

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

**Ronald J. Hedges, Editor**

**Nadira Persaud, Research Assistant**

**April, 2017**

© 2016 Ronald J. Hedges

*Reprint permission granted to all state and federal courts, government agencies, court appointed counsel, and non-profit continuing legal education programs*

# TABLE OF CONTENTS

<b>FOREWARD .....</b>	<b>7</b>
<b>TAGS.....</b>	<b>8</b>
<b>ABBREVIATION .....</b>	<b>9</b>

## **DECISIONS – UNITED STATES SUPREME COURT**

<b>Birchfield v. North Dakota.....</b>	<b>9</b>
<b>Perez v. Florida.....</b>	<b>10</b>

## **DECISIONS – FEDERAL**

<b>In re Application for Search Warrant.....</b>	<b>11</b>
<b>Garner v. Lee.....</b>	<b>11</b>
<b>In re Information Associated with One Yahoo.....</b>	<b>12</b>
<b>Microsoft v. United States.....</b>	<b>13</b>
<b>Microsoft Corp v. US Dept. of Justice.....</b>	<b>13</b>
<b>In Re Search Warrant to Google.....</b>	<b>14</b>
<b>United States v. Gilliam.....</b>	<b>14</b>
<b>United States v. Hulscher.....</b>	<b>15</b>
<b>United States v. Mohamud.....</b>	<b>16</b>
<b>United States v. Osborne.....</b>	<b>17</b>
<b>United States v. Patrick.....</b>	<b>18</b>

<b>United States v. Powell.....</b>	<b>19</b>
<b>United States v. Russian.....</b>	<b>19</b>
<b>United States v. Stratton.....</b>	<b>20</b>

## **DECISIONS – STATE**

<b>Garret v. Commonwealth.....</b>	<b>21</b>
<b>I/M/O Search of Content Stored by Google.....</b>	<b>22</b>
<b>I/M/O Search Warrants Directed to Facebook.....</b>	<b>23</b>
<b>Love v. State.....</b>	<b>23</b>
<b>In Re Mike H.,.....</b>	<b>24</b>
<b>People v. Badalamenti.....</b>	<b>25</b>
<b>People v. Bryant.....</b>	<b>26</b>
<b>People v. Durant.....</b>	<b>26</b>
<b>People v. Harris.....</b>	<b>27</b>
<b>People v. John.....</b>	<b>27</b>
<b>People v. Pakeman.....</b>	<b>28</b>
<b>People v. R.D.,.....</b>	<b>29</b>
<b>People v. Smith.....</b>	<b>29</b>
<b>States v. Bates.....</b>	<b>30</b>
<b>State v. Bray.....</b>	<b>30</b>
<b>State v. Diamond.....</b>	<b>31</b>
<b>State v. Edwards.....</b>	<b>31</b>

<b>State v. Hannah.....</b>	<b>32</b>
<b>State v. Stahl.....</b>	<b>33</b>
<b>State v. Worsham.....</b>	<b>33</b>
<b>United States v. Escamilla.....</b>	<b>34</b>

## **STATUTES, REGULATIONS, ETC. – FEDERAL**

<b>“Auto Parts Executive Pleads Guilt to Obstruction of Justice,” .....</b>	<b>34</b>
<b>“Evaluation of Corporate Compliance Programs,” .....</b>	<b>35</b>

## **STATUTES, REGULATIONS, ETC. – STATE**

<b>In re: Amendments to the Florida Evidence Code.....</b>	<b>35</b>
--	-----------

## **PUBLICATIONS**

<b>“Encryption Working Group Year-End Report,” .....</b>	<b>35</b>
<b>“Law Enforcement Use of Cell-Site Simulation Technologies: Privacy Concerns and Recommendations,” .....</b>	<b>36</b>

## **ARTICLES**

<b>Brennan Center for Justice, "New Analysis: Criminal Justice in President Trump's First 100 Days" .....</b>	<b>36</b>
<b>K. Coates, "Reporting Near the Border? The ACLU has some Advice for You," .....</b>	<b>36</b>
<b>J. Gershman, "Google and U.S. Fight Over Data," .....</b>	<b>37</b>

<b>T. Alper, “Criminal Defense Attorney Confidentiality in the Age of Social Media,”</b> .....	<b>37</b>
<b>L. Constantin, “U.S. Drops Child Porn Case to Avoid Disclosing Tor Exploit,”</b> .....	<b>37</b>
<b>H.B. Dixon, Jr., “Another Harsh Spotlight on Forensic Sciences,”</b> .....	<b>37</b>
<b>Hunton &amp; Williams, “Email Privacy Act Reintroduced in Congress,”</b> .....	<b>38</b>
<b>G. Joseph, “Cellphone Spy Tools Have Flooded Local Police Departments,”</b> .....	<b>38</b>
<b>O. Kerr, "The Fourth Amendment and Access to Automobile 'Black Boxes,'"</b> .....	<b>38</b>
<b>O. Kerr, “The Geek Squad and the Fourth Amendment”</b> .....	<b>39</b>
<b>O. Kerr, “Judge Rejects Warrant Provision Allowing Compelled Thumbprints to Unlock iPhones”</b> .....	<b>39</b>
<b>O. Kerr, “New York Court of Appeals to Hear Argument in ‘In re 381 Search Warrants’ Case”</b> .....	<b>39</b>
<b>O. Kerr, “9<sup>th</sup> Circuit Upholds Warrantless Email Surveillance of Person in the U.S. Communicating with Foreigners Abroad When the Foreigners are the ‘Targets’”</b> .....	<b>40</b>
<b>O. Kerr, “The Police Can’t Just Share the Contents of a Seized iPhone with Other Agencies, Court Rules”</b> .....	<b>40</b>
<b>O. Kerr, “The Surprising Implications of the Microsoft/Ireland Case”</b> .....	<b>40</b>
<b>S. Mahtani &amp; D. Seetharaman, “Live Video Grows as a Platform for Violent Crime,”</b> .....	<b>41</b>

<b>Pillsbury Winthrop Shaw Pittman LLP, “Social Media Gets a ‘Like’ from SCOTUS: Comments Suggest Possible First Amendment Protection” .....</b>	<b>41</b>
<b>Press Release, "Former Coach USA Inc. Executive Sentenced to 15 Months in Prison for Obstruction of Justice" .....</b>	<b>41</b>
<b>B.E. Rosenberg, “Statutory and Constitutional Limits on the Preservation of Evidence,” .....</b>	<b>41</b>
<b>T. Simonite, “How to Upgrade Judges with Machine Learning,” .....</b>	<b>42</b>
<b>D.R. Stoller, “Amazon Echo Murder Case in No Apple-FBI Encryption Battle,” .....</b>	<b>42</b>
<b>D.R. Stoller, “Attorney General Sessions Favors Encryption Backdoors,” .....</b>	<b>42</b>
<b>D.R. Stoller, “Senators Fail in Bid to Stop Long Distance Warrant Rule,” .....</b>	<b>42</b>
<b>D. Weiss, “Residue on Cellphones Could Help Investigators, Study Finds,” .....</b>	<b>42</b>
<b>M.L. Fox, "I Show You Exhibit E for Identification," .....</b>	<b>43</b>

## FOREWARD

This is the third edition of *Electronic Evidence in Criminal Investigations and Actions: Representative Court Decisions and Supplementary Materials*. The first was published in February and the second in December of 2016. The first edition attempted to be as “comprehensive” as a collection of representative things could be. The second and third editions update case law and materials. My intent is to continue updates on a somewhat regular basis and, at some indefinite point in time, consolidate every then-existing edition into one compilation which, of course, will itself be updated.

I have added additional tags in this third edition to assist anyone interested in undertaking searches. The new tags appear in red on page \_\_\_\_\_. My hope is that these new tags will be retroactively applied to the first and second editions.

This edition also features links to materials. The links were last visited as this edition was being compiled in March 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. As with the new tags, I hope to add links as appropriate in the first and second editions.

Now, a personal note about all the editions: 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 the editions 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:

The editions are 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 posting possible.

Not to be forgotten are the research assistants whose names appear on the cover pages of the editions and who toiled to assist me with digests of decisions and who labored over all the editorial work: Nadira Persaud and Trevor Satnick, recent graduates of Cardozo School of Law in New York City. I owe you both for your time and commitment. Thanks.

RJH April, 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*, No. 14-1468 (U.S. June 23, 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

***Perez v. Florida*, No. 16-6250 (Mar. 6, 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, Case No. 17M081 (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

### ***Garner v. Lee, No. 11-CV-00007 (PKC) (E.D.N.Y. Dec. 13, 2016)***

The petitioner in this *habeas* proceeding had been convicted of murder and other offenses. He argued in the petition that he had been denied effective assistance of counsel because his trial attorney had not obtained before trial records which would have detailed the petitioner's cellphone use on the night of the offenses,

although the State used the records on cross-examination to impeach the petitioner's alibi defense. Undertaking a *Strickland* analysis, the *habeas* court found that the State trial court had made an unreasonable application of the law when it denied the petitioner's ineffective assistance claim, that the failure of the trial attorney to secure the records was "inexcusable and devastating" to the defense, and that there was a reasonable probability that, but for the trial attorney's performance, the outcome would have been different. The *habeas* court granted the petition and ordered the petitioner released unless the State decided to retry him.

#Sixth Amendment Assistance of Counsel

#Trial-Related

***In re Information Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, 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

***Microsoft Corp. v. United States*, No. 14-2985 (2d Cir. Jan. 24, 2017)  
(denying *en banc* review)**

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

***Microsoft Corp. v. United States Dept. of Justice*, Case No. C16-0538JLR  
(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

***In re Search Warrant No. 16-960-M-01 to Google, Misc. No. 960-M-01 (E.D. Pa. Feb. 3, 2017)***

The Government secured warrants pursuant to Section 2703 Of 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

***United States v. Gilliam, No. 15-387 (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. 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. Mohamud, No. 14-30217 (9<sup>th</sup> 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. Osborne, No. 15-14283 (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*, No. 15-2443 (7<sup>th</sup> 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. Powell*, No. 14-2506/2507/15-1724 (6<sup>th</sup> 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. Russian*, No. 15-3213 (10<sup>th</sup> 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. Stratton*, Case No. 15-40084-01-DDC (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

## **DECISIONS – STATE**

### ***Garnett v. Commonwealth*, Record 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 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

### ***I/M/O Search of Content that is Stored at Premises Controlled by Google, Case No. 16-mc-80263-LB (N.D. Ca. Apr. 19, 2017)***

Google moved to quash a warrant issued pursuant to Section 2703(a) of the SCA that directed it to produce stored content of several email accounts. Google uses a “distributed system where algorithms determine how it sends and stored data – in packets or component parts – in aid of overall network efficiency.” As a result, responsive content was stored outside the United States. Relying on *I/M/O Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. (q.v.)*, Google argued that Section 2703(a) did not have extraterritorial effect. The court denied the motion. Relying on the reasoning of the dissenters from the denial of rehearing *en banc* in *Microsoft*, the court held that disclosure would be a domestic application of the SCA because Google was in the district from which the warrant issued and the warrant was directed to the only place where Google could access and produce the content.

#SCA

## ***I/M/O 381 Search Warrants Directed to Facebook, No. 16 (N.Y. Ct. App. Apr. 4, 2017)***

A trial court issued 381 warrants pursuant to the Stored Communications Act directed to Facebook for subscriber information and content from user accounts as part of a pending criminal investigation. The warrants also prohibited Facebook from, among other things, notifying its subscribers of the existence of the warrants. Facebook appealed and, after a stay was denied, complied with the warrants. While the appeal was pending some users were indicted and Facebook was permitted to advise the users of the existence of the warrants. However, Facebook's motion to compel disclosure of the affidavit that supported issuance of the warrants was denied. Facebook also appealed from that order. The Appellate Division dismissed both appeals because the orders were unappealable under New York law. The Court of Appeals affirmed the dismissal. Among other things, it held that, "because the orders resolving Facebook's motions relate to warrants issued in a criminal proceeding, and the Criminal Procedure Law does not authorize an appeal from either order."

#Miscellaneous

#SCA

## ***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

### ***In re Mike H., D069391 (5th Dist. Ca. Ct. App., Div. 1 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

### ***People v. Badalamenti, 2016 NY Slip Op 02556 (Ct. App. Apr. 5, 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. Bryant*, B271300 (Div. One, 2<sup>nd</sup> App. Dist., Ca. Ct. App. Apr. 3, 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. Durant*, 26 NY3d 341 (2015) (corrected through Feb. 3, 2016)**

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. Harris, F072865 (5<sup>th</sup> App. Dist. Ca. 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. John, 2016 NY Slip Op 03208 (N.Y. 2016)***

The defendant was convicted of possession of a weapon and menacing. The evidence against him included a handgun. The handgun was swabbed for DNA and reports issued which tied the defendant’s DNA to the handgun. At trial, the State offered a witness who did not conduct the DNA tests but instead asserted that the results, which had been conducted by a non-testifying analyst, were truthful. The defendant’s conviction was affirmed by the Appellate Division. The Court of Appeals reversed, holding that the reports were testimonial in nature and that, because the reports were admitted only “surrogate testimony,” the defendant’s right to confrontation had been denied. The Court of Appeals rejected the argument that every analyst who had been involved in DNA testing would have to testify. Rather, “an analyst who witnessed, performed or

supervised the generation of defendant’s DNA profile, or who used his or her independent analysis on the raw data, as opposed to a testifying analyst functioning as a conduit for the conclusions of others, must be available to testify.”

#Admissibility

#Sixth Amendment Right to Confrontation

***People v. Pakeman, A146013 (1<sup>st</sup> App. Dist., Div. 3, Ca. Ct. App. Jan. 24, 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. R.D., 2016COA186 (Dec. 29, 2016)***

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. Smith, No. 1-14-1814 (1<sup>st</sup> Dist., 3d Div., Ill. Ct. App. Mar. 1, 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

***State v. Bates*, Case 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*, 281 Or. App. 584 (2016)**

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. Diamond, A15-2075 (Minn. Ct. App. Jan. 17, 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. Edwards, SC 19735 (Conn. Sup. Ct. Apr. 11, 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. Hannah*, Docket No. A-5741-14-T3 (N.J. App. Div. Dec. 30, 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. Stahl*, Case No. 2D14-4283 (Fla. 2<sup>nd</sup> Dist. Ct. App. Dec. 7, 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. Worsham*, No. 4D15-2733 (4th DCA Mar. 29, 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 defendant 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

***United States v. Escamilla, No. 16-40333 (5<sup>th</sup> 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

**STATUTES, REGULATIONS, ETC. – FEDERAL**

**“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

“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?\\_ga=1.205433362.340464836.1489248103](https://www.justice.gov/criminal-fraud/page/file/937501/download?_ga=1.205433362.340464836.1489248103)

#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#search=sc16-181>

#Admissibility

#Trial-Related

## **PUBLICATIONS**

“Encryption Working Group Year-End Report,” House Jud. Comm. & House Energy and Commerce Comm. (Dec. 20, 2016),

<https://judiciary.house.gov/wp->

<content/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

## ARTICLES

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

K. Coates, "Reporting Near the Border? The ACLU has some Advice for You," Columbia J. Rev. (posted Apr. 7, 2017),

<http://www.cjr.org/watchdog/border-journalists-aclu-mexico.php?Daily>

#Miscellaneous

J. Gershman, "Google and U.S. Fight Over Data," Wall St. J. B4 (Apr. 4, 2017)

#SCA

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),

[http://www.americanbar.org/content/dam/aba/publications/criminal\\_justice\\_magazine/v31/TY\\_ALPER.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/publications/criminal_justice_magazine/v31/TY_ALPER.authcheckdam.pdf)

#Discovery Materials

#Miscellaneous

#Sixth Amendment Assistance of Counsel

#Social Media

L. Constantin, "U.S. Drops Child Porn Case to Avoid Disclosing Tor Exploit," *IDG News Service* (posted Mar. 6, 2017),

<http://www.computerworld.com.au/article/615386/us-doj-drops-child-porn-case-avoid-disclosing-tor-exploit/>

#Discovery Materials

#Fourth Amendment Warrant Required or Not

H.B. Dixon, Jr., "Another Harsh Spotlight on Forensic Sciences," Vol. 56,

No. 1, *Judges' Journal* 36 (ABA Jud. Div.: Winter 2017),  
[http://www.americanbar.org/content/dam/aba/publications/judges\\_journal/2009fall\\_jj\\_tech.authcheckdam.pdf](http://www.americanbar.org/content/dam/aba/publications/judges_journal/2009fall_jj_tech.authcheckdam.pdf)

#Admissibility

#Discovery Materials

#Trial-Related

#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)  
<http://www.citylab.com/crime/2017/02/cellphone-spy-tools-have-flooded-local-police-departments/512543/>

#Discovery Materials

#Fourth Amendment Warrant Required or Not

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=.5c5ace0aed16](https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/03/30/the-fourth-amendment-and-access-to-automobile-black-boxes/?utm_term=.5c5ace0aed16)

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=.94179ec985f1](https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/01/11/the-geek-squad-and-the-fourth-amendment/?utm_term=.94179ec985f1)

#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=.febd57ce4419](https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/23/judge-rejects-warrant-provision-allowing-compelled-thumbprints-to-unlock-iphones/?utm_term=.febd57ce4419)

#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=.78270decaaba](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=.78270decaaba)

#Fourth Amendment Warrant Required or Not

O. Kerr, “9<sup>th</sup> 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=.58992cfacc5](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=.58992cfacc5)

#Fourth Amendment Warrant Required or Not

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=.7496be0dd6d4](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=.7496be0dd6d4)

#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=.d39b7376ea53](https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.d39b7376ea53)

#Fourth Amendment Warrant Required or Not

#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

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),

<http://www.socialgameslaw.com/2017/03/scotus-social-media-first-amendment.html>

#Social Media

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

B.E. Rosenberg, "Statutory and Constitutional Limits on the Preservation of Evidence," 4 *Va. J. Crim. L.* 116 (2016)

#Preservation and Spoliation

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

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\\_coul](http://www.abajournal.com/news/article/residue_on_cellphones_coul)

[d\\_help\\_criminal\\_investigators\\_study\\_finds/](#)

#Miscellaneous

M.L. Fox, "I Show You Exhibit E for Identification," *NYLitigator* 14  
(NYSBA: Spring 2017)

#Trial Related

#Miscellaneous

END DOCUMENT

