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

Ronald J. Hedges, Editor

Nadira Persaud, Research Assistant

December, 2016

Table Of Contents

DECISIONS – FEDERAL

DECISIONS – STATE

STATUTES, REGULATIONS, ETC. – FEDERAL

STATUTES, REGULATIONS, ETC. – STATE

PUBLICATIONS

ARTICLES

“CRIMINAL ESI” UPDATE
November, 2016

TAGS

#Discovery Materials

#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

#Preservation and Spoliation

#Trial-Related

#Miscellaneous

#Social Media

ABBREVIATIONS
“Stored Communications Act” – SCA
“Cell Site Location Information” - CSLI

DECISIONS - FEDERAL

Belleau v. Wall, No. 15-3225 (7th Cir. Jan. 29, 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

Free Speech Coalition, Inc. v. Attorney General, No. 13-3681 (3d Cir. June 8, 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., No. 15-0603 (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

In re Order Requiring Apple, Inc., to Assist in the Execution of a Search Warrant, No. 15-MC-1902 (E.D.N.Y. Apr. 22, 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

In re: Grand Jury Subpoena, 16-MC-1300-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 Microsoft Corp., No. 16-MJ-8036 (D. Kan. Sept. 28, 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

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 Warrant to Search a Certain E-Mail Acct. Controlled and Maintained by Microsoft Corp., No. 14-2985 (2d Cir. July 14, 2016)

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

I/M/O Search of Info. Associated with E-Mail Addresses Stored at Premises Controlled by Microsoft Corp., No. 16-MJ-8036 (D. Kan. Sept. 28, 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 Application of the United States of America for an Order Relating to Telephones Used by Suppressed, No. 15 M 0021, 2015 WL 6871289 (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

Lane v. Anderson, No. 15-2153 (4th Cir. Aug. 17, 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, No. 14-3601 (6th Cir. Aug. 16, 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

Owner-Operator Indep. Drivers Ass'n v. USDOT, No. 15-3756 (7th Cir. Oct. 31, 2016)

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

United States v. Ackerman, No. 14-3265 (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 No

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. Brooks, No. 15-11015 (11th Cir. Apr. 15, 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. Browne, No. 14-1798 (3d Cir. Aug. 25, 2016)

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. 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. 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 extension is unwarranted and creates tension in case law.

#Trial Related

United States v. Caraballo, No. 12-3839-cr, 14-4203-cr (2d Cir. Aug. 1, 2016)

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

achieve the officers' necessary aim.

#Fourth Amendment Exigent Circumstances

United States v. Carpenter, No. Nos. 14-1572/1805 (6th Cir. Apr. 13, 2016)

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. Chavez, 14-cr-00185 (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. Ciara, No. 14-1003 (7th Cir. Aug. 17, 2016)

Ciara 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. Darby, No. 16-cr-00036-RGD-DEM (E.D. Va. June 3, 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. DE l'sle, No. 15-1316 (8th Cir. June 8, 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, No. 15-12033 (11th Cir. Oct. 25, 2016) (*per curiam*)

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. Elonis, No. 12-3798 (3d Cir. Oct. 28, 2016)

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, 2016 WL 953269 (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. Farrell, No. 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. Ganias, No. 12-240-cr (2d Cir. May, 27, 2016) (*en banc*)

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. Graham, No. 12-4659 (4th Cir. May 31, 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. Harry, No. 14-2160 (10th Cir. Feb. 29, 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. 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. Houston, No. 14-5800 (6th Cir. Feb. 8, 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. Kitzhaber, No. 15-35434 (9th Cir. July 13, 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, No. 16-cr-00053-TSE (E.D. Va. May 5, 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, No. 15-30001 (9th Cir. May 12, 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. Lambis, No. 15cr734 (S.D.N.Y. July 12, 2016)

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. Lara, No. 14-50120 (9th Cir. Mar. 3, 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. 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. Michaud, No. 15-cr-05351-RJB, 2016 WL 337263 (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. 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. Rarick, No. 14-4212 (6th Cir. Jan. 7, 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. Sember, No. 14-cr-141 (S.D. Ohio May 27, 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. Thomas, No. 14-14680 (11th. Cir. Apr. 1, 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. Valas, No. 15-50176 (5th Cir. May 20, 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. Williams, No. 13-cr-00764-WHO (S.D. Ca. Feb. 9, 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

DECISIONS – STATE

Commonwealth v. Carter, SJC-12043 (Mass. Sup. Jud. Ct. July 1, 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 for 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, SJC-11877 (Mass. Sup. Jud. Ct. Feb. 19, 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, SJC-11346 (Mass. Sup. Jud. Ct. Dec. 18, 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. Dorelas, SJC-11793 (Mass. Sup. Jud. Ct. Jan.14, 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

Gary v. State, A16A0666 (Ga. Ct. App. July 15, 2016)

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 he was charged. The Georgia Court of Appeals reversed the conviction, concluding that the conduct in a "private place" as required by the law.

#Miscellaneous

Moats v. Maryland, No. 1219 (Md. Ct. Special App. Oct. 25, 2016)

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 secure the warrant and to that there was a "common-sense nexus between the offenses Moats was accused of committing and the phone to be search." Moreover, the court held that, even assuming a lack of probable cause the good-faith exception to the Warrant Requirement would allow the admission of the photos and images.

#Fourth Amendment Good Faith Exception

#Fourth Amendment Warrant Required or Not

People v. Alejandro R., A144398 (Ca. Ct. App., 1st App. Dist., Div. 1 Dec. 30, 2015)

A juvenile was declared a ward of the state after he admitted to being an accessory to illegal drug sales. He challenged on appeal a condition of probation that required him to submit to warrantless searches of his electronic devices and his use of social media. The appellate court held that the condition was not so unrelated to the juvenile court's goal of preventing the appellant from selling and consuming illegal drugs as to be an abuse of discretion. However, the court modified the condition to "media of communication reasonably likely to reveal whether appellant is boasting about drug use or otherwise involved with drugs, such as text messages, voicemail messages, photographs, e-mail accounts, and social media accounts."

#Miscellaneous

#Social Media

People v. Badalamenti, 2016 NY Slip Op 02556 (Ct. App. Apr. 5, 2016)

The defendant was living with a woman and her minor child. The father of the child attempted to reach the mother over his cell phone and, over an open line, heard the defendant threatening the child. The father then used the "voice memo

function" of his phone to record what the defendant was saying. The recording was used against the defendant at trial and he was convicted of various child-abuse related offenses. On appeal, he challenged the admissibility of the recording, arguing that its making constituted an impermissible "eavesdropping" under New York law. The Court of Appeals affirmed the conviction. It interpreted the statute in issue to provide for vicarious consent on behalf of a child once a court finds that a parent had a good faith belief that the recording was "necessary to serve the best interests of the child" and that there was an "objectively reasonable basis for this belief." The record supported these findings.

#Trial-Related

#Miscellaneous

People v. Durant, 2015 NY Slip Op 08609 (Ct. App. Nov. 23, 2015)

At issue in this appeal was whether "the common law invariably require[s] a court to issue an adverse inference instruction against the People at trial based solely on the Police's failure to electronically record the custodial interrogation of a defendant." The Court of Appeals held that, "although the better practice would be for the police to use the equipment at their disposal to record interrogations, their failure to take such action does not, as a matter of law, automatically compel a trial court to deliver an adverse inference charge to the jury." The Court of Appeals left open the question whether a trial court could do so "based on the unique facts of a particular case."

#Trial-Related

#Miscellaneous

People v. John, 2016 NY Slip Op 03208 (Ct. App. Apr. 28, 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. Lopez, H041713 (Ca. Ct. App., 6th App. Dist. Jan. 25 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. P.O., A145284 (Ca. Ct. App., 1st App. Dist., Div. 1 Apr. 5, 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. Relerford, 2016 IL App (1st) 132531 (App. Ct., 6th Div. June 24, 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

Restrepo v. Carrera, No. 3D15-1964 (Fla. 3DCA Apr. 13, 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, concluding 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

State v. Andrews, No. 1496 (Md. Ct. Special. App. Mar. 30, 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. Bray, 281 Or. App. 584 (2016)

Defendant was convicted of various sexual assault charges and on appeal, argued that the court incorrectly denied his motion to compel the victim to comply with a subpoena *duces tecum* requiring her to turn over her computer for an in camera inspection for relevant evidence, and in denying his motion to dismiss based on prosecutorial misconduct. Court held that the court erred in denying defendant's motion to compel the victim to comply with the subpoena because the computer had already been subjected to forensic analysis, and the scope of the request was narrow, otherwise affirmed.

#Discovery Materials

State v. Buhl, SC 19412 (Conn. Sup. Ct. June 21, 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. Feliciano, A-24-14, 074395 (N.J. Sup. Ct. Mar. 9, 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 may 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 appeal from, among other things, the denial of his motion to suppress. The Appellate Division affirmed his convictions and his petition for certification was granted by the New Jersey Supreme Court.

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. Kohonen, No. 73339-7-I (Wash. Ct. App., Div. 1 Feb. 8, 2016)

The appellant, a juvenile, was found guilty of cyberstalking based on two tweets send 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. Jenkins, 294 Neb. 684 (Sup. Ct. Sept. 9, 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 in issue.

#Fourth Amendment Warrant Required or Not

State v. Loomis, Case No. 2015AP157-CR (Wisc. Sup. Ct. Apr. 5, 2016)

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. Moser, A15-2017 (Minn. Ct. App. Aug. 8, 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. Thomas, No. 34,042 (N.M. Sup. Ct. June 20, 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

Taylor v. State, 132 Nev. Advance Op. 27 (Nev. Sup. Ct. Apr. 21, 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

Wheeler v. State, No. 205, 2015 (Del. Sup. Ct. Mar. 2, 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, Case No. 15A01-1509-CR-1519 (Ind. Ct. App. Aug. 4, 2016)

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 appellate court reversed: "We decline to apply the third-party doctrine in the present case because 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." Moreover, "[c]ontinuing in the direction shown by our Supreme Court in *Riley* and Jones ***,

we hold that Zanders had a reasonable expectation of privacy in the historical location data generated by his cell phone but collected" by the provider. The court reversed the convictions.

#Fourth Amendment Warrant Required or Not.

STATUTES, REGULATIONS, ETC.- FEDERAL

"Intake and Charging Policy for Computer Crime Matters (USDOJ Sept. 11, 2014) (Released Oct. 25, 2016)

#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

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

STATUTES, REGULATIONS, ETC.- STATE

***Ch.* 651, Statutes of 2015, California Electronic Communications Privacy Act (enacted Oct. 8, 2015)**

#Fourth Amendment Warrant Required or Not

PUBLICATIONS

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

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

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

ARTICLES

T. Alper, "Criminal Defense Attorney Confidentiality in the Age of Social Media," *Criminal Justice* 4 (ABA Sec. of Crim. Justice: Fall 2016)

("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

#Social Media

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

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

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

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

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

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

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, "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, “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

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

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, “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, “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, “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)

#Miscellanous

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, “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, “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, “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, “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

_. 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

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. 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

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

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

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

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