant Required or Not

#Miscellaneous

D. Weiss, “Residue on Cellphones Could Help Investigators, Study Finds,” ABA Journal (posted Nov. 16, 2016),http://www.abajournal.com/news/article/residue_on_cellphones_could_help_criminal_investigators_study_finds

#Miscellaneous

D. C. Weiss, “Trade-Secret Claims Hide Details of Technology that Sends Criminal Defendants to Jail,” ABA Journal (posted June 14, 2017), http://www.abajournal.com/news/article/trade_secret_claims_hide_details_of_technology_that_sends_criminal_defendan/

#Admissibility

#Miscellaneous

#Probation and Supervised Release

#Trial-Related

R. Wexler, “When a Computer Program Keeps You in Jail,” N.Y. Times (posted June 13, 2017), https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html

#Admissibility

#Miscellaneous

#Probation and Supervised Release

#Trial-Related

J. Zittrain, “A Few Keystrokes Could Solve the Crime: Would You Press Enter?” (Just Security: posted Jan. 12, 2016)

(considering whether companies should conduct searches at request of government)

#Fourth Amendment Warrant Required or Not

#Miscellaneous

J. Larson & J. Angwin, “Fact-Checking the Encryption Debate,” *ProPublica* (posted Dec. 15, 2015)

#Warrant Required or Not

#Miscellaneous

Publications

“Encryption Working Group Year-End Report,” House Jud. Comm. & House Energy and Commerce Comm. (Dec. 20, 2016), https://judiciary.house.gov/wpcontent/uploads/2016/12/20161220EWGFINALReport.pdf

#Encryption

#Fourth Amendment Warrant Required or Not

“Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations,” House Comm. On Oversight and Gov’t Reform (Comm. Staff Rpt. Dec. 19, 2016), https://oversight.house.gov/wp-content/uploads/2016/12/THE-FINAL- bipartisan-cell-site-simulator-report.pdf

#Fourth Amendment Warrant Required of Not

#Miscellaneous

T. Claypoole, "Smarter Devices = More Vulnerability to Government and Criminals," *National L. Rev.* (posted Nov. 15, 2016) (exploring how technological advances increase "deeper and more complex intrusions")

#Miscellaneous

C. Doyle, Extraterritorial Application of American Criminal Law (CRS: Oct. 31, 2016)

#Miscellaneous

C. Doyle, *The Federal Grand Jury* (CRS: May 7, 2015)

#Miscellanous

K. Finklea, et al., Court-Ordered Access to Smart Phones: In Brief (CRS: Feb. 23, 2016)

#Fourth Amendment Warrant Required or Not

#Fifth Amendment Privilege Self-Incrimination

E.C. Liu, A. Nolan & R.M. Thompson III, Overview of Constitutional Challenges to NSA Collection Activities (CRS: May 21, 2015)

#Fourth Amendment Warrant Required or Not

J.P. Murphy & Louisa K. Marion, “Digital Privacy and E-Discovery in Government Investigations and Criminal Litigation,” Chapter 6, The State of Criminal Justice 2015 (ABA: 2015)

#Fourth Amendment Warrant Required or Not

J. Tashea, "Cell Block," *ABA Journal* 20 (July 2016) ("Police face constitutional challenges for using cellphone tracking devices to locate suspects")

#Fourth Amendment Warrant Required or Not

R.M. Thompson II, Digital Searches and Seizures: Overview of Proposed Amendments to Rule 41 of the Rules of Criminal Procedure (CRS: Sept. 8, 2016)

#Fourth Amendment Warrant Required or Not

#Discovery Materials

R.M. Thompson II, *Encryption: Selected Legal Issues* (CRS: Mar. 3, 2016)

#Fifth Amendment Privilege Self-Incrimination

#Fourth Amendment Warrant Required or Not

Forensic Science in Criminal Courts: Ensuring Scientific Validity of Featured-Comparison Methods (Executive Office of the President, President’s Council of Advisors on Science and Technology Sept. 2016)

#Discovery Materials

#Trial-Related

#Miscellaneous

O. Tene, "*Microsoft v. USA*: Location of Data and the Law of the Horse," *IEEE Security & Privacy* (Nov./Dec. 2016) ("decision threatens to strengthen the tide of data localization")

#Social Media

#Miscellaneous

#Discovery Materials

Criminal E-Discovery: A Pocket Guide for Judges (FJC: 2015)

This Pocket Guide, issued by the Federal Judicial Center in 2015, was developed to "help judges manage complex e-discovery in criminal cases." It is available at fjc.gov.

#Discovery Materials

Miscellaneous

Massachusetts Evidence Guide for First Responders (Mass. Digital Evid. Consortium: Jan. 2013)

#Fourth Amendment Warrant Required or Not

Massachusetts Digital Evidence Guide, Office of the Attorney General (Cyber Crime Division: June 9, 2015)

#Fourth Amendment Warrant Required or Not Trial Materials

END DOCUMENT