4th Amendment & Technology

2018 – March 2019 Update

- CELL PHONE SEARCHES POST-RILEY
- CARPENTER: DIGITAL TRACKING (HISTORICAL VS. REAL-TIME)

Cell Phone Searches

Cell Phone Searches Post-Riley

Principles from Riley:

A person has the highest expectation of privacy in his cell phone

If the justification for searching a suspect's cell is to prevent the destruction of evidence or do a protective sweep, then a warrantless search is unconstitutional

BUT warrantless cell phone searches are still alive and well:

1. Exigency
2. Independent Source

- **US v. Barron-Soto, 820 F.3d 409 (11th Cir. 2016) (Info in affidavit supported p/c to issue a search warrant for the cell phones of two suspects allegedly involved in a meth distribution conspiracy, without considering any info obtained from an initial warrantless search of the phones)**
- **US v. Bah, 794 F.3d 617 (6th Cir.), cert. denied sub nom. Harvey v. United States, 136 S. Ct. 561, 193 L. Ed. 2d 447 (2015) (4th A violation, arising from warrantless search of smartphone seized from driver incident to arrest, did not taint subsequent searches of driver's and passenger's additional smartphones conducted pursuant to later-obtained search warrant, as would require suppression under exclusionary rules, where officer's affidavit in support of probable cause for search warrant intentionally omitted any discussion of evidence obtained from warrantless search of smartphone, relying instead on results of scans of magnetic strips of driver's and passenger's counterfeit credit, debit, and gift cards to establish probable cause)**

Warrantless Cell Phone Searches Post-Riley

3. Plain View
   - **US v. Morgan, 842 F.3d 1070 (8th Cir. 2016) (D had no REP under Fourth Amendment when he voluntarily displayed his cell-phone screen in the presence of detectives; D had his phone because he asked for it, he did not object when the detective observed his activities, and according to the detective's uncontested testimony D spontaneously shared information about his contacts)**
4. Consent
5. Border search, within reason
   - **US v. Vergara, 884 F.3d 1309 (11th Cir.), cert. denied, 139 S. Ct. 70 (2018) (forensic searches by DHS agents of D's cell phones after D returned to the US from Mexico and disembarked from cruise ship occurred at the border, and thus, did not require search warrant or probable cause to comply with 4th A's reasonableness requirement)**
6. Good Faith
   - **United States v. Miller, 641 F. App'x 242 (4th Cir. 2016), cert. denied, No. 16-822, 2017 WL 670288 (U.S. Feb. 21, 2017) (exclusionary rule did not apply to officers' warrantless search of six cell phones since search occurred one year before Riley and officers relied in good faith on existing law)**
   - **United States v. Gary, 790 F.3d 704, 705 (7th Cir. 2015) (search of cell phone took place five years before Riley)**

Warrantless Cell Phone Searches Post-Riley

7. Harmless error
   - **United States v. Jenkins, No. 15-3068, 2017 WL 961738 (7th Cir. Mar. 13, 2017) (introduction of information obtained by police as result of unconstitutional search of D's cellphone data was harmless, and thus did not warrant reversal of cocaine conviction, despite D's contention that, without search, government could not have shown that he was using cellphone number to arrange drug transactions, where there was ample evidence, independent of cellphone data, demonstrating D's guilt)**
   - **United States v. Blackman, 625 F. App'x 231 (6th Cir. 2015) (District court did not plainly err in admitting, at trial on charge of drug-trafficking conspiracy, evidence consisting of information police accessed on defendant's cell phone without a warrant; there was overwhelming evidence of defendant's guilt, separate from the information recovered from his cell phone, including testimony from witnesses linking defendant directly to the conspiracy)**

Warrantless Seizure of Cell Phone (under Plain View) & Then Get a Warrant

United States v. Henry, 827 F.3d 16, 28 (1st Cir.), cert. denied, 137 S. Ct. 374, 196 L. Ed. 2d 298 (2016)

- At the time Officer seized the phones, he had p/c to believe the phones had evidentiary value based on (1) D's nervousness and anxiety when questioned about the phones; (2) D's statement that he used the phones to take photographs, which Officer believed was significant in the context of a sex-trafficking investigation; (3) the possible existence of a sex-trafficking relationship with young woman in room, given the large sums of cash found in the motel room, D's inability to provide much information about woman's identity, and his statement that woman was from Michigan, which connected her to the report received from the Michigan HSI; and (4) the fact that other officer knew that D had previously used a phone to contact the fifteen-year-old girl who had been reported missing in Portland and suspected of being involved in trafficking.
- And although using a phone to take photographs is not inherently criminal, in the context of a sex-trafficking investigation, and based on Officer's knowledge and experience that smart phones are frequently used to take photographs of sex trafficking victims and to facilitate prostitution, this, along with the other information known to him at the time, was enough for Officer to have p/c to believe that the phones likely had evidentiary value in the investigation of the suspected crimes.
- Riley's concerns about the warrantless search of digital data stored within a smart phone are not implicated here, however, because by the time the phones were searched, a warrant had been obtained. It thus appears that the officers did exactly what the Supreme Court suggested they do: seize the phones to prevent destruction of evidence but obtain a warrant before searching the phones.

Warrantless Cell Search Ruled Unconstitutional & Excluded

Warrantless search of probationer's cellular telephone and the data it contained was unreasonable under the Fourth Amendment. While probationer's privacy interest was somewhat diminished by his status as a probationer and he had agreed to submit his person and property, including any residence, premises, container or vehicle under his control, to search and seizure, his privacy interest was still substantial in light of the broad amount of data contained in the phone, condition in probation order did not clearly encompass his cellular telephone and its data, and search was not needed to promote legitimate government interests of combatting recidivism and helping probationers integrate back into the community, as probationer had been convicted of a nonviolent drug offense and had merely missed his meeting with probation officer

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

Cell Phone Searches Post-Riley: Warrants

Warrants must meet particularity standard – a confusing standard when applied to cell phones

Search warrant that authorized search of defendant's residence and seizure of any cell phones found inside was not sufficiently particular to permit search of defendant's cell phones that were seized at the time of his arrest, and thus search warrant was invalid under Fourth Amendment; although application for warrant requested authorization to search the two phones already seized, the warrant did not identify either of the phones already in law enforcement custody and did not specify what materials law enforcement was authorized to seize from those phones.

United States v. Russian, 848 F.3d 1239 (10th Cir. 2017) (but not excluded b/c officer acted in good faith)

Search warrant permitting law enforcement officers to search for and seize "all computer hardware, including, but not limited to, any equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical or similar computer impulses or data" located in the defendant's residence authorized officers to search and seize defendant's cell phone; the cell phone was encompassed within the warrant's broad definition of "computer hardware," as the phone was a device capable of storing and transmitting computer data

United States v. Horton, 638 F. App'x 126 (3d Cir. 2016), cert. denied, 137 S. Ct. 679, 196 L. Ed. 2d 562 (2017)

Probable cause supported a magistrate judge's issuance of a warrant to search a defendant's cell phone, where the affidavit supporting the search warrant application stated that the defendant was suspected of crimes in which cell phones were frequently used by conspirators to text or call each other during the times that the fraudulent activity was taking place, and that the defendant continued to use his phone before opening a security door when police officers came to arrest the defendant.

United States v. Bass, 785 F.3d 1043 (6th Cir.), cert. denied, 136 S. Ct. 192, 193 L. Ed. 2d 151 (2015)

A search warrant authorizing the search of a defendant's cell phone for any records of communication, indicia of use, ownership, or possession, including electronic calendars, address books, e-mails, and chat logs was reasonable under the circumstances at the time, and thus was not overbroad, where, at the time the phone was seized, the officers could not have known where the information sought was located in the phone or in what format the information was

United States v. Bass, 785 F.3d 1043 (6th Cir.), cert. denied, 136 S. Ct. 192, 193 L. Ed. 2d 151 (2015)

Cell Phone Searches Post-Riley: Pennsylvania

Homicide detective received cell phones at police station as part of evidence seized at crime scene during investigation of recent homicide. Detective opened each phone, powered them on, searched the menu to discern its number. Left one phone on and monitored its incoming calls and texts. Answered the phone and identified himself as police officer. Court held that each act was a search: (1) opening phone; (2) navigating through phone's menus to obtain its number; (3) monitoring phone's incoming calls and text messages.
Violation of 4th A and Riley -> suppression warranted. Not harmless error.

Commonwealth v. Fulton, 179 A.3d 475 (Pa. 2018)

Parole Exception

Parole agent's warrantless search of defendant's cell phone for text messages and photos, after defendant admitted to agent that he had possessed a firearm following altercation with housemates, was reasonably related to his duty to investigate a suspected parole violation, and therefore, search complied with Fourth Amendment and statutory requirements; based on agent's prior experience he believed defendant's phone could contain additional evidence of a parole violation, such as conversations about the firearm or photographs of defendant with the firearm

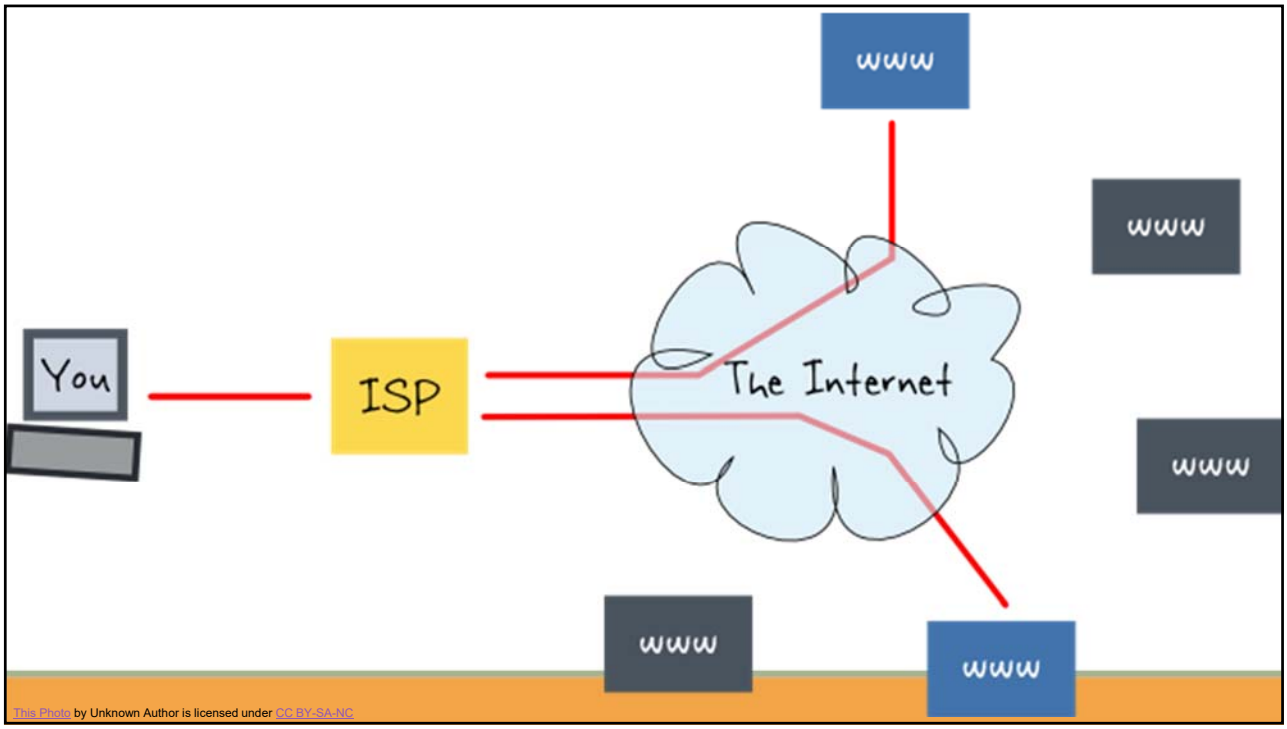
Commonwealth v. Murray, 174 A.3d 1147 (Pa. Super. 2017), appeal denied, 187 A.3d 204 (Pa. 2018)

Passage of Time from Initial Warrant

"In instances where the facts and circumstances upon which the search warrant was based remain unchanged with the passing of time, probable cause still exists."

Commonwealth v. Knoble, 2018 PA Super 135, 188 A.3d 1199, appeal denied, 198 A.3d 332 (Pa. 2018)

Digital Tracking: Internet Protocol Addresses



Digital Tracking & Computer Addresses

No REP in internet protocol address or file shared through peer-to-peer network

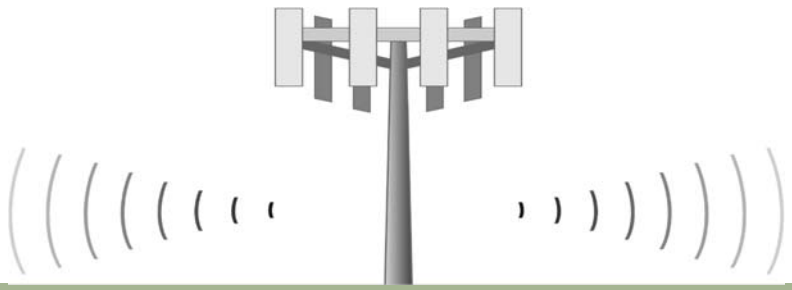
1. **United States v. Weast, 811 F.3d 743 (5th Cir.), cert. denied, 137 S. Ct. 126 (2016)** (D who used computer to share and download child pornography did not have reasonable expectation of privacy in his internet protocol address or a file shared through a peer-to-peer network, and thus law enforcement's warrantless use of peer-to-peer software to identify defendant's internet protocol address and to download possible child pornography from the file shared by defendant did not violate his Fourth Amendment right).

Cell Site Location Information

Carpenter v. US, -- U.S. --, 138 S.Ct. 2206 (June 22, 2018)

Cell Site Location Information

- What is CSLI
  - Registration & Handing off
  - In 1986 , 913 Cell Towers. In October, 2016, 277,087



Historical Cell Site Location Information (CSLI)

"The case before us involves the Government's acquisition of wireless carrier cell-site records revealing the location of Carpenter's cell phone whenever it made or received calls. This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake."

- A person's REP in his physical location and movements, and
- Third-party doctrine

Carpenter, 138 S. Ct. at 2214–15

"The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in Jones. ***Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.***"

Carpenter, 138 S. Ct. at 2216

Historical Cell Site Location Information (CSLI)

Historical CSLI present even more privacy concerns than GPS tracking of vehicle:

"Unlike the bugged container in Knotts or the car in Jones, a cell phone—almost a "feature of human anatomy," Riley, 573 U.S., at ——, 134 S.Ct., at 2484—tracks nearly exactly the movements of its owner. While individuals regularly leave their vehicles, they compulsively carry cell phones with them all the time. A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales. See id., at ——, 134 S.Ct., at 2490 (noting that "nearly three-quarters of smart phone users report being within five feet of their phones most of the time, with 12% admitting that they even use their phones in the shower"); contrast Cardwell v. Lewis, 417 U.S. 583, 590, 94 S.Ct. 2464, 41 L.Ed.2d 325 (1974) (plurality opinion) ("A car has little capacity for escaping public scrutiny."). Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user."

Carpenter, 138 S. Ct. at 2218

Historical Cell Site Location Information (CSLI)

"Moreover, the retrospective quality of the data here gives police access to a category of information otherwise unknowable. In the past, attempts to reconstruct a person's movements were limited by a dearth of records and the frailties of recollection. With access to CSLI, the Government can now travel back in time to retrace a person's whereabouts, subject only to the retention polices of the wireless carriers, which currently maintain records for up to five years. Critically, because location information is continually logged for all of the 400 million devices in the United States—not just those belonging to persons who might happen to come under investigation—this newfound tracking capacity runs against everyone. Unlike with the GPS device in Jones, police need not even know in advance whether they want to follow a particular individual, or when.

Whoever the suspect turns out to be, he has effectively been tailed every moment of every day for five years, and the police may—in the Government's view—call upon the results of that surveillance without regard to the constraints of the Fourth Amendment. ***Only the few without cell phones could escape this tireless and absolute surveillance."***

Carpenter, 138 S. Ct. at 2218

Historical Cell Site Location Information (CSLI)

"We decline to grant the state unrestricted access to a wireless carrier's database of physical location information. In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection. The Government's acquisition of the cell-site records here was a search under that Amendment."

Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018)

Historical Cell Site Location Information (CSLI)

"Our decision today is a narrow one."

Does NOT address:

- Real-time CSLI
- "Tower Dumps"
  (a download of information on all the devices that connected to a particular cell site during a particular interval)
- Conventional surveillance techniques and tools, such as security cameras
- Other business records that might incidentally reveal location information
- Other collection techniques involving foreign affairs or national security

Historical Cell Site Location Information (CSLI)

FOUR Dissents:

KENNEDY, THOMAS, ALITO DISSENT - caution on limitation of law enforcement:

"The new rule the Court seems to formulate puts needed, reasonable, accepted, lawful, and congressionally authorized criminal investigations at serious risk in serious cases, often when law enforcement seeks to prevent the threat of violent crimes. And it places undue restrictions on the lawful and necessary enforcement powers exercised not only by the Federal Government, but also by law enforcement in every State and locality throughout the Nation. Adherence to this Court's longstanding precedents and analytic framework would have been the proper and prudent way to resolve this case."

THOMAS DISSENT - Katz needs to be reconsidered because it didn't adequately address WHO has REP

Historical Cell Site Location Information (CSLI)

FOUR Dissents:

ALITO DISSENT - huge departure, unintended damaging consequence

"I share the Court's concern about the effect of new technology on personal privacy, but I fear that today's decision will do far more harm than good. The Court's reasoning fractures two fundamental pillars of Fourth Amendment law, and in doing so, it guarantees a blizzard of litigation while threatening many legitimate and valuable investigative practices upon which law enforcement has rightfully come to rely."

GORSUCH DISSENT - agrees with conclusion but suggests dismantling of entire REP analysis and starting over

Real-Time GPS Tracking through Cell Phone

Exigent circumstances justify the obtaining of real-time GPS tracking through cell phone

- Exigent circumstances justified global positioning system (GPS) tracking defendant's cell phone and obtaining such information under Stored Communications Act (SCA) from cell phone provider without a warrant, where law enforcement, after discussions with foster mother, social worker, and biological mother, believed defendant was taking child to a city to work as a prostitute.

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

- Police officers had legitimate, good faith belief that defendant needed to be apprehended immediately, and thus exigent circumstances justified warrantless "pinging" of defendant's cell phone by his phone service provider to locate him following discovery of body of woman who dealt drugs for defendant; position of woman's body and gunshot wound to back of her head indicated that her death was an execution, officers properly considered defendant to be primary suspect in woman's murder, given woman's statement to police at time of her arrest that she was involved in drug activity with defendant and was extremely afraid of him, and officers had specific reasons to think defendant would commit acts of violence against undercover agents and police informants, as woman's murder suggested that police's investigation of defendant's drug operation had been discovered.

  United States v. Caraballo, 831 F.3d 95 (2d Cir. 2016), cert. denied, 137 S. Ct. 654, 196 L. Ed. 2d 546 (2017)

Real-Time GPS Tracking through Cell Phone

A person wanted on probable cause (and an arrest warrant) who is taken into custody in a public place, where he had no legitimate expectation of privacy, cannot complain about how the police learned his location. Recall that the cell-site simulator (unlike the GPS device in *Jones*) was not used to generate the probable cause for arrest; probable cause to arrest Patrick predated the effort to locate him. From his perspective, it is all the same whether a paid informant, a jilted lover, police with binoculars, a bartender, a member of a rival gang, a spy trailing his car after it left his driveway, the phone company's cell towers, or a device pretending to be a cell tower, provided location information. A fugitive cannot be picky about how he is run to ground. So it would be inappropriate to use the exclusionary rule, even if the police should have told the judge that they planned to use a cell-site simulator to execute the location warrant.

The Department of Justice announced last September that in the future it would ordinarily seek a warrant, plus an order under the pen-register statute, 18 U.S.C. § 3123, before using a cell-site simulator, but it has not conceded that this is constitutionally required. 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 any United States court of appeals. We think it best to withhold full analysis until these issues control the outcome of a concrete case.

United States v. Patrick, 842 F.3d 540, 545 (7th Cir. 2016)