FIRST DISTRICT APPELLATE PROJECT
TRAINING SEMINAR
January 16, 2015

TECHNOLOGY, PRIVACY AND THE FOURTH AMENDMENT: GPS LOCATION TRACKING AND CELL PHONE SEARCHES

KATHRYN SELIGMAN
Staff Attorney
First District Appellate Project
January 2015

TABLE OF CONTENTS

PART ONE
LAW ENFORCEMENT USE OF GPS DEVICES FOR SURVEILLANCE AND INVESTIGATION

I. *UNITED STATES V. JONES* (2012) 132 S.CT. 945

In *United States v Jones*, all nine Supreme Court justices agreed that law enforcement's surreptitious attachment of a GPS tracking device to the underside of a vehicle, and the subsequent use of that device to constantly monitor the defendant's movements in the vehicle on public streets for four weeks, constituted a search within the meaning of the Fourth Amendment. However, the justices disagreed as to why this was so.

A. Overview of the Three Opinions in *Jones*[1]

The justices filed three separate opinions: 1) Justice Scalia filed the majority opinion, joined by Chief Justice Roberts and Justices Kennedy, Thomas and Sotomayor. 2) Justice Sotomayor filed a separate concurring opinion. 3) Justice Alito filed a concurring opinion, joined by Justices Ginsburg, Breyer and Kagan.

In these three opinions, the justices spent much of their time debating which test should be used to determine whether the officers conducted a Fourth Amendment search. Does a court employ the traditional trespass test requiring a physical invasion of the individual's property, or does the court use the test introduced in the mid-20th century which determines whether the officers' actions violated the individual's reasonable expectation of privacy? (See *Katz v. United States* (1967) 389 U.S. 347.) Moreover, did the reasonable expectation of privacy test augment or replace the older trespass standard?

The majority opinion, authored by Justice Scalia, concluded that the trespass test is still viable. (*United States v. Jones* (2012) 132 S.Ct. 945, 949-51.) Scalia then applied that test to determine that the officers conducted a search when they physically occupied the defendant's property, by secretly attaching a GPS device to the underbody of his jeep, for the purpose of obtaining information about his movements on public roads. (*Jones, supra*, at 949.) Scalia famously analogized this police practice to "a constable concealing

---

[1] **I recommend that you first read this summary of the three *Jones* opinions. If you are interested in a more detailed discussion of the three justices' analyses, read all or part of the remainder of section I.**

himself in the target's coach in order to track its movements." (*Id*., at 950. fn. 3.) Scalia found it unnecessary to determine whether the use of the GPS device to track the defendant's movements for four weeks violated his reasonable expectation of privacy. (*Id*., at 953-54.) Scalia also declined to decide if a GPS search requires probable cause and a warrant. (*Ibid*.)

In his concurring opinion, Justice Alito criticized the majority's reliance on the out-dated trespass theory and its focus on the installation of the GPS device. Alito concluded that in the later half of the 20th century, the Supreme Court effectively replaced the trespass test with the *Katz* reasonable expectation of privacy standard. (*Jones, supra*, at 958-61 [conc. opn. of Alito, J].) In deciding whether a search occurred in this case, Alito focused on the officers' use of the device for surveillance and concluded that the four-week-long tracking of the movements of the vehicle that the defendant drove violated his reasonable expectation of privacy. (*Id*., at 955-56.)

In her concurring opinion, Justice Sotomayor agreed that both the trespass test and the reasonable-expectation-of-privacy test can be used to determine whether a Fourth Amendment search has occurred. (*Jones, supra*, at 954-55 [conc. opn. of Sotomayor, J.].) She joined the majority opinion because she agreed that the officers in this case conducted a search, under the trespass theory, when they installed the GPS device on the defendant's car for surveillance purposes. However, she also agreed with Justice Alito that the officers' use of GPS to monitor the defendant's public movements for four weeks violated his reasonable expectation of privacy, as it allowed the state to capture a wealth of private details regarding the defendant's activities and associations. (*Id.*, at 955-56.)

Justice Sotomayor provided the fifth vote for Scalia's position that the installation of the GPS device on a subject's vehicle was an unconstitutional trespass, and the fifth vote for Alito's position that use of that device to monitor the subject's movements in the vehicle for four weeks violated the suspect's reasonable expectation of privacy.

In the majority opinion, Justice Scalia never addressed the threats to privacy raised by law enforcement's use of this new location-tracking technology. However, more interesting discussions are found in the concurring opinions. Justice Alito discussed how our use and awareness of these increasingly sophisticated location monitoring devices, including smart phones, may affect the average person's reasonable expectation of privacy. As a society, are we willing to sacrifice privacy for convenience and security? (*Id.*, at 962-63.) Justice Sotomayor wrote eloquently about the threat to long-term privacy posed by the government's storage and continuing access to the considerable personal information gained through GPS tracking of an individual's movements. (*Id.*, at 955-56.)

B. The Underlying Facts and Lower Court Proceedings

Because Defendant Jones, a nightclub owner, was suspected of drug trafficking, he became the target of a law enforcement investigation. Using various techniques, including visual surveillance of the nightclub, the officers obtained incriminating information which they used to obtain a warrant from the federal district court. This warrant authorized the officers to place an electronic tracking device on a jeep used by Jones within 10 days. On the 11th day, officers installed a GPS tracking device on the undercarriage of the jeep while it was parked in a public lot. For the next 28 days, the officers used this GPS device to track the movements of the jeep driven by Jones. The device established the jeep's locations and sent that information to a government computer. In the four weeks, the device relayed more than 2,000 pages of data. (*Jones, supra*, at 948.)

Jones and his co-conspirators were charged with conspiracy to possess and distribute cocaine. Before trial in district court, Jones filed a motion to suppress all the evidence obtained through the use of the GPS tracking device. (In this litigation, the government conceded that the officers had not complied with the warrant requirements, but argued that no warrant was required to install and use GPS surveillance.) The district court denied the suppression motion. At trial, the prosecution introduced the evidence obtained through GPS tracking that connected Jones to the alleged conspiracy. Jones was convicted. (*Id.*, at 948-49.)

Jones appealed, and the United States Court of Appeals for the D.C. Circuit reversed the conviction based on the lower court's erroneous denial of the motion to suppress the GPS-generated evidence. (*Id.*, at 949.) The Circuit Court held that the warrantless use of the GPS device violated the Fourth Amendment. (See *United States v. Maynard* (D.C. Cir. 2010) 625 F.3d 766.)[2] The Court applied the *Katz* reasonable-expectation-of-privacy test to conclude that the law enforcement officers had conducted a Fourth Amendment search when they *used* the GPS device that had been surreptitiously placed on Defendant Jones's jeep to track his movements 24 hours a day for four weeks. (*Maynard, supra*, 615 F.3d at 555-566.) This constant long-term surveillance, made possible by recent GPS technology, violated the defendant's reasonable expectation of privacy as it revealed a pattern of his activities and associations over a month's time. The appellate court did not discuss whether the surreptitious installation of the GPS device on the defendant's jeep was a trespass.

---

[2] Mr. Maynard and Mr. Jones were co-defendants, both found guilty of participating in the drug conspiracy.

C. The Grant of Certiorari, the Split of Authority and the Supreme Court's Beeper Cases

The Supreme Court granted certiorari, presumably because of a split of authority in the lower courts on this issue. Prior to *United States v. Maynard*, the majority of appellate courts that considered the issue ruled that the surreptitious attachment of an electronic location-tracking device to an individual's vehicle, and the use of that vehicle to track his movements on public roads, did not violate the individual's reasonable expectations of privacy, and therefore, did not constitute a Fourth Amendment search. (See, e.g. *United States v. McIver* (9th Cir. 1999) 186 F.3d 1119, 1126-27; *United States v. Garcia* (7th Cir. 2007) 474 F.3d 994, 996-98; *United States v. Marquez* (8th Cir. 2010) 605 F.3d 604, 609-10; *United States v. Pineda-Moreno* (9th Cir. 2010) 591 F.3d 1212, 1214-17.) For the former point, the court's reasoned that the undercarriage was part of the vehicle's exterior – an area in which the vehicle owner has no reasonable expectation of privacy. (See, e.g. *United States v. McIver, supra*, 186 F.3d at 1126-27; *United States v. Pineda-Moreno, supra*, 591 F.3d at 1214.)[3] For the latter point, these federal cases relied on the Supreme Court's statement in it's leading beeper case, *United States v. Knotts*: "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." (*United States v. Knotts* (1983) 460 U.S. 276, 281.) These courts believed that *Knotts* had settled the issue of whether the electronic tracking of a vehicle on public streets constituted a Fourth Amendment search. (See, e.g. *United States v. Garcia, supra*, 474 F.3d at 996.)

After the Supreme Court's decisions in the two beeper cases, *United States v. Knotts* (1983) 460 U.S. 276 and *United States v. Karo* (1984) 468 U.S. 705*, United States v. Maynard, supra,* 625 F.3d at 766, was the first federal circuit case to hold that officers conducted a search when they attached an electronic tracking device to the underside of a suspect's car and used it for location monitoring following.[4] In *Knotts*, the Court held that

---

[3] Three state Supreme Courts had concluded that the use of electronic tracking devices violated the search and seizure protections afforded by their state constitutions. (See *Pineda-Moreno, supra*, at 1216, fn.2, citing *People v. Weaver* (2009) 12 N.Y.3d 433 [909 NE.2d 1195]; *State v. Jackson* (2003) 150 Wash.2D 251 [76 P.3d 217]; *State v. Campbell* (1988) 306 Or. 157 [759 P.2d 1040].)

[4] Eight years prior to *Knotts* and *Karo*, the Fifth Circuit held that the installation of a beeper on the defendant's car and the use of that device to monitor the defendant's movements while he drove the van on public streets violated his reasonable expectation of privacy. Thus, it was a search requiring a warrant based on probable cause. (*United*

officers' *use* of a concealed beeper, transported in the defendants' vehicle, to track the vehicle's movements on public streets was not a Fourth Amendment search.[5] In *Karo*, the Court had concluded that officers did not invade the defendant's reasonable expectation of privacy when they *installed* a beeper in a container with the container owner's consent.[6] In *Maynard*, the D.C. Circuit found that *Knotts* was not controlling authority, as it involved the limited use of beeper signals to track the defendant's movements during a single discrete journey; the GPS device attached to the defendant's vehicle allowed the officer to conduct comprehensive and sustained monitoring 24 hours a day for one month. (*Maynard, supra*, 615 F.3d at 556-58.)

States v. Holmes (1975) 521 F.2d 859 [affd. en banc in *United States v. Holmes* (1976) 537 F.2d 227].) The reasoning in *Holmes* anticipated conclusions reached in *Maynard* and Jones, nearly a quarter century later.

[5] In *Knotts*, the police suspected that three individuals (Armstrong, Petschen and Knotts) were purchasing chemicals to use in manufacturing methamphetamine. They learned that Armstrong was buying the chemicals and delivering them to Petschen, but they did not know the location of the suspected drug lab. With the consent of the chemical company's owner, officers installed a beeper (a radio transmitter which emits periodic signals) into a container of chloroform that was sold to Armstrong. Armstrong transferred the container carrying the hidden beeper to Petschen's vehicle. The officers used both visual surveillance and intermittent signals emitted by the beeper to track the container's 100-mile journey from Petschen's house to a rural cabin owned by Knotts, where they found the drug lab. (*Knotts, supra*, 460 U.S. at 277-79.) The Supreme Court determined that Petschen had no reasonable expectation of privacy in his movements on public streets; his travel over particular roads to a specific destination were facts he voluntarily conveyed to anyone who wanted to look. The officers' use of the beeper to efficiently augment their visual surveillance was not a Fourth Amendment search. (*Id*., at 281-82.)

[6] In *Karo*, DEA agents learned from an informant that the co-defendants had contacted him and ordered 30 gallons of ether, which they were using for criminal purposes. The agents obtained a court order authorizing the installation of a beeper in one of the containers of ether in order to monitor the co-defendants' future movements. The informant transferred the container, with the beeper inside, to Defendant Karo. The agents relied on signals transmitted by the beeper to determine that Karo took the container inside his home. (*Karo, supra*, at 708-10.) The Court held that the use of the beeper to monitor the container's location within a private residence violated the reasonable expectation of privacy of those with interests in the residence; this information could not have been visually verified without entering the home. (*Id.*, at 714-15.)

D. The *Jones* Majority Opinion Authored by Justice Scalia (Joined by Chief Justice Roberts and Justices Kennedy, Thomas and Sotomayor)

In the majority opinion, Justice Scalia held that the attachment of a GPS tracking device to an individual's vehicle, and the subsequent use of that device to monitor the vehicle's movements on public streets constitutes a search within the meaning of the Fourth Amendment" (*Jones, supra*, at 949.) Scalia employed a traditional Fourth Amendment analysis, which looked to the past rather than the future. He focused on the surreptitious installation of the GPS device on the defendant's vehicle, and concluded that the officers trespassed by "physically occupied private property for the purpose of obtaining information. ... [S]uch a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted" in the late 18th Century. And it was still a search in the first decade of the 21st Century. (*Id*., at 949) Scalia paid no attention to the expanded scope and duration of the surveillance permitted by modern electronic location-tracking technology.

1. The Traditional Trespass Test Survives to Determine Whether An Officer's Actions Qualify as a Fourth Amendment Search

Justice Scalia emphasized that the Fourth Amendment expressly protects "the right of the people to be secure in their persons, houses, papers and *effects*" from unreasonable searches and seizures." (*Jones, supra*, at 949 [emphasis added].) These words reflect the founders' concern with preventing unreasonable physical intrusions by government officials upon citizens' private property. (*Ibid*.) Consistent with this intent to protect private property, the Court's Fourth Amendment jurisprudence was tied to common-law trespass from the 18th Century until the latter half of the 20th Century. Under the trespass test, a search occurred only when law enforcement officers physically entered or occupied private property for the purpose of obtaining information. (*Id.*, at 949-50 [citations omitted].) Then, beginning with *Katz v. United States* (1967) 389 U.S. 347, the Court deviated from this property-based approach. In *Katz*, the Court held that "the Fourth Amendment protects people, not places". (*Katz, supra*, at 351.) A new standard was adopted to determine whether a search had occurred: Did the actions of the government officers violate the person's reasonable expectation of privacy? (*Jones*, *supra*, at 950, citing *Katz*, *supra, at 360* [conc. opn. of Harlan, J.]; *Bond v. United States* (2000) 529 U.S. 334, 338.)[7]

---

[7] In *Katz*, the Supreme Court held that the government's use of an electronic device attached to the outside of a public phone booth to record calls that the defendant placed

Justice Scalia stated that the *Katz* reasonable-expectation-of-privacy standard did not replace the traditional trespass test. Rather, it provided an alternative method of assessing whether a Fourth Amendment search had occurred, particularly when the officers had *not* trespassed upon the person's property. (*Id.*, at 950-51.)

2. Applying the Trespass Test, the Officers Conducted a Fourth Amendment Search When They Installed the GPS Device on the Defendant's Jeep For the Purpose of Obtaining Information

Justice Scalia reasoned that "[i]t is beyond dispute that a vehicle is an 'effect' as that term is used in the [Fourth] Amendment." (*Id.*, at 949, citing *United States v. Chadwick* (1977) 433 U.S. 1, 12.) Moreover, the defendant had a property interest in the jeep; although the vehicle was registered to his wife, Jones was the exclusive driver and had the property rights of a bailee. (*Id*., at 949, fn. 2.) When the officers surreptitiously installed the GPS device on the underbody of the jeep, they physically occupied the defendant's property. (*Id.*, at 949-950.) However, a physical trespass on a suspect's property does not qualify as a Fourth Amendment search unless it is conducted to obtain information or discover evidence. (*Ibid*.) In the current case, the officers trespassed on the defendant's private property and then used the installed GPS device to monitor the defendant's movements while he was driving the vehicle. *The installation combined with the use constituted a search*. (*Id.*, at 949.)

3. A Tiny Constable in a Gigantic Coach

In the majority opinion's most-quoted passage, Justice Scalia proposed an 18th Century analog. Scalia stated that the officers' installation and use of the GPS device in the current case was analogous to "a constable's concealing himself in the target's coach in order to track its movements. There is no doubt that the information gained by that trespassory activity would be the product of the unlawful search – whether that information consisted of the conversations occurring in the coach, or the destinations to which the coach traveled." (*Jones, supra*, at 950, fn. 3.) Justice Alito noted that this hypothetical scenario "would have required either a gigantic coach, a very tiny constable, or both - not to mention a constable with incredible fortitude and patience." (*Id*., at 958, fn. 3. [conc. opn. of Alito, J.])

---

on the phone inside was a Fourth Amendment search; the government's actions violated the defendant's expectation of privacy that he reasonably relied upon when using the phone inside the booth. A warrant based on probable cause was required to authorize the government's installation and use of the device. It didn't matter that there was no physical entry into the area occupied by the defendant. (*Katz, supra,* at 348-58.)

4. The Majority Distinguished the Supreme Court's Prior Beeper Cases, Because the Government Had Not Invaded the Defendants' Property When They Placed the Beepers in Containers of Chemicals.

Justice Scalia rejected the government's contention that the Supreme Court's prior beeper cases - *United States v. Knotts* (1983) 460 U.S. 276 and *United States v. Karo* (1984) 468 U.S. 705 - governed this case and foreclosed "the conclusion that what occurred her constituted a search." (*Jones, supra*, 132 S.Ct., at 951-52.) Scalia stressed that in each of those cases, the officers did not commit a trespass when they concealed the beeper into a container of chemicals, with the container owner's consent and then transferred the container, with the beeper hidden inside to the defendant. (See *Knotts*, *supra*, 460 U.S. at 277-79; *Karo, supra*, 468 U.S. at 707, 712 [neither the original installation of the beeper into the container nor the transfer of the container to the defendant violated the defendant's reasonable expectation of privacy, as the beeper was not conveying any information at the time of the transfer].)[8] Justice Scalia concluded that "Jones, who possessed the Jeep at the time the government trespassorily inserted the information-gathering device, is on much different footing." (*Jones, supra*, at 952.)

Justice Scalia noted that in *Knotts*, *supra*, at 283, the Court had emphasized the government's limited use of the beeper signals to intermittently track the co-defendant's vehicle's movements on a single journey; *Knotts* had reserved the question of whether more extensive 24-hour surveillance, as made possible by GPS tracking, might constitute a Fourth Amendment search. (*Jones, supra*, at 952, fn. 6; see also *Id*., at 956 [conc. opn. of Sotomayor, J.].) **Although Scalia did not address whether the use of the GPS device to monitor Defendant Jones's movements 24 hours a day for four weeks constituted a search, he suggested that *Knotts* did not preclude a finding that it did.**

5. Scalia Declined to Determine if Prolonged Surveillance by Electronic Means, Without a Trespass, Would Violate the Suspect's Reasonable Expectation of Privacy and Constitute a Fourth Amendment Search.

Justice Scalia acknowledged that the trespass standard is not the exclusive test to determine whether a search had occurred. If officers relied on the transmission of electronic signals to obtain information *without committing an initial trespass*, their actions would be subject to the *Katz* analysis – i.e. whether they invaded the subject's reasonable expectation of privacy. (*Jones, supra*, at 953.)

---

[8] For a description of the facts of *Knotts* and *Karo*, and the Supreme Court's analyses in those cases, see footnotes 5 and 6 on page 5.

Justice Scalia conceded that achieving the long-term surveillance that occurred in this case through electronic means, without a trespass, "may be ... an unconstitutional invasion of privacy." (*Id.*, at 954.) However, he refused to determine the effect of new location-monitoring technology on society members' reasonable expectations of privacy.[9] The present case did not require the Court to answer this question, because the officers' installation of the GPS device was achieved by trespassing upon the defendant's property, and thus clearly constituted a search. (*Id*., at 950, 953-54.)

6. Scalia Declined to Determine Whether Officers Need to Obtain a Warrant Based on Probable Cause Before Attaching a GPS Device to the Subject's Vehicle to Use For Surveillance

Justice Scalia declined to determine whether a GPS search requires a warrant, whether the search must be justified by reasonable suspicion or probable cause, and whether the search in this case was justified by probable cause. The government had argued that even if the officers' actions qualified as a search, it was reasonable because the officers had "reasonable suspicion, and indeed probable cause," that the defendant was a leader of a large-scale drug distribution conspiracy. Scalia noted that this argument had not been raised in the district court and was therefore forfeited. (*Id*., at 954.)[10]

---

[9] Justice Scalia's reluctance was surprising given statements he made in the majority opinion in *Kyllo v. United States* (2001) 533 U.S. 27, acknowledging the effects of evolving technology on privacy. In *Kyllo*, the Court held that law enforcement's use of a thermal-imaging device to detect the amount of heat emanating from the surface of the defendant's residence intruded upon his reasonable expectation of privacy in the interior of his home. Thus, applying the *Katz* test, it was a search requiring a warrant. It did not matter that the officers using the device never actually entered the defendant's residence, but merely scanned the exterior surfaces while sitting in a car across the street. (*Kyllo, supra*, at 29-30, 34-35, 40.) **Justice Scalia stated: "It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology." (*Id*., at 33-34.) Scalia also warned that the rule adopted in *Kyllo* "must take account of more sophisticated [technological] systems that are already in use or development."** (*Id.*, at 36.)

[10] In *Maynard*, while acknowledging that this argument was forfeited, the Circuit Court held that a warrant would be required and that the "automobile exception" would not authorize the installation of a GPS tracking device on a vehicle without the approval of a neutral magistrate. (*Maynard, supra*, 615 F.3d at 567.)

E. The Concurring Opinion Authored by Justice Alito (Joined by Justices Ginsberg, Breyer and Kagan)

Justice Alito's concurring opinion was firmly grounded in the 21st century and looked to the future, rather than back to the 18th Century, to consider the effects of new electronic surveillance technology on peoples' reasonable expectations of privacy: "This case requires us to apply the Fourth Amendment's prohibition of unreasonable searches and seizures to a 21st-century surveillance technique the use of a Global Positioning (GPS) device to monitor a vehicle's movements for an extended period of time." (*Jones, supra*, at 957 [conc. opn. of Alito, J.])

Whereas Justice Scalia focused on the officers' physical installation of the GPS device on the defendant's property, Justice Alito focused on the government's use of the device for four weeks of constant surveillance, formulating the question presented as : "[W]hether [the defendant's] reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove." (*Id.*, at 958.) Writing on behalf of four concurring justices, Alito concluded that the lengthy monitoring that occurred in this case impinged on the defendant's reasonable expectations of privacy and constituted a search under the Fourth Amendment. (*Id.*, at 964.)

1. The Appropriate Test to Determine Whether a Fourth Amendment Search Occurred Considers Whether the Conduct of the Officers Violated the Defendant's Reasonable Expectations of Privacy

Justice Alito devoted the bulk of his opinion to criticizing the majority's resurrection and application of the trespass test. (*Jones, supra*, at 957-962.) According the Alito, the traditional trespass test, which required a physical penetration into a person's property, had proved inadequate when the police were able to use electronic surveillance (e.g. wiretapping) to monitor a suspect's conversations without trespassing on private property. Alito contended that in 1967, the Court "finally did away with the old approach, holding that a trespass was not required for a Fourth Amendment violation." (*Id.*, at 959, citing *Katz v. United States, supra*, 389 U.S. at 347.) Pursuant to *Katz* and subsequent opinions, the appropriate test to determine whether the law enforcement officers' conduct constituted a search considers whether that conduct violated the subject's reasonable and legitimate expectations of privacy. (*Id.*, at 959-961.)

2. Justice Alito Criticized the Majority's Focus on the Physical Installation of the GPS Devise on the Vehicle, and its Failure to Consider Whether the Use of the Device for Long-Term Surveillance Constituted a Search

Justice Alito contended that the majority's focus on trespass disregarded the more important government conduct in this case - the use of GPS for the purpose of long-term location tracking - and accorded too much significance to the relatively minor act of physically installing the small device on the subject's car. (*Id*., at 961) This approach improperly ignored the extensive surveillance made possible by modern technology.

Justice Alito noted that officers could monitor a driver's movements, *without committing a technical trespass*, by relying on GPS location tracking devices that are installed in vehicles by manufacturers prior to purchase, including disabled vehicle and stolen car detection systems. (*Id.*, at 961-62). Moreover, "recent years have seen the emergence of many new devices that permit the monitoring of a person's movements" without trespass or consent: video monitoring of traffic (including cameras installed at automatic toll collection booths), as well as cell phones and other wireless devices that permit service providers to track the location of users. (*Id.*, at 963) Would police use of these other devices qualify as a search?

3. Justice Alito Held That The Use of the Installed GPS Device to Monitor the Defendant's Movements in the Vehicle for Four Weeks Violated His Reasonable Expectations of Privacy

Justice Alito noted that not so long ago, the surveillance at issue in this case - the constant monitoring of a vehicle's location for four weeks - would have required several officers, multiple vehicles and possibly aerial assistance. It would have been difficult, prohibitively expensive and impractical.[11] However, recent advances in technology, including GPS devices, make such long-term monitoring relatively easy and cheap. (*Id.*, at 963-64.) This affects society members' reasonable expectations of privacy; a reasonable person would not expect law enforcement officers to secretly monitor and catalogue every movement of his car for a very long time.

Thus, while short-term monitoring of a person's movements on public streets

---

[11] Alito emphasized that the beepers used in *Knotts* and *Karo*, did not permit the constant long-term surveillance made possible by GPS. Those beepers merely emitted periodic signals that could be picked up by a radio receiver. The signals had a limited range and could be lost if police did not stay close enough. (*Jones, supra*, at 963, fn. 10.)

accords with expectations of privacy that our society recognizes as reasonable, "the use of longer term GPS monitoring in investigations of most offenses impinges on [reasonable] expectations of privacy." (*Id.*, at 964) In the current case, officers tracked every movement the defendant made in the jeep for four weeks. Justice Alito declined to "identify with precision the point at which the tracking of the vehicle became a search, for the line was surely crossed before the 4-week mark." Thus, the monitoring that occurred *in this case* constituted a Fourth Amendment search. (*Ibid*.)

4. Society Members' Reasonable Expectations of Privacy May Change With the Increased Use of New Electronic Location-Monitoring Technology

Justice Alito acknowledged that the *Katz* reasonable-expectation-of-privacy test rests on the assumption that the hypothetical reasonable person has a stable set of privacy expectations. And yet, dramatic technological change can change those expectations and lead to periods in which privacy concerns are in flux. The increasing availability and use of GPS devices and the emergence of other electronic devices that permit the monitoring of a person's movements will shape and possibly lessen the average person's expectations about the privacy of his or her daily movements. (*Id.*, at 962-63.) "New technology may provide increased convenience or security at the expense of privacy, and many people may find that tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable." (*Id.*, at 962; see also *United States v. Garcia* (7th Cir. 2007) 474 F.3d 994 ["There is a tradeoff between security and privacy, and often it favors security"].)

F. Justice Sotomayor's Concurring Opinion

Justice Sotomayor's opinion is the most important. Sotomayor joined Justice Scalia's majority opinion because she agreed that the officers' conduct in this case constituted a trespass for the purpose of obtaining information and thus constituted a Fourth Amendment search. However, she also agreed with Justice Alito's concurring opinion, joined by three other justices, that the use of the GPS device for long-term surveillance violated the subject's reasonable privacy expectations. (*Jones, supra*, at 954-55 [conc. opn. of Sotomayor, J.].) Thus, Sotomayor provided the crucial fifth vote for the holdings of both Scalia and Alito. "In light of Justice Sotomayor's apparent endorsement of Justice Alito's concurrence, *Jones* can be plausibly understood as having two separate majority opinions." (*United States v. Graham* (D. Maryland 2012) 846 F.Supp. 2d 384, 405, fn. 15.)

1. Justice Sotomayor Concluded That Either the Traditional Trespass Test or the More Modern Reasonable Expectation of Privacy Test May Be Applied to Determine if Law Enforcement Officers' Conduct Qualified as a Fourth Amendment Search. Under Both Tests, a Search Occurred in This Case

Justice Sotomayor agreed with the majority that a Fourth Amendment search occurs when the government obtains information by physically intruding on the defendant's property. That is what happened in this case when the government installed a GPS device on the defendant's jeep without a valid warrant or his consent, and then used that device to monitor the jeep's every movement for four weeks. (*Id*., at 954.) But Sotomayor insisted that the Fourth Amendment is not only concerned with trespassory intrusions on property. The reasonable-expectation-of-privacy test, set forth in *Katz*, "augmented, but did not displace or diminish, the common-law trespassory test that preceded it." (*Id*., at 955.) A Fourth Amendment search also occurs when government officials, without committing a trespass, violate an individual's reasonable expectation of privacy to obtain information. (*Ibid*.) In resolving this case, the Court did not need to consider the effects of the long-term surveillance on the defendant's privacy expectations because "the trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case." (*Ibid*.)

But Justice Sotomayor also agreed with Justice Alito's observation that many forms of surveillance, including GPS monitoring, may occur without a physical intrusion into the subject's property. With increasing regularity, officers will be capable of duplicating the monitoring that occurred in this case by using factory-or-owner installed vehicle tracking devices or GPS-enabled smartphones. In these situations, "the majority opinion's trespassory test may provide little guidance." Sotomayor agreed that longer term GPS monitoring impinges on reasonable expectations of privacy. (*Id.*, at 955.)

2. Justice Sotomayor Explained How the Unique Attributes of GPS Surveillance Violate A Person's Reasonable Expectations of Privacy

Justice Sotomayor explained how in cases involving *both long-term and short-term monitoring*, the unique attributes of GPS surveillance intrude on the subject's privacy expectations in his or her associations, habits and activities :

> **" GPS monitoring generates a precise, comprehensive record of a person's public movements that reflect a wealth of detail about her familial, political, professional, religious and sexual associations. 'Disclosed in [GPS] data ... will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on'." (*Jones, supra*, at 955, quoting *People v. Weaver* (2009) 12 N.Y. 3d 433, 441-42 [909 N.E.2d 1195, 1199].)**

Moreover, Sotomayor emphasized that GPS monitoring not only gives the government access to all this private information. They can store such records and effectively mine them for information years into the future. (*Id.*, at 955-56.)

In considering the existence of a reasonable expectation of privacy in the sum of one's public movements, Justice Sotomayor asked "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more at less at will, their political and religious beliefs, sexual habits, and so on." (*Id.*, at 956.) The answer is plainly no.[12]

It makes no difference that law enforcement officers can access this location information without attaching a GPS device to the subject's vehicle. Sotomayor opined that "[o]wners of GPS-equipped cars and smartphones do not contemplate that these devices will be used to enable covert surveillance of the movements." (*Id*., at 956, fn *.) And if they do so, "[a]wareness that the government may be watching chills associational and expressive freedoms." (*Id*., at 956.) Finally, Justice Sotomayor warned that GPS surveillance is amenable to police abuse, particularly if there is no oversight by the legislature or the courts. (*Ibid*.)

---

[12] Justice Sotomayor's analysis mirrors the reasoning of the D.C. Circuit in *United States v. Maynard*, the opinion affirmed in *Jones*. In *Maynard*, the Court held that the whole of the defendant's movements on public streets were more revealing than the parts. Prolonged continual surveillance reveals the pattern of one's movements and private information not exposed by a single journey. (*Maynard, supra*, 615 F.3d at 560-63.)

3. Justice Sotomayor Considered the Effects of Evolving Technology on Society Members' Reasonable Expectations of Privacy and Questioned the Continued Validity of the Third Party Doctrine

Like Justice Alito, Justice Sotomayor considered the effects of evolving technology on privacy interests. However, she did not agree with Alito that some people would necessarily find the tradeoff of privacy for convenience worthwhile or come to accept the diminution of privacy as inevitable. (*Jones, supra*, at 957.)

Most importantly, Sotomayor proposed that in this digital age, it may be necessary to reconsider the premise, supported by Supreme Court precedent, that an individual has no reasonable expectation of privacy in information that he or she voluntarily discloses to third parties - data that could end up in government hands. (*Id.*, at 957, citing *Smith v. Maryland* (1979) 442 U.S. 735, 742; *United States v. Miller* (1976) 425 U.S. 435, 443.) After all, people reveal a great deal of information about themselves to third parties (e.g. cell phone and internet service providers) whenever they punch in a number on their cell phone, send a text, or visit a web site. Justice Sotomayor questioned whether "people would accept without complaint the warrantless disclosure to the government of a list of every web site they had visited in the last week, or month, or year." (*Id.*, at 957.)

II. QUESTIONS LEFT UNANSWERED BY *JONES*

If you have a case on "all fours" with *Jones*, in which the officers surreptitiously installed a GPS device on the defendant's vehicle and then used that device to monitor his or her movements while driving the vehicle for at least two to four weeks, you can argue that the officers conducted a search within the meaning of the Fourth Amendment. But you will also need to argue and convince the court that this search required a warrant based on probable cause. However, if the facts of your client's case differ from this scenario, the constitutional significance of those differences will need to be litigated.

Here are some of the questions that are not answered by the opinions in *Jones*:

1. Law enforcement officers secretly install a GPS device on the defendant's vehicle and use it to monitor his or her movements in the vehicle for an extended period of time. Do the officers need probable cause to believe that this location monitoring will reveal incriminating evidence? Would reasonable suspicion be sufficient? Assuming the officers need probable cause, are they required to seek a warrant or would an exception to the warrant requirement (e.g. the automobile exception) apply?

The majority opinion, written by Justice Scalia, expressly declined to address these questions. (*Jones, supra*, at 954.) The concurring opinions did not discuss these issues.

2. Law Enforcement officers use GPS or another electronic tracking device to monitor the movements of the vehicle that the defendant drives without committing a trespass to place the device. For example, the officers access GPS data generated by the defendant's cell phone? Would the continual surveillance of the vehicle's movement violate the driver's reasonable expectation of privacy and qualify as a 4th Amendment search?

In the majority opinion, Justice Scalia relied on trespass theory, so he declined to decide whether the use of electronic means to continually monitor the subject's movements on public roads, accomplished without trespass, would constitute a search under the reasonable-expectation-of-privacy test. (*Jones, supra*, at 953-54.) In his concurring opinion, Justice Alito relied exclusively on the *Katz* test and concluded that the long-term GPS monitoring of the defendant's movements in a vehicle violated his reasonable expectation of privacy. The issue of whether officers had trespassed to install the device was irrelevant. (*Jones, supra*, at 963-64 [conc. opn. of Alito, J.].) In her concurring opinion, Justice Sotomayor agreed with Scalia that a search occurred in this case because the officers trespassed on the defendant's property, by surreptitiously installing the device on his vehicle and using it to gather information. But Sotomayor also held that if law enforcement officers, without committing a trespass, used GPS or other electronic means for long-term monitoring of the vehicle driver's movements, this would violate the subject's reasonable expectation of privacy. (*Id.*, at 954-56 [conc. opn. of Sotomayor, J.) Because of Sotomayor's concurrence, I would argue that there were five votes, in *Jones*, for the principle that the use of GPS, or another electronic location tracking device, to constantly monitor a subject's movements for an extended period constitutes a search, irregardless of whether installation of the device is accomplished by trespass. However, the question still needs to be litigated.

3. What if the law enforcement officers use GPS or another electronic tracking device to continually monitor the vehicle driver's movements for less than four weeks? How many days or weeks of surveillance are sufficient to invade the driver's reasonable expectation of privacy?

For Justice Alito, the fact that the officers monitored Jones' movements as the driver of the vehicle for four weeks was dispositive. Alito noted that relatively short-term monitoring of a person's movements on public streets accords with reasonable expectations of privacy, but longer term monitoring does not. Alito declined to determine precisely when the tracking becomes a search, although he believed the line was clearly

crossed before the four-week mark. (*Jones, supra*, at 964 [conc. opn. of Alito, J.].)

Justice Sotomayor seemed less concerned with the fact that the surveillance lasted an entire month. In explaining how pervasive location-monitoring collects cumulative information about the subject's private associations and activities, she noted that "[i]n cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention." (*Jones, supra*, at 955 [conc. opn. of Sotomayor, J.].)

Justice Scalia authored the majority opinion, and his analysis of why the GPS installation and monitoring in Defendant Jones' case constituted a search does not depend on the length of the surveillance. According to Justice Scalia, the search occurred when the officers surreptitiously installed the GPS device on the defendant's vehicle and used that device to gather information. (*Jones, supra*, at 949-950.) Presumably, a search would occur if officer's trespassed to install the device and used it for one of two days.

Consequently, after *Jones*, in a case where you have a trespass, the length of the surveillance may not matter. However, if the GPS device was installed on the vehicle without a trespass or if location monitoring was otherwise achieved, you will have to persuade the court that monitoring was sufficiently long to invade the defendant's reasonable expectation of privacy.

4. Assuming that a GPS device was surreptitiously installed on a vehicle and then used to monitor the vehicle's movements for several weeks, would it matter if the defendant was not the owner or the exclusive driver of the vehicle?

It could make a difference in assessing whether the defendant's property rights or reasonable expectation of privacy had been violated.

*****

The answers to these questions will be addressed in future cases, but as discussed in the next sections of these materials, those answers may be slow in coming unless the GPS search was conducted after *Jones* was decided. In his concurring opinion, Justice Alito suggested that the regulation of law enforcement's use of GPS tracking devices and other new digital devices might better be handled by Congress and state legislatures. "[C]oncern about new intrusions on privacy may spur the enactment of legislation to protect against these intrusions. This is what ultimately happened with respect to wiretapping" after the *Katz* decision. (*Jones, supra*, at 962-64.) To date, however, neither the federal Congress nor the California Legislature has acted.

III. POST-*JONES* CASES

Since *Jones* was decided on January 23, 2012, 614 opinions from various state and federal courts have cited or discussed the Supreme Court case. Admittedly, in preparing these materials, I reviewed only California appellate decisions (published and unpublished),opinions from the federal circuit courts and a few federal district court opinions. Some post-*Jones* cases have applied the trespass test, resurrected by Justice Scalia in the majority opinion, to conclude that a search did or did not occur in an entirely different factual context.[13] However, I focused on cases addressing the effects of officers' installation and use of GPS devices and other electronic tracking technology on society members' reasonable expectations of privacy.

As discussed above, the majority in *Jones* did not decide: 1) whether a warrant is required before secretly attaching a GPS device to a vehicle and using it for location monitoring; 2) the quantum of suspicion required for a GPS search, regardless of the need for a warrant; or 3) whether GPS monitoring, conducted without a trespass, would violate the subject's reasonable expectation of privacy and qualify as a search? (See *Jones, supra*, 132 S.Ct. at 953-54.) Unfortunately, few cases have addressed these unanswered questions. Most courts have avoided that analysis by invoking the good faith exception to the exclusionary rule if the GPS search was conducted before *Jones* was decided**.**

Practice note: If you have a case involving a GPS search and you want to argue that the officers' actions were unconstitutional as they lacked a warrant based on probable cause, you will not likely persuade the appellate court to address this issue unless the search occurred after January 23, 2012.

---

[13] The most notable is the Supreme Court's decision in *Florida v. Jardines* (2013) 133 S.Ct. 1409, decided 14 months after *Jones*. Once again, Justice Scalia wrote the majority opinion on behalf of five justices, and once again, he relied on trespass theory. The Court held that the police trespassed on the defendant's property when they brought a trained drug-sniffing dog onto the front porch (the curtilage) of his home to detect whether drug odors were emanating from the residence. This was an unlicensed physical intrusion into a constitutionally protected area, intimately associated with the home, for the purpose of gathering evidence. (*Jardines, supra*, at 1413-17.) Justice Scalia reiterated that "the *Katz* reasonable-expectation test had been added to, not substituted for, the traditional property-based understanding of the Fourth Amendment." (*Id.*, at 1417.)

A. IF THE GPS SEARCH IN YOUR CASE OCCURRED PRIOR TO JANUARY 23, 2012: A Warrantless Pre-*Jones* GPS Search May be Unconstitutional Under *Jones*, but Incriminating Evidence Discovered Following That Search Will Not be Suppressed

1. Pre-*Jones* Searches: Federal Circuit Court of Appeals Cases

After *Jones* was decided in January 2012, the first cases that reached the federal appellate courts involved GPS installation and use conducted prior to that date and had facts were similar to those in Jones: Without obtaining a warrant, law enforcement officers surreptitiously attached a GPS device to the underside of the defendant's vehicle and monitored the vehicle's movements for an extended period of time. (See, e.g. *United States v. Sparks* (1st Cir. 2013) 711 F.3d 58, 60-61 [11 days of GPS location monitoring]; *United States v. Baez* (1st Cir. 2014) 744 F.3d 30, 31-32 [347 days]; *United States v. Aguiar* (2d Cir. 2013) 737 F.3d 251, 255 [six months]; *United States v. Stephens* (4th Cir. 2014) 764 F.3d 327, 339 [two months]). Because *Jones* applied retroactively to GPS installation and monitoring conducted before January 23, 2012, the officers in these cases conducted Fourth Amendment searches. The defendants either assumed that a warrant and probable cause were required for the GPS search, or expressly argued this position. (See, e.g. *Sparks, supra*, at 60, 62 [this case presented the issue of whether a warrant is required for a GPS search; *Baez, supra*, at 35 [presented the question of whether the government agents needed a warrant *and* either probable cause or reasonable suspicion to install a GPS device and track the defendant's car].)

The circuit courts declined to answer this and other unresolved questions, because even if the pre-*Jones* GPS searches were unconstitutional, incriminating evidence discovered during or as a result of the location monitoring would not be suppressed. Relying on the Supreme Court's decision in *Davis v. United States* (2011) 131 S.Ct. 2419; the courts invoked the good faith exception to the exclusionary rule; at the time of the search, the officers relied on binding appellate precedent which authorized the officers to attach a GPS device to a vehicle, without a warrant, and to and monitor the vehicle's movements on public roadways without implicating the Fourth Amendment.[14] (See, e.g.

---

[14] In *Davis v. United States*, the Supreme Court expanded the good-faith exception to the exclusionary rule. The seven-justice majority held that when law enforcement officers conducted a search in objectively reasonable reliance on binding appellant precedent, in effect at the time of the search, the exclusionary rule does not apply even though the search is unconstitutional pursuant to a subsequent Supreme Court decision. (*Davis, supra*, 131 S. Ct. at 2423-24 [Even if the vehicle search incident to arrest was unconstitutional under the rules subsequently set forth in *Arizona v. Gant* (2009) 129

Sparks, supra, at 62-63; *Aguiar, supra*, at 261.)

In holding that the officers in these cases had acted in reasonable reliance on binding appellate precedent, some courts cited prior decisions from their own Circuit Court of Appeals. (See, e.g. *United States v. Pineda-Moreno* (9th Cir. 2012) 688 F.3d 1087, 1090 [relying on prior Ninth Circuit cases holding that neither the installation of an electronic device on the car, nor the use of that device to track the car's movements on public roads were searches].)[15] Other courts, having no on-point circuit authority, relied on *United States v. Knotts, supra*, 460 U.S. at 276 and *United States v. Karo, supra*, 468 U.S. 705, the Supreme Court's beeper cases from the 1980's. (See, e.g. *Sparks, supra*, 711 F.3d at 65-67 [1st Circuit]; *Aguiar, supra*, 737 F.3d at 261-62 [2nd Circuit]; *Stephens, supra*, 764 F. 3d at 337-38 [4th Circuit]; *United States v. Katzin* (3rd Cir. 2014) 769 F.3d 163 [divided 8-5 en banc opinion holding that in the absence of on-point Third Circuit authority, the officers who did not obtain a warrant before attaching a GPS device to the defendant's vehicle and using it for location monitoring reasonably relied on *Knotts* and *Karo*, as well as the weight of authority from other federal circuits].) [16]

The dissenting opinion in *United States v. Stephens* is worth reading. Judge Thacker found that the law enforcement officers in that case had not acted with an objectively reasonable belief that their conduct was lawful. (*Stephens, supra*, 764 F.3d at

---

S.Ct. 1710, evidence discovered during that search would not be suppressed because the officers reasonably relied on binding Eleventh Circuit preceden, which then in effect that authorized the officers' search of the car's passenger compartment following the arrest of a recent occupant in every case].)In her concurring opinion, Justice Sotomayor emphasized that the officer who conducted the search needed to rely on unequivocal settled binding precedent that specifically authorized the particular police practice. *(Davis, supra, at 2434*-35 [conc. opn. of Sotomayor J.].)

[15] The 2012 opinion in *Pineda-Moreno* was a reconsideration of the Ninth Circuit's prior opinion in the same case (*United States v. Pineda-Moreno* (9th Cir. 2010) 591 F.3d 121), after the Supreme Court had granted certiorari, vacated judgment and remanded for reconsideration under *Jones*.

[16] Unlike the Supreme Court in *Jones*, the federal circuit courts, in these opinions, declined to address important distinctions between the facts of their cases and the facts of *Knotts* – e.g. that the GPS devices, unlike the beeper in *Knotts,* were installed without trespass, and that GPS devices, unlike beepers, permit 24-hour location monitoring for months without the need for officers' visual surveillance. (See, e.g *Sparks, supra*, at 66-67; *Baez, supra*, at 33-35)

345 [dis. opn. of Thacker, J.].) He emphasized that no binding appellate precedent – from the Fourth Circuit or the United States Supreme Court - authorized the officers to attach a GPS device to the underside of the defendant's vehicle and track his movements for two months. (*Stephens, supra*, at 339-342.) Specifically, the majority's reliance on *Knotts* as binding precedent was misplaced because of differences in the facts and distinctions between the more primative beepers and GPS. (*Id.*, at 341-43.) **Finally, Judge Thacker reasoned that if precedent was unsettled, officers should seek a warrant. In "this era of fast-moving technological advancements and our ever-shrinking zone of privacy, ... [t]he Government must err on the side of the Constitution and obtain a warrant, especially as 'the disturbing specter of [G]overnment agents hiding electronic devices in all sorts of personal property and then following private citizens who own such property ...' becomes ever more possible." (*Id.*, at 346, citing *United States v. Jones* (4th Cir. 1994) 31 F.3d 1304, 1311.)** Many of these same points were made by Judge Greenaway, writing on behalf of the five dissenting justices in the en banc option in *United States v. Katzin, supra*, 769 F.3d at 188-193 [dis. opn. of Greenaway, J.]

2. Pre-*Jones* Searches: California Court of Appeal Cases

In a series of unpublished opinions, involving GPS searches conducted prior to January 23, 2012, California appellate courts, like the federal courts, declined to decide whether surreptitious installation and use of the GPS device requires a warrant and probable cause. There was no point determining this issue, because any evidence resulting from GPS location monitoring would not be suppressed under the *Davis* good faith exception to the exclusionary rule; the officers reasonably relied on then-binding appellate precedent holding that the installation and use of the electronic monitoring device was not a search. (See, e.g., *People v. Eason* (March 12, 2013) 2013 WL 523362 [3rd Dist.]; *People v. Castro* (March 29, 2013) 2013 WL 1277063 [1st Dist., Div. 1]; *People v. Royal* (July 18, 2013) 2013 WL 3777147 [2d Dist.]; *People v. Alejandre* (September 5, 2013) 2013 WL 4761059 [1st Dist., Div 3]; *People v. Mackabee* (June 20, 2014) 2014 WL 2803595 [2d Dist., Div. 4].)

According to these unpublished appellate decisions, the binding precedent in effect in California prior to January 2012, was *People v. Zichwic* (2001) 94 Cal. App. 4th 944 [6th Dist.]. In *Zichwic*, the Sixth District held that the officers' installation of the electronic device, a beeper, on the defendant's truck and their use of it to monitor his movements on public streets for one hour did not constitute a Fourth Amendment search. The court focused on the installation of the device. First, the court ruled that even assuming that attaching an electronic tracking device to the undercarriage of the truck constituted a search, it was authorized by the defendant's parole search condition. (*Id.*, at 951-53.) But the court did not stop there; it stated, "If the defendant was not subject to a parole search condition, we would conclude .... that installing an electronic tracking

device on the undercarriage of the defendant's truck did not amount to a search within the meaning of the Fourth Amendment." (*Id.*, at 953.) Agreeing with *United States v. McIver* (9th Cir. 1999) 186 F.3d 1119, 1127, the Sixth District concluded that an individual has no reasonable expectation of privacy in his car's exterior, including the undercarriage of the vehicle, which is regularly exposed to public view. (*Zichwic, supra*, at 955-56.) Turning briefly to the question of whether the monitoring of signals from the tracking device constituted a search, the court relied on *Knotts*, reasoning that the beeper monitoring in this case revealed only the movements of the defendant's vehicle on public streets – information in which the subject had no reasonable expectation of privacy(*Ibid*.)

The California appellate decisions rejected various defense contentions as to why *Zichwic* was not binding precedent in our state prior to the *Jones* decision. For example, the courts rejected all claims that the Sixth District's statement that that GPS installation and use did not qualify as a search was dicta, since the actual holding was that any search was justified by Defendant Zichwic's parole search condition. The courts held that this discussion was not dicta, but an alternative holding.

Practice Note: One might be able to successfully argue that *Zichwic* was not binding authority if the police officer used a GPS device to constantly monitor the defendant's movements in his vehicle for a month or more. However, this fact was not present in any of these California Court of Appeal cases.

B. California Appellate Cases Involving Post-*Jones* GPS Searches

Eventually, the California Court of Appeal will review cases in which the officers installed a GPS device on a vehicle and used it for location monitoring after January 23, 2012 (the date *Jones* was decided). In those cases, the law enforcement officers' actions will no longer be covered by the good faith exception to the exclusionary rule, and the courts will need to address the questions left unanswered by *Jones* - i.e. is a warrant based on probable cause required for a GPS search?

1. *People v Glass* (May 27, 2014) 2014 WL 2194502 [Fourth Dist., Div. 1]: The Court Declined to Decide if a GPS Search Conducted After *Jones* Required a Warrant, Because Co-Defendant Wellnitz's Probation Search Condition Permitted the Warrantless Search of the Shared Truck

According to my research, *Glass* is the first California case considering the constitutionality of a GPS search conducted after *Jones*. Unfortunately, the court's unpublished opinion does not address any of the issues left unresolved by the Supreme

Court. In this case, officers suspected that Co-defendant Wellnitz was involved in copper thefts. After verifying that Wellnitz was on probation with a search condition, officers attached a GPS device to his truck in December 2012. They used this device to monitor the truck's movements for three weeks. The GPS device informed the officers when and where the vehicle was moving, but visual surveillance was necessary to ascertain the identity of the driver. During that period, the truck was driven by both Wellnitz and Co-defendant Glass; sometimes they shared the driving and other times, Wellnitz or Glass drove alone. Location information derived from the GPS monitoring revealed incriminating evidence which led to the arrest of both men. (*Glass, supra*, at *1-*2.) Only Co-defendant Glass appealed, claiming the evidence against him was obtained from an unconstitutional warrantless GPS search.

The appellate court acknowledged that "under *Jones*, placing the GPS device on Wellnitz's truck and using the device to monitor the movements of Wellnitz's truck on public thoroughfares [was] a 'search' within the meaning of the Fourth Amendment." (*Glass, supra*, at *4.) However, the court did not decide whether a warrant had been required to install the device on the vehicle for the following reasons: 1) Wellnitz had consented to the warrantless search by accepting a probation search condition. (*Glass, supra*, *4.) 2) Neither the installation of the GPS device on the truck, nor the location monitoring, involved a trespassory invasion of Glass's rights; thus Glass had to prove that the incriminating evidence was the product of a warrantless search that transgressed his own reasonable expectations of privacy. However, this evidence was derived solely from monitoring the truck's movements when Wellnitz was present and had common authority over the truck; Glass was then subject to the consent derived from Wellnitz's probation search condition. (*Glass, supra*, at *5.) The outcome might have been different if Glass had sought to suppress any evidence produced by monitoring the truck when Glass was the sole driver and occupant. (*Glass, supra*, at *5, fn. 2.)

C. Is a Warrant Based on Probable Cause Required for a GPS Search?[17]

1. Three Federal Circuit Cases Assume a Warrant is Required

As discussed above, post-*Jones* cases evaluating pre-*Jones* GPS searches avoided answering this question by invoking the *Davis* good faith exception to the exclusionary

[17] At least four states (Hawaii, New York, Washington and Oregon) require police to obtain a warrant in order to track a person's movements using GPS or another electronic tracking device.

rule. Nevertheless, the federal circuit courts in two of those cases assumed without deciding that officers need a warrant before conducting a GPS search. (See *Pineda-Moreno*, supra, 688 F.3d at 1090 [Ninth Circuit assumed that warrantless GPS searches were unreasonable under the Fourth Amendment after *Jones*]; *Stephens, supra*, 764 F.3d at 334 [Fourth Circuit accepted the district court's ruling that officer's warrantless installation and use of GPS was an unreasonable search].)

In *United States v. Gibson* (11th Cir. 2013) 708 F.3d 1256, a case addressing whether the defendant had standing to challenge the installation and use of a GPS device on a car he regularly borrowed (discussed below), both the majority and the dissent assumed that officers need a warrant before conducting a GPS search. (*Id*,, at 1276, 1278; *Id.*, at 1285 [dis. opn. of Kravitch, J.].)

2. *United States v. Ortiz* (E.D. Pennsylvania 2012) 878 F.Supp.2d 515: A warrant based on probable cause is required before law enforcement officers can install a GPS device on a person's vehicle and use GPS for location monitoring.[18]

United States v. Ortiz, decided six months after *Jones*, that was willing to directly address some of the unresolved questions, even though the GPS installation and monitoring had occurred prior to *Jones*. After ruling that probable cause (not reasonable suspicion) and a warrant were required for a GPS search, the district court held that the *Davis* good faith exception to the exclusionary rule did not preclude suppression of the evidence obtained from the warrantless GPS search, as no binding appellant precedent specifically authorized law enforcement officers' actions in this jurisdiction.[19] (*Ortiz,*

---

[18] Because *Ortiz* is the only case to date to thoroughly analyze this issue, I will summarize the district court's reasoning in the 30-page opinion. Obviously, a federal district court decision from Pennsylvania is not binding, or even particularly persuasive, authority in California. However, we can rely on its reasoning when arguing that a warrant based on probable cause is required for a GPS search.

[19] The Pennsylvania district court is within the Third Circuit. Prior to *Jones*, the Third Circuit had not ruled on the constitutionality of GPS tracking, although other circuits that considered the issue had determined that the installation and use of a GPS tracker was not a Fourth Amendment search. The district court held that the Supreme Court's beeper cases *(Knotts* and *Karo*) did not qualify as binding appellate authority, because these cases did not specifically authorize the installation of a GPS tracker (as opposed to a less sophisticated beeper) on a subject's car, accomplished by trespass. (*Ortiz, supra*, at 537-541.)

supra, 878 F.Supp. 2d at 518.)

DEA agents suspected that Defendant Ortiz and others were involved in a massive drug trafficking operation. The agents placed two successive GPS tracking devices on the undercarriage of the defendant's pick-up truck and monitored the truck's movements for about six weeks. Data from the second GPS tracker led to the discovery of inculpatory evidence. Prior to his trial on drug trafficking charges, the defendant moved to suppress that evidence. The district court granted the motion. (*Ortiz, supra*, at 517-525.)

First, the court rejected the government's assertion that requiring a warrant and probable cause before installing a GPS device would impede the state's ability to investigate drug trafficking and terrorism. The district court weighed the individual privacy interests against the government interest and concluded that there was no reason to dispense with the warrant and probable cause requirements. The installation of the GPS tracker is a trespass on personal property. Moreover, GPS trackers gather much more data than beepers; obtaining information regarding a vehicle's whereabouts 24 hours a day for approximately a month is a significant invasion on privacy. The government asserted no "special need" beyond the normal need for law enforcement, as is usually required to search without a warrant and probable cause. (*Ortiz, supra*, at 527-533.)

Second, the district court rejected the government's argument that the "automobile exception" to the warrant requirement should apply to a GPS search and excuse the need for a warrant. This exception, based on the mobility of vehicles, applies when the officers have probable cause to believe that a vehicle contains contraband. The government asked the district court to expand the exception to permit GPS tracking of a vehicle without a warrant when officers have probable cause to believe that the vehicle is being used in the furtherance of criminal activity. The district court declined the government's request. The court noted that in this case, as in most cases involving the use of GPS monitoring, no exigency tied to the vehicle's mobility (e.g. fear of destruction or concealment of evidence) justified officers' failure to seek a warrant. (*Ortiz, supra*, at 534-38.)

Practice Note: If you have a case where the GPS installation and tracking was conducted post-*Jones*, and you want to argue that a warrant based on probable cause, you might want to rely on recent Supreme Court cases acknowledging that technological developments have enabled police officers to secure warrants from magistrates more quickly. Federal magistrates are permitted to issue a warrant based on sworn testimony communicated by telephone or other reliable electronic means, such as e-mail and video conferencing. (See *Missouri v. McNeely* (2013) 133 S.Ct. 1552, 1562; see also *Riley v. California* (2014) 134 S.Ct. 2473, 2493.)

D. Who Has Standing to Challenge the Installation and/or Use of a GPS Tracking Device?

1. *United States v. Gibson* (11th Cir. 2013) 708 F.3d 1256. THE DEFENDANT IS THE USER OF THE VEHICLE, NOT THE OWNER. The Defendant, the Regular User of a Vehicle Registered to Another, Lacked Standing to Challenge the Use of the Tracking Device When he Was Not in the Vehicle as the Driver or Passenger

In 2009, DEA agents installed a GPS tracking device on the undercarriage of a vehicle when it was parked in Defendant Gibson's driveway, because they suspected that Gibson used the vehicle for drug trafficking. The agents knew Gibson was a regular driver of the vehicle, although the registered owner was Burton. Over three days the agents tracked Gibson's movements in the vehicle as he took a suspicious short trip to a known source city for narcotics. Acting on a DEA request, local deputy sheriffs stopped the vehicle after noticing that the driver had committed two traffic violations. Burton, the vehicle owner, was driving at this time and Gibson was not present in the vehicle. Burton consented to a search of the vehicle and two kilograms of cocaine where found inside. Burton and Gibson were prosecuted for drug trafficking and Gibson moved to suppress the evidence discovered in the vehicle, as a result of the GPS monitoring. The district court denied the suppression motion, finding that Gibson lacked standing to challenge the installation or use of the GPS device. Gibson appealed. (*Gibson, supra*, at 1260-63.)

The Eleventh Circuit re-affirmed that an individual who borrows a vehicle with the owner's consent has a legitimate expectation of privacy in the vehicle and standing to challenge its search while it is in his possession. (*Gibson, supra*, at 1276-77.) Because Gibson qualified as a borrower of the vehicle, he had standing to challenge the installation of the GPS device and its use to track the vehicle's movements *while he was driving*.[20] However, Gibson lacked standing to challenge the use of the tracking device to monitor the vehicle's movements when he was neither a driver nor a passenger, as was the case at the time of the vehicle stop and search. Thus, the court declined to exclude the incriminating drug evidence discovered during that search. (*Id*., at 1277-79.)

---

[20] It is interesting that the Eleventh Circuit did not apply the trespass test used by the majority in *Jones*, given that Defendant Gibson had property rights equivalent to Defendant Jones. (See *Jones, supra*, at 949, fn. 2 [Defendant Jones's wife was the registered owner of the jeep to which the GPS device was attached, but Jones was the exclusive driver].)

Judge Kravitch filed a dissent in *Gibson*. He concluded that Gibson was effectively a co-owner of the tracked vehicle with the right to exclude others. Thus, he had a reasonable expectation of privacy in the vehicle even when he was not occupying it. (*Gibson, supra*, at 1283-85 [dis. opn. of Kravitch, J.] Judge Kravitch also stated that after *Jones*, a warrant is required before installing and using the GPS device. (*Id*., at 1285.)

2. *United States v. Davis* (10th Cir. 2014) 750 F.3d 1186. THE DEFENDANT WAS NEITHER THE CAR'S OWNER NOR A REGULAR DRIVER, BUT A PASSENGER IN THE CAR: The Defendant was a passenger in a car stopped because of location information derived from a GPS device that had been installed on the vehicle driven by his co-defendant and owned by the co-defendant's girlfriend. The defendant lacked standing to challenge the stop of the car, his detention, and the search of the vehicle.

Police officers were investigating a series of armed robberies. They suspected the robbers were using a car owned by Co-Defendant Baker's girlfriend, so without seeking a warrant, they surreptitiously installed a GPS tracking device on that car. The next day, GPS coordinates from the device indicated that the car was located near the scene of a robbery that had just occurred. Based on this information, combined with visual surveillance, the officers stopped the car. Baker was driving and Defendant Davis was the passenger. Both men were arrested. Upon searching the car, the officers found evidence incriminating both Baker and Davis. Davis moved to suppress this evidence, asserting that the warrantless attachment and use of the GPS device to locate the car violated the Fourth Amendment. The district court denied the motion. (*Davis, supra*, at 1188-89.)

The Tenth Circuit held that Davis, a mere passenger in Baker's girlfriend's car at the time of the stop, lacked standing to challenge the warrantless GPS search which led to the discovery of incriminating evidence. Davis had no possessory interest or reasonable expectation of privacy in the car owned by Co-Defendant Baker's girlfirend. "Because Mr. Davis did not own or regularly drive the car to which the GPS device was attached, it appears he lacks a sufficient Fourth Amendment interest to challenge the derivative evidence." (*Davis, supra*, at 1190.)

3. *People v. Castro* (March 29, 2013) 2013 WL 1277063 [1st Dist., Div. 1]. THE DEFENDANTS WERE PASSENGERS IN TWO VEHICLES STOPPED BASED ON GPS LOCATION-TRACKING DATA: As passengers in the stopped vehicles, the defendants had standing to challenge the GPS search that provided reasonable suspicion to stop the cars and detain the occupants.

In this case, five co-defendants appealed their theft and robbery convictions and challenged the trial court's denial of their suppression motions. In 2010, police officers conducted visual surveillance of several co-defendants, confirming their suspicions that the co-defendants were involved in recent jewelry thefts. One of the vehicles occupied by the co-defendants was a silver Acura registered to Co-Defendant Castro; the officers believed that the Acura was the main vehicle used by the suspected thieves. Without obtaining a warrant, the officers attached a GPS device to the undercarriage of Castro's Acura. For the next 33 hours, the officers used the GPS device to track the Acura's movements as it was driven on Interstate 5. Officers physically following the Acura noticed that it was driving in tandem with a white Chrysler. The officers stopped the two vehicles and arrested the occupants (the co-defendants). Searches of both cars yielded evidence incriminating them in the robberies. (*Castro, supra*, at *1-*3.)

The Court of Appeal addressed the question of whether the co-defendants other than Castro (the registered owner of the Acura) had standing to challenge the warrantless installation of the GPS device on the Acura and its use to track the car's movements. Disagreeing with the reasoning of the Tenth Circuit in *United States v. Davis, supra*, Division One found that all the co-defendants had standing to raise this claim, as they were occupants of the two cars (the Acura and the Chrysler) at the time of the traffic stop.

Pursuant to *Brendlin v. California* (2007) 551 U.S. 249, all occupants of a car are detained during a traffic stop and thus have standing to challenge the constitutionality of the stop, arguing that the officers lacked reasonable suspicion. The occupants could challenge antecedent actions by the police that were pertinent the determination of whether the traffic stop was reasonable. In this case, the installation and use of the GPS device to monitor the Acura's movements "were the means essential to locating and detaining the Acura, the Chrysler, and the occupants (drivers and passengers) of both vehicles." The co-defendants had standing to challenge that search, as the GPS location data was instrumental in their detention. (*Castro, supra*, at *8-*10.)[21]

---

[21] As discussed above, *Castro* was one of the unpublished California appellate decision that invoked the good-faith exception to the exclusionary rule.

4. *People v. Barnes* (2013) 216 Cal. App. 4th 1508 [First 1st., Div. 2]. THE DEFENDANT POSSESSED A STOLEN CELL PHONE THAT WAS EQUIPPED WITH GPS;WITH THE OWNER'S CONSENT, THE SERVICE PROVIDER TRACKED THE LOCATION OF THE CELL PHONE: A person in possession of a stolen cell phone has no reasonable expectation of privacy in that phone and cannot argue that police use of location data generated by the phone constituted a Fourth Amendment search.

In November 2009, a man robbed two people and fled with one victim's cell phone. The victim told the responding officer that her cell phone was equipped with "GPS", and at the officer's suggestion, she asked Sprint to "ping" the phone to determine it's location. The Sprint employee pinged the phone about three times and determined its approximate location on Mission Street between 16th and 17th. This information was relayed to officers who went to that neighborhood. Two officers saw the defendant, a man meeting the victims' physical description of the robber, at 16th and Mission. They observed him get into a car and they followed, made a traffic stop, searched the car and found the cell phone and other stolen property. The Court of Appeal affirmed the trial court's denial of the motion to suppress evidence. (*Barnes, supra*, at 1510-12.)

As one of several arguments made in the trial court in support of the suppression motion, defense counsel had argued that use of the GPS technology to track the phone and the defendant's location violated his reasonable expectation of privacy. As the Court of Appeal acknowledged, this argument was not repeated on appeal. (*Barnes, supra*, at 1513, 1517.)[22] Nevertheless, Division Two went ahead and ruled that the use of GPS or another electronic-tracking method to locate the stolen cell phone did not constitute a Fourth Amendment search, because there was no trespass on the defendant's property interests and the "defendant did not have a legitimate expectation of privacy in the cell phone he had stolen." (*Id*., at 1518, citing *United States v. Caymen* (9th Cir. 2005) 404 F.3d 1196, 1200 [a person lacks a reasonable expectation of privacy in the contents of a laptop computer he fraudulently purchased].) The only person with a legitimate expectation of privacy in the cell phone and its contents was the victim who owned the phone, and she had asked Sprint to track the location of the phone and convey that information to the police. (*Ibid*.)

---

[22] On appeal, the defendant argued that the prosecution had not established the precise electronic method used to track the phone or its reliability in this particular case. Since reasonable suspicion was based only on the unreliable phone location data and the fact that the defendant matched a generic description of the robber, the defendant's detention was unconstitutional.

E. Does the *Jones* Ruling Apply to Other Electronic Surveillance Devices, Installed Without a Trespass

1. *United States v. Moore* (Sept. 15, 2014) 2014 WL 4639419 [Dist. Ct., S.D. Florida, Slip Opinion]: The use of surveillance cameras mounted on poles to videotape the outside areas of an apartment complex and individuals' activities in those areas for eight months did not constitute a Fourth Amendment search.

Without a warrant, but with the property owners' consent, government officials installed six surveillance video cameras – four on utility poles, one on an apartment building's roof, and one on the side of a business. These cameras were focused on the outside areas of an apartment complex known for drug dealing, firearm offenses and other violent crimes. For about eight months from June 2013 until February 2014, the cameras captured various people, including the defendant, engaged in illegal activities. There was video footage of the defendant conducting drug transactions and holding a firearm. The defendant did live in that apartment complex. The district court denied the defendant's motion to suppress the video recordings of his illicit activities as the products of an unconstitutional search. (*Moore, supra*, at *1-*2.)

Citing *Jones*, the district court noted that a search can occur when there is a physical trespass for the purpose of obtaining information or when an individual's reasonable expectation of privacy has been violated. No search occurred in this case under either test. Because the government obtained the property owners' permission before installing the surveillance cameras, there was no physical trespass. (*Moore, supra*, at *1.) Moreover, the government did not invade the defendant's reasonable expectation of privacy in his image and activities. When the cameras recorded the defendant, he was in areas accessible to the public and in plain view. Anybody watching the areas where the defendant conducted his illegal activities would have seen the same scenes and images captured by the cameras. (*Moore, supra*, at *2.) Relying on *Jones*, the defendant argued that the lengthy camera surveillance (eight months) violated his reasonable expectation of privacy. He asserted that "the information gathered over such a long period of time revealed more personal information than that which would be obtained for a shorter period", and also revealed "personal information that an isolated surveillance would not." (*Moore, supra*, at *3.) The district court rejected this argument The concurring justices in *Jones*, who found a violation of the defendant's reasonable expectation of privacy relied on "the detailed data obtained by tracking an individual's travels to many different locations over a period of time." In this case, the surveilling cameras focused on a particular area over time, not on any one individual. (*Ibid*.)

F. After *Jones*, Does the Government Need a Warrant Based on Probable Cause to Acquire Historical Cell Site Location Data from Cell Phone Service Providers to Determine a Suspect's Past Movements? [23]

1. *United States v. Graham* (D. Maryland 2012) 846 F.Supp. 384: Because cell phone subscribers do not have a legitimate expectation of privacy in historical cell site location records, maintained by their cell phone service providers, government officials did not violate the subscribers Fourth Amendment rights when they obtained this information from the service providers.

The defendants, Graham and Jordan, were suspects in two robberies. Cell phones were seized at the time of their arrest, one belonging to each defendant. During an on-going investigation, the defendants were suspected of having committed several additional robberies. Relying on provisions of the Stored Communications Act, 18 U.S.C.

---

[23] There are numerous federal cases discussing whether government officials violated the Fourth Amendment when they obtained phone records, specifically historical cell site location records, from cell phone service providers pursuant to the Stored Communications Act, 18 U.S.C. §§ 2701 et. seq.. A full discussion of these cases is outside the scope of these materials. In this section, I will discuss just two of those cases that considered the application of *Jones* to this question. I could not find any published federal court decisions, not subsequently vacated, requiring that government officials obtain a warrant based on probable cause to acquire *historical* cell-site location records. The Eleventh Circuit recently decided that the provision of the Stored Communications Act which allowed the government to obtain cell site location information without a warrant based on probable cause violated a defendant's Fourth Amendment rights. (*United States v. Davis* (11th Cir. 2014) 754 F.3d 1205.) However, this Eleventh Circuit opinion has been vacated pending rehearing en banc. (*United States v. Davis* (11th Cir. 2014) 573 Fed. Appx. 925.) As discussed below, a federal district court decision which would have required a warrant based on probable cause was vacated by the Fifth Circuit. (*See In re U.S. for Historical Cell Site Data* (S.D. Texas 2010) 747 F.Supp. 2d 827, subsequently vacated by *In re U.S. for Historical Cell Site Data* (5th Cir. 2013) 724 F.3d 600.) The Ninth Circuit has not yet ruled on this issue. Nevertheless, a growing number of states have ruled that police must obtain a search warrant to obtain historical cell site data. The states of Colorado, Maine, Minnesota, Montana and Utah passed statutes requiring law enforcement officers to secure a warrant in order to obtain this historic cell site data from service providers. The Supreme Courts of Massachusetts and New Jersey ruled that their respective state constitutions require a warrant to obtain this data. (*Commonwealth v. Augustine* (Mass. 2014) 4 N.E.3d 846; *State v. Earles* (N.J. 2013) 70 A.3d 630.)

§§ 2701 et. seq, government officials applied to federal magistrates for two court orders requiring the defendants' service provider, Sprint/Nextel, to disclose cell site location data for each cell phones during designated time periods. possibly linking them with these prior robberies. The magistrates issued orders requiring Sprint/Nextel to turn over the cell site location records upon making the requisite finding – that the government had offered specific and articulable facts showing a reasonable belief that the records sought were relevant to an ongoing criminal investigation. (This is a reasonable suspicion standard, less than probable cause.) Sprint/Nextel complied with this request and provided the data to the government. The first order required the release of records for 14 days, and the second order required records for 221 days. The cell site location data revealed the location of the cellular towers that received signals when the defendants' used their phones. This information helped law enforcement officers determine the defendants' locations during the relevant periods and implicated the defendants in various robberies. (*Graham, supra*, 846 F.Supp., at 385-87.)

The defendants filed a motion to suppress this evidence. They argued that the government's acquisition of this data *in this case* was a Fourth Amendment search requiring warrants supported by probable cause, and not just the orders issued under the Stored Communications Act. The defendants emphasized that the historical cell site location data obtained in this case allowed the officers to track their whereabouts over an extended period of time, giving them access to intimate information regarding the defendants' travels and associations. The government's acquisition of this cumulative data violated their reasonable expectations of privacy. The government asserted that the defendants had no reasonable expectation of privacy in information, including their location at the time of a call, which they voluntarily conveyed to a third party, the cell phone service provider, every time they dialed their phones. (*Graham, supra*, at 387-88.)

While the suppression motion was pending before the district court, the Supreme Court issued its opinion in *Jones*. The district court acknowledged that five justices of the Supreme Court believed that electronic location tracking, conducted over an extended period of time can implicate an individual's reasonable expectations of privacy. [24] The five justices suggested that while short-term tracking of a defendant's location during a single journey on public roads would not violate his reasonable expectation of privacy,

---

[24] The district court was referring to the four justices represented by Justice Alito's concurring opinion and Justice Sotomayor, who concurred separately and essentially cast the fifth vote for two separate opinions – Justice Scalia's official majority opinion relying on trespass theory and Alito's four-justice concurrence, relying on the reasonable-expectation-of privacy test. "Jones can plausibly be understood as having two separate majority opinions." (*Graham, supra*, at 405, fn. 15.)

constant 24-hour surveillance for a month would do so, as it would provide the government officials with aggregate information regarding the defendant's movements. This "mosaic" would allow the government to ascertain one's political or religious beliefs, habits and associations. (*Graham, supra*, at 390-95.) The district court did not believe that *Jones* governed the outcome of this case or resolved the issue of whether the government's acquisition of historical cell site location data over an extended period, violated the defendants' reasonable privacy expectations. The district court stressed factual differences between the surreptitious placement of a GPS device on a defendant's vehicle to precisely track the vehicle's every move from that moment on, and the government's acquisition of historical cell phone data indicating the defendant's past locations, data that the defendant had voluntarily conveyed to his cell phone service provider. (*Id.*, at 391-92.)

The district court concluded that the government's acquisition of historic cell site location records from the defendants' cell phone service provider did not violate the defendant's reasonable expectations of privacy. The court relied on the "third-party doctrine" which states that a person has no reasonable privacy expectation in information that he voluntarily conveys to a third party, information that the third party maintains in its business records. The person assumes the risk that the third party will share this information with the government. (See *Smith v. Maryland* (1979) 442 U.S. 735 [the defendant had no reasonable expectation of privacy in the phone numbers he dialed from his home phone which were captured by a pen register installed by the telephone company at the government's request, because he voluntarily conveyed that information to the phone company when he dialed the phone].) Similarly, a cell phone user voluntarily exposes his cell site location to his phone service provider every time he dials his cell phone or receives a call. (*Graham, supra*, at 397-401.)

2. *In re Application of the United States of America for Historical Cell Site Data* (5th Cir. 2013) 724 F.3d 600: To compel cell phone service providers to provide a subscriber's historical cell site data from a cell phone service provider, government officials need only obtain a court order authorized by the Shared Communication Act under the reasonable suspicion standard; they do not need a warrant based on probable cause. Note, however, that there is a dissent in this panel decision which would require a warrant supported by probable cause.

Government officials applied under the Stored Communications Act for a court order compelling a cell phone service provider to produce sixty days of a particular cell phone's historical cell site records. Even though each application set forth specific and articulable facts supporting a reasonable belief that the records were relevant to an on-going criminal investigation, the magistrate refused to order disclosure of these records,

holding that compelled warrantless disclosure of cell site data violates the Fourth Amendment. The district court agreed, stating that the government must seek a warrant based on probable cause to obtain these cell phone location records. The government appealed to the Fifth Circuit. As there was no party opposing the government's ex parte application, the ACLU and Electronic Frontier Foundation (EFF) participated as amici curiae and filed a joint brief. (*In re Application, supra*, at 602-03.)

Writing for a two-judge majority, Circuit Judge Clement disagreed with the magistrate and the district court; the government need only obtain a court order based on a statutory standard less than probable cause to compel cell phone service providers to hand over historical cell cite location records. The cell phone user has no reasonable expectation of privacy in this location data that he voluntarily discloses to his service provider. The ACLU/EFF contended that individuals have a reasonable expectation of privacy in their location information when they are tracked in a constitutionally protected place, like the home, or when they are tracked for an extended period of time, i.e. 60 days. The ACLU/EFF relied on *United States v. Karo*, supra, 468 U.S. at 705, for the first point, and on the *Jones* concurring decisions for the second point.[25] Judge Clement rejected this analysis, because in *Karo* and in *Jones*, government officials were collecting the location information by surreptitious means. In the present case, the cell site location data was legitimately collected and stored by a third party, the service provider, with the cell phone user's knowledge.[26] Each time an individual uses his cell phone to make a call, he knowingly exposes his approximate location to his service provider and thus

---

[25] As discussed above, the Supreme Court held, in *Karo*, that officers' use of a beeper, concealed in a container of chemicals, to monitor the container's location within the defendants' private residences violated their reasonable expectations of privacy in their homes. (*Karo supra*, at 714-15.)

[26] Justice Clement stated that a telephone user understands that when he makes a call, his phone sends a signal to a nearby cell tower and that the service provider keeps records of location information. Moreover, this information is generally set forth in the contracts between the service providers and their subscribers. (*In re Application, supra*, at 613.) The Third Circuit, in a 2010 opinion, questioned the assumption that a cell phone customer "voluntarily" shares his location information with a cell phone service provider in any meaningful way. "[I]t is unlikely that cell phone customers are aware that their cell phone providers collect and store historical location information. Therefore, 'when a cell phone user makes a call, the only information that is voluntarily and knowingly conveyed to the phone company is the number that is dialed'." (See *In re Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't* (3rd Cir. 2010) 620 F.3d 304, 317-318 [citing an amicus brief filed by EFF].)

surrenders any reasonable expectation of privacy in that information. Complying with the procedures set forth in the Stored Communication Act, the government can apply for a court order compelling the release of this information for use in a criminal investigation. (*In re Application, supra*, at 608-615.)

In his dissent, Judge Dennis decided the issue – whether the government needs to obtain a warrant in order to compel a service provider to release historical cell site location data – as a matter of statutory construction rather than as a Fourth Amendment issue. Judge Dennis noted that provisions of the Stored Communications Act require that the government obtain a warrant supported by probable cause *or* a court order based on reasonable suspicion to obtain cell phone records from a service provider. The statute is ambiguous as to when the government must follow the warrant procedure. Judge Dennis noted that ambiguous language in a statute must be construed to avoid serious constitutional doubts. He interpreted the language in the Shared Communications Act to require a warrant, based on probable cause when law enforcement officers seek records that may be protected by the Fourth Amendment, specifically including historic cell site location data. (*In re Application, supra*, 724 F.3d at 615-629 [diss. opn. of Dennis, J.].)

In addressing whether cell phone users have a reasonable expectation of privacy in cumulative cell site location information, Judge Dennis discussed *United States v. Jones*. Judge Dennis noted that in *Jones*, "every member of the Court acknowledged ... that law enforcement's access to the location information generated by cell phones [or other electronic devices] raises serious constitutional questions." (*In re Application, supra*, at 622.)[27] Judge Dennis also emphasized that Justice Sotomayor's concurring opinion "expressed serious doubts about extending the third party records doctrine applied in *Smith v. Maryland* - and relied upon by today's majority - to location information generated by modern devices such as 'GPS-enabled smartphones'." (*In re Application, supra*, at 623-624, citing *Jones, supra*, at 955-57 [conc. opn. of Sotomayor, J.].)[28]

---

[27] Indeed, the Eleventh Circuit recently decided that the provision of the Stored Communications Act which allowed the government to obtain cell site location information by court order and without a warrant based on probable cause violated a defendant's Fourth Amendment rights. (*United States v. Davis* (11th Cir. 2014) 754 F.3d 1205.) However, this Eleventh Circuit opinion has been vacated pending rehearing en banc. (*United States v. Davis* (11th Cir. 2014) 573 Fed. Appx. 925.) The *Davis* opinion is still worth reading, particularly the court's discussion of *Jones*.

[28] **Justice Sotomayor proposed that in this digital age, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information that he or she voluntarily discloses to third parties - data that could**

G. After *Jones*, Does The Government Need a Warrant Based on Probable Cause to Obtain Cell-Site Location Data to Track a Cell Phone Users Future Movements in Real Time[29]

1. *United States v. Skinner* (6th Cir. 2012) 690 F.3d 772: Government officials did not conduct a Fourth Amendment search, requiring a warrant based on probable cause, when they obtained data emanating from the defendant's cell phones to track his movements for three days.

DEA agents were investigating a marijuana-trafficking conspiracy. They learned that the defendant was a courier in the operation, using his truck to transport money and drugs across the country. During their investigation, the agents discovered that the defendant and other conspirators used discardable pay-as-you go cell phones to communicate, as they believed these phones were more difficult to trace. They may not have been aware that these phones were equipped with GPS. The agents believed that the defendant was using two such phones to communicate with co-conspirators, so they obtained orders from a magistrate authorizing the phone company to ping the GPS-equipped phones to ascertain the defendant's location as he drove his truck cross-country.

---

end up in government hands. After all, people reveal a great deal of information about themselves to third parties (e.g. cell phone and internet service providers) whenever they punch in a number on their cell phone, send a text, or visit a web site. Justice Sotomayor questioned whether "people would accept without complaint the warrantless disclosure to the government of a list of every web site they had visited in the last week, or month, or year." (*Jones, supra*, at 957.)

[29] In these cases, law enforcement officers sought access to service records documenting a suspect's prospective and future locations, whenever the suspect used his cell phone. These records allowed the officers to monitor the suspect's movements in real time. In contrast to the cases involving government requests for historic cell site data (service provider records of the cell phone user's past locations), the majority of federal courts considering the issue – with the notable exception of *United States v. Skinner* (6th Cir. 2012) 690 F.3d 772 -- have held that a warrant based on probable cause is required to obtain real-time and prospective cell site location information from service providers. (See *United States v. Powell* (E.D. Mich 2013) 943 F.Supp.2d 759, 770-73; *United States v. White* (E.D. Mich. November 24, 2014) 2014 WL 6682645. In *White*, the district court cited several federal district court and state court cases which had held that an individual has a reasonable expectation of privacy in cell cite location information that indicates his present and future movements in real time, as opposed to the individual's past movements, revealed by historic cell site location data. (*White, supra*, at *5.)

After three days of tracking the phones, they learned that one phone was stationary at a truck stop. The agents went there, discovered the defendant's motorhome and truck, searched the motorhome and found over 1,000 pounds of marijuana. The defendant moved to suppress the incriminating evidence, arguing that it was derived from a warrantless search - i.e. the agents use of the GPS location data emitted from his cell phones. The district court denied the motion and the Sixth Circuit affirmed that denial. (*Skinner, supra*, at 774-77.)

The Sixth Circuit found that there was no Fourth Amendment violation because the defendant did not have a reasonable expectation of privacy in the location data given off by his voluntarily procured pay-as-you-go cell phone. Relying on *Knotts*, the court reasoned that the agents could have obtained the same information regarding the defendant's movements on public roads through visual surveillance. "There is no inherent constitutional difference between trailing a defendant and tracking him via technology. **Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system." Advances in technology should help the police, not the criminals**. (*Skinner, supra*, 777-78.)

The Sixth District distinguished *Jones* on two grounds: 1) The *Jones* majority opinion explicitly relied on the officers' trespass in installing the GPS device on the defendant's car. No such physical intrusion occurred in Skinner's case. 2)The concerns raised by Justice Alito's concurrence regarding comprehensive long-term location tracking are not present in this case; the officers tracked Skinner's pay-as-you-go cell phones for only three days. (*Id*., at 779-780.)[30]

[30] In *United States v. Barajas* (10th Cir. 2013) 710 F.3d 1102, 1108, fn. 2, the Court of Appeal disagreed with *Skinner*; it assumed without deciding that the pinging of the defendant's cell phone to determine its location is a search within the meaning of the Fourth Amendment. Although the court order authorizing the GPS pinging of the defendant's phone may not have been supported by probable cause, the *Leon* good-faith exception precluded suppression of the incriminating evidence obtained by the location tracking. (*Barajas, supra*, at 1108-11.)

2. *United States v. Powell* (E.D. Mich. 2013) 943 F. Supp. 2d 759: Government officials need a warrant based on a showing of probable cause for long-term real-time site-location tracking of cell phones, in both public and private areas.[31]

Defendants in a drug prosecution moved to suppress evidence, including cell-site location data acquired from six cell phones from March through October 2011, pursuant to search warrants. Warrants were issued on five different dates. Each warrant authorized DEA agents to obtain real-time location for the cell phone for up to thirty or forty-five days, allowing a total of nine months of tracking. The defendants argued that the warrants authorizing the acquisition of this data regarding the phones' future movements were not supported by probable cause, and thus, all evidence that resulted from the location tracking should be suppressed. (*Powell, supra*, at 764-67.)

The district court noted that the majority of federal courts that have considered the issue require the government to make a probable-cause showing in order to obtain real-time cell-site location data. (*Id.*, at 770-72.) The Sixth Circuit's 2012 decision in *Skinner* (discussed above) was a notable exception and *Skinner* was distinguishable from this case on its facts, i.e. the obtained cell phone data in *Skinner* indicated the defendant's movements on public roads for three days, whereas the warrants issued in *Powell* authorized the agents to obtain tracking data for multiple cell phones for nine months. (*Id.*, at 773-76.) The district court's Fourth Amendment concerns regarding the nine-months of tracking authorized in this case overlapped with those expressed by the five concurring justices in *Jones*, regarding the amount of private information that could be gleaned from the totality of this comprehensive surveillance. (*Id.*, at 776.)

The district court concluded that government agents needed a warrant supported by probable cause to acquire authorization for long-term real-time cell-site location tracking. (*Id.*, at 778-79.)The court concluded that the DEA agents did not make a sufficient showing of probable cause in this case. Nevertheless, the incriminating evidence derived from location-tracking would not be suppressed as the agents relied on those warrants in good faith. (*Id.*, at 780-84.)

---

[31] **The most valuable aspect of this long opinion is the explanations given on a variety of topics: 1)the different methods used to locate a cellular phone, cell-site tracking (using cell towers) versus GPS signal locating of smart phones; 2) the differences between real-time prospective cell site location information (future locations of the cell phone) and historical cell site location information (past locations); and 3)for both types of tracking, the split of authority as to whether probable cause is required to obtain cell phone site location tracking data.**

PART TWO
LAW ENFORCEMENT SEARCHES OF THE CONTENTS OF CELL PHONES AND OTHER DIGITAL DEVICES

For years, the United States Supreme Court was reluctant to assess the interplay between Fourth Amendment protection and new and evolving digital technology. Even as the percentage of people carrying cell phones (particularly smart phones) increased, the Court declined to decide whether the police may search a cell phone's data files, following an arrest, without obtaining a warrant. Repeatedly, the Court denied petitions for certiorari filed in cases that had given opposite answers to this important question.(See, e.g., *State of Ohio v. Smith* (2009) 920 N.E. 2d 949 [Ohio Supreme Court held that a warrant was required; cert. den. 10/4/2010]; *People v. Diaz* (2011) 51 Cal. 4th 84 [California Supreme Court held that no warrant was required; cert. den. 10/3/11].) Apparently, the U.S. Supreme Court was not interested in resolving the split of authority.

In *City of Ontario v. Quon*, its 2010 decision upholding the work-related search of an employee's text messages stored on a government-issued pager, the Supreme Court explained that it must proceed with care when considering government intrusions on an individual's privacy expectations in communications stored on electronic equipment, including pagers and cell phones. "The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear." (*City of Ontario v. Quon* (2010) 130 S.Ct. 2619, 2629.)

Finally, in 2014, the Court overcame its reluctance when it granted certiorari in *People v. Riley*, 2013 WL 475242 (Cal. App. 4 Dist), and *United States v. Wurie* (1st Cir. 2013) 728 F.3d 1.) On June 25, 2014, the Supreme Court issued its decision in *Riley v. California* (2014) 134 S.Ct. 2473, which is the subject of Part Two of these materials.

I. *RILEY V. CALIFORNIA* (2014) 134 S.CT. 2473

In *Riley v. California*, and the companion case of *United States v. Wurie*, a unanimous Supreme Court held that law enforcement officers generally need to obtain a warrant before they may search the contents of a cell phone seized from an individual at the time of his arrest.[32] The Court recognized that the degree of privacy secured to citizens by the Fourth Amendment has been affected by advances in digital technology -- specifically, the advent of cell phones that store vast quantities of personal data.

A. An Overview of the Chief Justice Roberts' Majority Opinion[33]

In determining whether law enforcement officers must obtain a warrant to search the data files of cell phones seized from arrestees, Chief Justice acknowledged the need to assess whether the traditional search incident to arrest exception applies to modern cell phones. This task was challenging because the ever-increasing number of people who own cell phones "keep on their persons a digital record of nearly every aspect of their lives from the mundane to the intimate". (*Riley, supra*, 134 S.Ct. at 2490.)

Supreme Court precedents had defined the scope of the search incident to arrest exception in accordance with its purposes - to protect officer safety and prevent the destruction or concealment of evidence. From these precedents, the *Robinson-Chadwick* rule emerged: Following arrest, officers could conduct a warrantless search of personal property found on or near the arrestee that was immediately associated with his person, including wallets, address books and purses. (*Riley, supra*, at 2482-2384, 2388; see *United States v. Robinson* (1973) 414 U.S. 218; *United States v. Chadwick* (1977) 433 U.S. 1.) Chief Justice Roberts concluded that although a cell phone may be found on the arrestee, it is not a personal effect that can be searched without a warrant. Because of the vast amount of private data stored in the cell phone's files, it is not like a wallet. Rather, it is a minicomputer that can also be used as a telephone. (*Riley, supra*, at 2488, 2489.)

---

[32] Chief Justice Roberts wrote the majority opinion, which was joined by seven justices. Justice Alito wrote a concurring opinion, and agreed that the a warrant was required to search data stored on a cell phone following an arrest. He wrote separately because he believed that the regulation of evolving electronic surveillance should be left to legislatures, elected by the people, and not to the federal courts.

[33] **I recommend that you first read this summary of the *Riley* majority opinion. If you are interested in a more detailed discussion of Chief Justice Robert's analysis and Justice Alito's short concurring opinion, read Section IC and ID.**

Roberts discussed the enormous quantity and the private nature of the information that cell phone users store on these ubiquitous devices – months worth of e-mails, scores of photos, calendar entries, financial statements, medical data, books and videos. From viewing all these files together, along with the "apps" the user has downloaded, GPS records and internet search history, the sum of an individual's private life can be reconstructed. (*Id*., at 2488-90.) "Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house." (*Id.*, at 2490-91.)

Roberts also reasoned that an immediate search of the data files of a cell phone that has been seized and secured by officers would not serve the government interests underlying the search incident to arrest exception - the need to protect officer safety and to prevent the destruction or concealment of evidence. The threat that incriminating information stored on the seized cell phone could be destroyed by remote wiping or data encryption would not justify an immediate search in every case. (*Id*., at 2484-88.)

Finally, Chief Justice Roberts acknowledged that requiring a warrant might impede law enforcement efficiency – i.e. officers ability to immediately access incriminating information. However, "[p]rivacy comes at a cost." The Court was not stating that the cell phone's data files could never be searched; they were merely requiring the government to seek and obtain a warrant before doing so. Given that modern technology has enabled officers to acquire a warrant more quickly, this was not a great burden. (*Id.*, at 2493.)

In exceptional cases, where the officers reasonably believed that they needed to immediately view the contents of the arrestee's cell phone to protect officer safety or prevent a crime, they could rely on exigent circumstances. A court would then determine whether the emergency justified the warrantless search in that specific case. (*Id.*, at 2494.)

B. The Underlying Facts, Appellate Court Opinions, and the Grants of Certiorari to Resolve the Split of Authority

1. *Riley v. California*

The Facts and Trial Court Proceedings

Defendant Riley was stopped by a police officer for a traffic violation and ultimately arrested. During a search incident to arrest, an officer seized a "smart phone" from Riley's pocket. The officer immediately searched the cell phone's data files and noticed the repeated use of a term associated with a local criminal street gang. At the police station, about two hours after the arrest, another officer examined the phone's

digital contents and found videos indicating Riley's association with this local gang, as well as photos implicating Riley in a recent shooting. Riley was charged with multiple crimes arising from the shooting incident, with a gang enhancement. Prior to trial, Defendant Riley moved to suppress the evidence obtained from his cell phone, arguing that the two warrantless searches violated his Fourth Amendment rights The trial court rejected this argument. The photos and videos retrieved from Riley's cell phone were submitted into evidence at his jury trial and Riley was convicted. Riley appealed.

People v. Riley, 2013 WL 475242 (Cal. App. 4th Dist)

In an unpublished decision, the California Court of Appeal (Fourth District, Division 1) affirmed the trial court's denial of the motion to suppress. (*People v. Riley*, 2013 WL 475242 (Cal. App. 4th Dist).) The Court of Appeal relied on the California Supreme Court's decision in *People v. Diaz* (2011) 51 Cal. 4th 84*,* which held that an arrestee's cell phone could be searched incident to arrest, without a warrant. (See *People v. Riley*, supra, at *6 [stating that "*Diaz* controls the present case"].)

> ***People v. Diaz*** **(2011) 51 Cal. 4th 84 [cert. den. 10/3/11)**: **In a 5-2 opinion, the California Supreme Court applied U.S. Supreme Court precedents from the 1970's to hold that the warrantless search of the text message folder of the defendant's seized cell phone, conducted at the detention facility 90 minutes after the defendant's arrest, was a lawful search incident to arrest; the cell phone was personal property immediately associated with the defendant's person and thus lawfully subject to a delayed warrantless search.**

An officer arrested Diaz after observing him sell drugs to a police informant. While searching Diaz and finding drugs, the officer also discovered a cell phone on "his person", but the phone was not seized until Diaz arrived at the police station. About 30 minutes later, and 90 minutes after Diaz's arrest, an officer searched the phone's text message folder and discovered incriminating messages. (*Diaz, supra*, at 89.)

To determine whether this delayed warrantless search of the cell phone's contents was justified by the search incident to arrest exception, the California Supreme Court reviewed three United States Supreme Court precedents from the 1970's: 1) *United States v. Robinson* (1973) 414 U.S. 218 [upholding the officer's removal of cigarette packet from the arrestee's pocket and the immediate inspection of its contents, without a warrant, as a search incident to arrest]; 2) *United States v. Edwards* (1974) 415. U.S. 800 [upholding a warrantless search of the arrestee's clothing ten hours after his arrest, as the clothes could have been searched at the arrest scene]; 3) *United States v. Chadwick* (1977) [invalidating the warrantless search of a large locked footlocker seized from the area within the arrestee's immediate control, but not searched until 90 minutes after the

arrest while securely in police custody].)

From these cases, the California court derived this rule: Following an arrest, law enforcement officers may – without obtaining a warrant -- search personal property found on the arrestee which is immediately associated with his person; that search can be done at the arrest scene or any reasonable time thereafter, even if the item is within the officer's exclusive control and no longer accessible by the defendant. Pursuant to this rule, officers have been permitted to search non-digital items found on arrestees, including wallet, photos, letters and diaries which may contain personal information. Cell phones seized from the arrestee qualify as items immediately associated with the person and may be searched without a warrant. (*Diaz, supra*, 51 Cal. 4th at 91-96, 100-01.)

The California Court insisted on treating a cell phone as though it was a conventional container found on the arrestee's person. The Court refused to consider the unique attributes of cell phones – i.e. that their files hold vast amounts of personal information, far more than pre-digital containers like wallets or diaries. Pursuant to binding United States Supreme Court precedent, the propriety of the search depended on the cell phone's location at the time of arrest, not it's character. (*Diaz, supra*, at 94-98.) It should be up to the Supreme Court to reconsider these precedents in light of modern technology. (*Id*., at 101-03.)[34]

2. *United States v. Wurie*

The Facts and Trial Court Proceedings

A police officer observed Defendant Wurie make an apparent drug sale from a car. Wurie was arrested and transported to the police station. At the station, an officer seized two cell phones from Wurie, one of which was a "flip phone" (generally having a smaller range of features than a smart phone). Five to ten minutes later, the officers noticed that the flip phone was receiving calls from a source identified as "my house" on the phone's external screen. The offices accessed the phone's call log to determine the phone number associated with "my house". With that information, the police determined Wurie's

[34] The dissenting justices focused on the massive amount of highly personal information that can be stored on cell phones, and concluded they were very different than small spacial containers such as wallets, purses and address books. Fourth Amendment rules should be re-evaluated in light of this new technology and police should obtain a warrant before searching cell phone contents. The dissenting justices anticipated many of the observations made by Chief Justice Roberts three and one-half years later in *California v. Riley*. (*Diaz, supra*, at 104-111 [dis. opn. of Werdegar, J.].)

address and obtained a warrant to search his home. Upon executing the warrant, the officers found and seized drugs, cash, and a firearm. Wurie was charged with drug and firearm offenses. Prior to trial, Wurie moved to suppress evidence obtained from the search of his home, claiming that this later search was the fruit of the unconstitutional search of his cell phone. The trial court denied the suppression motion and Wurie was convicted. He appealed to the First Circuit Court of Appeals.

> ***United States v. Wurie*** **(1st Cir. 2013) 728 F.3d 1: In a 2-1 opinion, the First Circuit Court of Appeals held that the search incident to arrest exception does not authorize the warrantless search of cell phone data, after the phone has been seized from the arrestee's person, because the search invades substantial privacy interests and does not serve the purposes of the exception.**

In determining that the warrantless search of the cell phone contents was not authorized by the search incident to arrest exception and violated the defendant's Fourth Amendment rights, the First Circuit acknowledged the split of authority on this issue. Noting that the majority of courts considering the issue have ultimately upheld warrantless cell phone data searches, the court, in *Wurie*, sided with the minority. (*Wurie, supra*, at 5-6.) The First Circuit rejected the suggestion that the constitutionality of a cell phone search should be decided after the fact on a case-by-case basis and opted for a single standard to guide police officers, a bright-line rule. (*Id*., at 6.) Although the search of the call log on Wurie's flip phone was less invasive than the search of text messages, e-mails or photographs on more sophisticated smart phones, it is necessary for all warrantless cell phone data searches to be governed by the same rule. (*Id.*, at 13.)

In rejecting strict application of the *Robinson-Chadwick* rule (allowing a warrantless search of items found on an arrestee that are immediately associated with his person), the court found that Wurie's cell phone was *not* like a wallet or an address book. Rather, a modern cell phone is a computer; it stores large amounts of highly personal information, far more than could fit in a conventional container. (*Id.*, at 7-9.)

Most importantly, the First Circuit concluded that a warrantless search of a cell phone's contents, particularly after officers have seized and secured the device, does not serve the purposes of the search incident to arrest exception as set forth in *Chimel v. California* (1969) 395 U.S. 752, 763.) After officers have examined the cell phone's exterior and assured that it is not actually a weapon, there is no need to search the phone's data files as that data cannot harm them. Because there are ways to prevent the overwriting or remote wiping of data stored on a cell phone, there is no need to search the phone's contents immediately to prevent the destruction of evidence. There is time to get a warrant. (*Wurie, supra*, at 9-12.)

3. The United States Supreme Court Grants Certiorari in Both Cases

Presumably, the Supreme Court granted certiorari in these two cases because of the continuing split of authority on the issue of whether a warrant was required to search the contents of a cell phone seized from an arrestee at the time of arrest or soon after. As noted, in finding that no warrant is required, the Court of Appeal in *People v. Riley* insisted that the California Supreme Court's 2011 decision in *People v. Diaz* controlled the outcome. (*People v. Riley, supra*, at *6 .)[35] The majority opinion in *United States v. Wurie* represented the opposing position. (*Wurie, supra*, at 3-14.)[36]

C. The *Riley* Majority Opinion Authored by Chief Justice Roberts (Joined by Justices Scalia, Kennedy, Thomas, Ginsburg, Breyer, Sotomayor and Kagan)

Writing for the majority, Chief Justice Roberts firmly grounded his reasoning in the modern era of digital technology. This case presented the question of "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested." (*Riley, supra*, 134 S.Ct. at 2480.) Consequently, Roberts reviewed Supreme Court precedents that permit a warrantless search incident to arrest of the person and of property items found on or near him at the time of his arrest which are immediately associated with the arrestee's person. (*Riley, supra*, at 2482-84.) Chief Justice Roberts recognized, however, that reliance on these older precedents could not resolve the question presented because cell phones, particularly smart phones, are distinct from their pre-digital counter-parts. Because of the quantity and private nature of the information stored on the device, a modern cell phone is not the equivalent of an

---

[35] Several other courts agreed with the position of the California Supreme Court majority in *Diaz*, that police did not need a warrant to search the contents of a cell phone seized from an arrestee. (See, e.g., *United States v. Finley* (5th Cir. .2007) 477 F.3d 250 [cert. den. 4/16/07]; *United States v. Murphy* (4th Cir. 2009) 552 F.3d 405 [cert. den. 4/20/09]; *United States v. Flores-Lopez* (7th Cir. 2012) 670 F.3d. 803; *United States v. Curtis* (5th Cir. 2011) 635 F.3d 704 [cert. den. 10/3/11]; *Commonwealth v. Phifer* (2012) 979 N.E. 2d 210 [Supreme Judicial Court of Massachusetts].)

[36] The First Circuit approved the reasoning of the smaller number of courts ruling that police need to obtain a warrant before searching the contents of a cell phone seized from an arrestee:. (See, e.g. *State of Ohio v. Smith* (2009) 920 N.E. 2d 949 [Ohio Supreme Court; cert. den. 10/4/10]; *Smallwood v. State* (2013) 113 So. 3d 724 [Florida Supreme Court].)

address book, a wallet or a purse found on the arrestee, items that could be searched without a warrant. (*Riley, supra*, at 2484-90.) Roberts stated:

> **"These cases [referring to *Riley* and *Wurie*] require us to decide how the search incident to arrest doctrine applies to modern cell phones, which are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of human anatomy. A smart phone of the sort taken from Riley was unheard of ten years ago; a significant majority of American adults now own such phones." (*Riley, supra*, at 2484.)**

Moreover, Roberts observed that "many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives, from the mundane to the intimate." (*Riley, supra*, at 2490.) "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the founders fought." (*Id.*, at 2495.) Roberts concluded: "Our answer to the question of what police must do before searching [the contents of] a cell phone seized incident to arrest is accordingly simple - get a warrant." (*Ibid.*)

1. Chief Justice Roberts Reviewed Precedents Defining the Purpose and Scope of Warrantless Searches Incident to Arrest, Specifically Searches of Items of Personal Property Found on the Arrestees

The cell phones belonging to Mr. Riley and Mr. Wurie were seized from the two men immediately following their arrests. The contents of Mr. Riley's smart phone was searched at the arrest scene and then, more thoroughly, at the police station two hours later. Mr. Wurie's flip phone was seized when he arrived at the station after his arrest. The phone's call log was searched five to ten minutes later. In neither case, did the police obtain a warrant prior to searching the phones' digital files. (*Riley, supra*, 134 S.Ct. at 2480-81.) Were these warrantless searches of the cell phones' contents valid searches of the arrestees' personal property incident to arrest?

Regarding the search incident to arrest exception to the Fourth Amendment's warrant requirement, Chief Justice Roberts stated: "Although the existence of the exception for such searches has been recognized for a century, it's scope has been debated for nearly as long. The debate has focused on the extent to which officers may search property found on or near the arrestee." (*Id.* at 2482-83.)

Supreme Court decisions have defined the scope of a search incident to arrest, in accordance with its purposes: to disarm the arrestee to protect officer safety; and to prevent the destruction or concealment of evidence. Thus, at the time of arrest, the officer can search the arrestee and the area within his immediate control – the space from which he might grab a weapon or destructible evidence. (*Riley, supra*, at 2483, citing *Chimel v. California* (1969) 395 U.S. 752*,* 762-63; see also *United States v. Robinson* (1973) 414 U.S. 218 [upholding the officer's removal of cigarette packet from the arrestee's pocket and the immediate inspection of its contents, without a warrant, as a search incident to arrest]; *United States v. Chadwick* (1977) 433 U.S. 1 [invalidating the warrantless search of a 200 pound locked footlocker seized from the area within the arrestee's immediate control, but not searched until 90 minutes after the arrest while securely in police custody].) In *Chadwick*, the Court had explained the rule derived from its current decision and *Robinson*: Following an arrest, the police could search the person and the contents of personal property found on the arrestee and immediately associated with his person (e.g. a cigarette pack found in the arrestee's pocket). However, a search of property found within the arrestee's reaching area, but seized and secured in police custody, required a warrant (e.g. a locked footlocker). (*Riley, supra*, at 2384, citing *Chadwick, supra*, at 15.)

Subsequently, Roberts discussed appellate court cases that had applied the *Robinson-Chadwick* rule to approve warrantless searches, incident to arrest, of a variety of items found on the arrestee's person at the time of arrest, including a billfold, an address book, a wallet and a purse. (*Riley, supra*, at 2488 [citations omitted].)[37]

---

[37] Here are some cases that applied the *Robinson-Chadwick* rule to validate warrantless searches of conventional items seized from arrestees when they were taken into custody as searches incident to arrest. In each case, the item was found to be immediately associated with the arrestee. Some of these searches were conducted right after the arrest; others were conducted minutes or hours later: *United States v. Passaro* (9th Cir. 1980) 624 F.2d 938 [validated the delayed search of the defendant's wallet incident to arrest]; *United States v. Burnette* (9th Cir. 1983) 698 F.2d 1038 [validated the immediate cursory search of the defendant's purse at the arrest scene, and the more thorough search at the police station]; *Curd v. City of Judsonia, Arkansas* (8th Cir. 1998) 141 F.3d 839 [validated the delayed search of the defendant's purse which had been seized from her at the time of arrest]; *United States v. Holzman* (9th Cir. 1989) 871 F.ed 1496 [validated the initial search of the defendant's address book at the arrest scene and the more thorough search at the police station]; *United States v. Garcia* (7th Cir. 1979) 605 F.2d 349 [validated the immediate search of the defendant's hand-held unlocked suitcase at the arrest scene].)

2. A Cell Phone is Not a Wallet, but a Minicomputer. Chief Justice Roberts Considered the Unique Attributes of Modern Cell Phones in Concluding That They Were Distinct From Pre-Digital Items Found to be Immediately Associated With the Arrestee's Person

Unlike the majority of California Supreme Court justices in *People v. Diaz, supra*, 51 Cal. 4th at 84, Chief Justice Roberts was willing to consider the unique attributes of 21st Century cell phones. Roberts rejected the government's claim that cell phones were "materially indistinguishable" from items found on arrestees, like wallets, that could be searched because they were immediately associated with the person. "That is like saying a ride on horseback is materially distinguishable from a flight to the moon. Both are ways of getting from Point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet or a purse." (*Riley, supra*, 134 S.Ct. at 2488.)

Preliminarily, there is the element of pervasiveness. More than 90% of American adults own cell phones, and most of these are smart phones that allow people to carry vast amounts of sensitive private information with them as they go about their day – something that was impossible prior to the digital age. (*Riley, supra*, at 2490.) **"Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person." These devices are in fact minicomputers that can also be used as telephones. (*Id*, at 2489.)**

Cell phone's have immense storage capacity. Users of modern cell phones store the emails they have received for several months, financial data, medical records, scores of photos, and even books and videos on these devices. To lug all of these things around in non-digital form, the person would need a 200-pound trunk of the sort possessed by Mr. Chadwick, and in that case, the Supreme Court required a warrant before the contents of the trunk could be searched. (*Riley, supra,* at 2489.) The cell phone's vast storage capacity affects the user's privacy. The cell phone collects in one place several distinct types of personal information, gathered over time. The phone's digital files reveal more, when viewed in combination, than any isolated record. For example, by browsing through hundreds of photographs stored on a cell phone, the sum of an individual's private life can be reconstructed. (*Ibid*.)

The type of information stored on a cell phone is also significant. By searching the "apps" that the user has chosen to download, the user's internet search history and the nature of the files he has stored on the phone, one can discern his private interests and political or religious affiliations. If the phone is equipped with GPS, one could reconstruct the users movements over time. (*Riley, supra*, at 2490, citing *United States v. Jones*

supra, 132 S.Ct. at 955-56 [conc. opn. of Sotomayor, J.].) **"Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house", an intrusion that clearly requires a warrant. (*Id.*, at 2490-91.)** Searches of cell phones, containing vast quantities of personal information, implicate weighty privacy concerns, even when the cell phone user is in custody. (*Id.*, at 2485, 2488.)

3. Searches of Cell Phone Contents do not Serve the Government Interests Underlying the Search Incident to Arrest Exception

Roberts concluded that in the vast majority of cases, warrantless searches of cell phones seized from an arrestee at arrest would not serve the two government interests identified in *Chimel* – the need to protect officer safety at the arrest scene and the need to prevent the destruction or concealment of evidence. (*Riley, supra*, at 2484-88.)

"Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape." (*Id.*, at 2485.) Incident to an arrest, officers can seize the phone and examine its physical aspects to ensure that the phone itself cannot be used as a weapon. "Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one." (*Ibid*.) Roberts rejected the government's assertion that a search of cell phone data might ensure officer safety by revealing potential dangers; for example, a search of e-mails or text messages might alert officers that the arrestee's confederates are headed to the scene. This would not be a concern in all arrests, sufficient to dispense with the warrant requirement. If the facts in a particular case supported a reasonable belief that threats outside the arrest scene might be discerned by immediately checking the cell phone's contents, that could constitute an exigent circumstance, excusing the warrant requirement in that case. (*Id.*, at 2485-86.)

The government argued that law enforcement officers should be allowed to quickly review a cell phone's data files for incriminating evidence to prevent its destruction. Roberts rejected this concern, noting that officers have the right to seize and secure the arrestee's cell phone while seeking a warrant. "[O]nce law enforcement officers have secured a cell phone, there is no longer any risk that the arrestee himself will be able to delete incriminating data from the phone."

The government also argued that the potentially incriminating information stored on seized cell phones could still be destroyed by either remote wiping or data

encryption.[38] Roberts countered these concerns with several observations. First, "these broader concerns about the loss of evidence are distinct from *Chimel's* focus on a defendant who responds to arrest by trying to conceal or destroy evidence with in reach." With either method, the arrestee does not actively attempt to destroy the evidence; remote wiping usually depends on the actions of third parties not present at the arrest scene and encryption happens automatically. (*Riley, supra*, at 2486.) Second, the government did not present evidence indicating that either of these practices were prevalent. (*Ibid*.) Third, law enforcement officers can prevent remote wiping by disconnecting a phone from the network; they can turn the phone off, remove its battery or place it in an enclosure that isolates the phone from radio waves. (*Ibid*.)

4. Chief Justice Roberts Rejected Arguments Made by the Government in Support of Searching Cell Phone Data Without a Warrant

Chief Justice Roberts also rejected other arguments advanced the government in support of permitting cell phone searches, without a warrant, in certain circumstances. Roberts preferred to set forth a general rule – requiring a warrant before law enforcement officers could search cell phone data files in almost all cases. All of the government's proposed rules would necessitate a disfavored and unworkable case-by-case analysis, contravening "our general preference to provide clear guidance to law enforcement through categorical rules." (*Riley, supra*, at 2491-92.)

The government had suggested that the *Arizona v.Gant* standard be imported from the vehicle context to allow a warrantless search of cell phone contents whenever officers reasonably believes that the phone contained evidence of the crime of arrest.[39] Roberts opined that because of the range of information that can be stored on cell phones, application of this *Gant* rule would give the police unbridled discretion to search cell

---

[38] Remote wiping occurs when a phone, connected to a wireless network, receives a signal that erases stored data. This could happen when a third party sends a remote signal or when a phone is pre-programmed to delete data upon entering or leaving a particular geographical area. Encryption is a feature on some modern cell phones. When the phone locks, its data becomes protected by sophisticated encryption so that the police could not read it. (*Riley, supra*, at 2486.)

[39] In *Arizona v. Gant* (2009) 556 U.S. 322, the Supreme Court held that officers who had arrested a vehicle occupant could only search the passenger compartment when the arrestee was unsecured and within reaching distance of the passenger compartment at the time of the search. Also, officers could search the passenger compartment when it was reasonable to believe that evidence relevant to the crime of arrest might be found there.

phone contents in every case. "It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone." (*Riley, supra*, at 2492.)

Roberts dismissed another limiting principle proposed by the government – i.e. that officers could search cell phone data if they could have obtained the same information from a pre-digital counterpart. Roberts countered that the fact that an arrestee could keep a couple of photographs in his wallet or tuck a paper bank statement into his pocket does not justify the search of the thousands of photographs he stores in his cell phone's digital gallery or the vast amounts of financial information that can be kept on a modern cell phone. (*Id.*, at 2493.)

5. "Privacy Comes at a Cost"

Chief Justice Roberts recognized that all cell phone users, including arrestees have significant privacy interests in the vast amount of private information stored on their cell phones even after they are taken into custody. He also noted that the government interests underlying the search incident arrest exception are not well served by allowing warrantless searches of cell phone data. Consequently, warrants are required in most circumstances before an officer can search a cell phone's contents. (*Riley, supra*, 134 S.Ct. at 2484-85, 2494-95.)

Roberts acknowledged that protecting privacy may necessarily impede law enforcement efficiency:

> **"We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. *Privacy comes at a cost*."**
> ***Riley, supra*, at 2493 [emphasis added]**

Roberts emphasized that the Court was not holding that the information stored on an arrestee's cell phone could never be searched. They merely held that "a warrant is generally required before such a search, even when a cell phone is seized incident to arrest." The warrant requirement is the bedrock principle of the Fourth Amendment, subject to only limited exceptions. Roberts continued: "Our cases have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow weighted against the

claims of police efficiency'." *Riley, supra*, at 2493, citing *Coolidge v. New Hampshire* (1971) 403 U.S. 443, 481.)

The Chief Justice noted another effect of recent technological advances; it is easier and quicker for law enforcement officers to secure a warrant. Officer could use their digital devices to e-mail a warrant request to a judge's iPad and have the signed warrant e-mailed back to the officer in less than 15 minutes. (*Riley, supra*, at 2493; see also *Missouri v. McNeely* (2013) 133 S.Ct. 1552, 1562 [noting that technological developments have enabled police officers to secure warrants from magistrates more quickly, using telephones or other electronic means].)

Roberts concluded that even though the search incident to arrest exception does not allow warrantless searches of *all* seized cell phones, other case-specific circumstances, including exigent circumstances, may justify searching the data on a particular phone without a warrant. Roberts elaborated: "In light of the availability of exigent circumstances, there is no reason to believe that law enforcement officers will not be able to address some of the more extreme hypotheticals that have been suggested: a suspect texting an accomplice who, it is feared, is preparing to detonate a bomb, or a child abductor who might have information about the child's location on his cell phone." (*Id.*, at 2494.) Roberts emphasized, however, that if police officers relied on the exigent circumstances exception, a court would subsequently determine whether an emergency justified the warrantless search in that particular case. (*Ibid*.)

D. The Concurring Opinion Authored by Justice Alito

Justice Alito began his concurrence with this statement: "I agree with the Court that law enforcement officers, in conducting a lawful search incident to arrest, must generally obtain a warrant before searching information stored or accessible on a cell phone." (*Riley, supra*, 134 S.Ct. At 2495 [conc. opn. of Alito, J.].) Alito also agreed that modern cell phones store a quantity of information, some highly personal, that no person could have carried in hard-copy form. Consequently, the Court could not "mechanically apply the rule used in the predigital era to the search of a cell phone." A new balancing of law enforcement and privacy interests was necessary. (*Id*., at 2496.)

Justice Alito wrote separately to address two points: The first was a disagreement about doctrine. Alito was not convinced that the original rules permitting a search of the person incident to arrest were based on the need to protect officer safety and prevent the destruction of evidence. He noted that searches incident to arrest were sanctioned in English common law years prior to the adoption of the Fourth Amendment. These searches were permitted to take probative evidence from the arrestee, evidence that would

be used in the government's criminal prosecution. (*Id.*, at 2495-96.)

Alito's second point was a reiteration of a view point that he'd expressed two years earlier in *United States v. Jones, supra*, 132 S.Ct. at 962-64 [conc. opn. of Alito, J.] – that the regulation of electronic surveillance, and rules regarding searches of cell phone contents in particular, are better left to legislatures rather than the courts. He noted that searching the contents of modern cell phones "implicates very sensitive privacy interests that this Court is poorly positioned to understand and evaluate." (*Riley, supra*, at 2497.) Justice Alito concluded:

> **"Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago. In light of these developments, it would be very unfortunate if privacy protection in the 21st Century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to access and respond to the changes that have already occurred and those that almost certainly will take place in the future." (*Id.*, at 2497-98.)**

II. QUESTIONS LEFT UNANSWERED BY *RILEY*

Compared to *United States v. Jones*, the Supreme Court's opinion in *California v. Riley* left fewer unanswered questions for future courts to resolve.

1. Would a warrant be required before law enforcement officers could search the contents of other digital devices with large storage capacity which have been seized from the arrestee's person – for example, flash drives, digital cameras, small tablets, apple watches?

Presumably, based on Chief Justice Robert's reasoning, the rule of *Riley*, requiring a warrant would apply to these types of digital devices.

2. What kind of exigent circumstances would excuse the officer's obligation to obtain a warrant before searching cell phone contents?

Defense advocates must be vigilant to assure that this exception does not swallow the rule.

3. What if a vehicle driver is arrested for selling drugs and following his arrest, police relying on *Arizona v. Gant* (2009) 556 U.S. 322, search the vehicle's passenger compartment based on a reasonable belief that evidence relevant to the crime might be found there. If, during that search, a cell phone is found on the front seat and seized, may the officers consider it a container and search its contents, or search its data based on a reasonable belief that it will reveal evidence of the crime of arrest?

One might argue that under *Riley*, a cell phone is not a mere container but a mini-computer, and that under *Chadwick*, a warrant is required to search this item found within the arrestee's reaching distance but subsequently secured in police custody. (See *United States v. Chadwick* (1977) 433 U.S. 1; but see *People v. Nottoli* (2011) 199 Cal. App. 4th 531 [the Sixth District relied on *Arizona v. Gant* and *People v. Diaz* to uphold the warrantless search of the defendant's smart phone, a container that was in the passenger compartment of the defendant's car when he was arrested for being under the influence of a controlled substance].)

III. POST-*RILEY* CASES

California v. Riley was decided just over six months ago, on June 24, 2014. Consequently, in comparison to the post-*Jones* cases, there have been many fewer decisions citing or discussing Riley -- 129 at last count. I concentrated on reading decisions from the California Court of Appeal and the federal circuit courts. I also read some federal district court opinions.

A. IF THE CELL PHONE SEARCH IN YOUR CASE OCCURRED PRIOR TO JUNE 24, 2014: A Warrantless Pre-*Riley* Search of Cell Phone Data May be Unconstitutional Under *Riley*, but Evidence Discovered During or Following That Search Will Not be Suppressed

As expected, the first post-*Riley* cases that reached the California Court of Appeals and the federal district courts involved warrantless searches of the contents of arrestees' cell phones that had been conducted prior to June 24, 2014, the date *Riley* was decided.

1. Pre-*Riley* Searches: California Court of Appeals Cases

There have been at least three California Court of Appeal cases affirming trial court denials of motions to suppress incriminating evidence found when police officers, without a warrant, searched the data files of cell phones seized from defendants at the time of arrest. In all three cases, the cell phone searches were conducted prior to the date of the *Riley* decision (June 24, 2014). *Riley* was decided while the cases were pending on appeal. (See *People v. Macabeo* (2014) 229 Cal. App. 4th 486 [2d Dist., Div. 5; just prior to formal arrest, the officer seized a cell phone from the defendant's pocket, and another officer immediately searched the phone's files, finding incriminating photos]; *Kennedy v. Superior Court* (October 29, 2014) 2014 WL 5468967 [1st Dist., Div. 3; after arresting the defendant, officers searched his person and recovered a cell phone from his pocket; they looked at the phone's data and discovered incriminating text messages]; *People v. Rodriquez* (November 26, 2014) 2014 WL 5509829 [1st Dist., Div. 4; after arresting the defendant, the officer seized the defendant's cell phone from his person, reviewed the contents and found numerous items implicating the defendant in suspected crimes].)

In all three cases, the appellate courts decided that *Riley* applied retroactively, so the warrantless searches of the cell phones' contents were unconstitutional. However, the courts declined to apply the exclusionary rule, because the officers had reasonably relied on *People v. Diaz*, *supra*, 51 Cal. 4th at 84, which had authorized warrantless searches of cell phone data incident to arrest. Pursuant to the rule of *Davis v. United States, supra,* 131 S.Ct. at 2423-24, *Diaz* was found to be binding appellate precedent in effect in California at the time of the three searches.[40]

---

[40] In *Davis v. United States*, the Supreme Court expanded the good-faith exception to the exclusionary rule. The seven-justice majority held that when law enforcement officers conducted a search in objectively reasonable reliance on binding appellant precedent, in effect at the time of the search, the exclusionary rule does not apply even though the search is unconstitutional pursuant to a subsequent Supreme Court decision. (*Davis, supra*, 131 S. Ct. at 2423-24 [Even if the vehicle search incident to arrest was unconstitutional under the rules subsequently set forth in *Arizona v. Gant* (2009) 129 S.Ct. 1710, evidence discovered during that search would not be suppressed as the officers reasonably relied on binding Eleventh Circuit precedent then in effect that authorized the officers' search of the car's passenger compartment following the arrest of a recent occupant in every case].)In her concurring opinion, Justice Sotomayor emphasized that the officer who conducted the search needed to rely on unequivocal settled binding precedent that specifically authorized the particular police practice. (*Davis, supra*, at 2434-35 [conc. opn. of Sotomayor J.].)

The California Supreme Court will ultimately decide if this is a proper application of the *Davis* rule. The Court granted the defendant's Petition for Review in *People v. Macebo*, supra, 229 Cal. App. 4th at 486. The second question presented reads as follows:

> "Did *Riley v. California* [citation omitted] require the exclusion of evidence obtained during the warrantless search of the suspect's cell phone incident to arrest, or did the search fall within the good faith exception to the exclusionary rule (see *Davis v. United States* [citation omitted] in light of *People v. Diaz* [citation omitted]." (*People v. Macebo*, Supreme Court Case No. S221852.)

Of course, by the time the California Supreme Court decides this case, there will be a diminishing number of cases reaching the trial courts and the appellate courts in which the search of the cell phone contents, following arrest, occurred prior to June 2014.[41]

Practice Note: If you have a California case in which a seized cell phone's contents were searched, without a warrant, following an arrest that occurred prior to June 24, 2014, and incriminating evidence was discovered in the phone's data files, do you have any chance of getting this evidence suppressed? Probably not. If the cell phone was

---

[41] In granting the Petition for Review, the Supreme Court listed a second question presented for review in *People v. Macebo*: "May law enforcement officers conduct a search incident to the authority to arrest for a minor traffic offense, so long as a custodial arrest (even for an unrelated crime) follows?" I suspect this issue may be the major reason the Court granted review. This question arose because of Macebo's facts: At approximately 1:30 a.m., two officers stopped the defendant, who was riding a bicycle, because he had failed to make a full stop at a stop sign. Officer #1 acquired the defendant's consent to search his pockets and removed various items, including a cell phone. Officer #2 searched the phone's contents; he found photos showing young girls, under age 18, engaging in sexual activity. Since possession of these photos is a crime, the officers arrested the defendant. Relying on *Atwater v. Lago Vista* (2001) 532 U.S. 318 and *People v. McKay* (2002) 27 Cal. 4th 601, the court held that the officers could have made a custodial arrest of the defendant because they had probable cause he had committed the traffic violation (failure to stop at the sign). Thus, they had the constitutional authority to conduct a search incident to arrest, even though they did not make a formal arrest for this traffic crime. *People v. Diaz*, binding authority in effect at the time of the search, authorized Officer #2's search of the cell phone photos during the search incident to arrest. It did not matter that the defendant was ultimately arrested for possession of matter depicting minors engaged in sexual conduct, based on these photos.

found on the arrestee's person, I don't see any way to argue that *People v. Diaz* was not unequivocal binding appellate precedent authorizinga warrantless search of the cell phone's contents. (See *Davis, supra*, 131 S.Ct. at 2434-35 [conc. opn. of Sotomayor J.].)

If the cell phone was not found on the arrestee, you might argue that *Diaz* did not authorize a warrantless search of the phone's contents. After all, if the cell phone was on the vehicle's front passenger seat or inside a briefcase found in the back of the car, it would not qualify as personal property immediately associated with the person, the rationale adopted in *Diaz* to permit the warrantless search of the phone's data. If the officer has seized and secured the phone before the search, you could argue that the relevant precedent requiring a warrant to explore the cell phone's files is *United States v. Chadwick* (1977) 433 U.S. 1 [invalidated the warrantless search of a 200 pound locked footlocker seized from the area within the arrestee's immediate control, but not searched until 90 minutes after the arrest while securely in police custody]; see also *United States v. Schleis* (8th Cir. 1978) 582 F.2d 1166 [invalidated the delayed warrantless search of a locked briefcase that the defendant had been carrying at the time of arrest; the briefcase was forced open and searched after the defendant was secured in a jail cell].)

However, if the cell phone was discovered in the defendant's vehicle and you make this argument, you may need to discuss *People v. Nottoli* (2011) 199 Cal. App. 4th 531. In *Nottoli*, the Sixth District relied on *Arizona v. Gant*, *supra*, 556 U.S. at 322, to uphold the contemporaneous search of the defendant's cell phone, found in the car's center console, because it was a container found in the passenger compartment of the defendant's car. Pursuant to *Gant*, the passenger compartment, and any containers found therein, could be searched as the officers reasonably believed that evidence of the crime of arrest (being under the influence of a controlled substance) would be found in the car. (*Nottoli, supra*, at 551-559.) The Sixth District noted that under *People v. Diaz*, a cell phone should not be treated any differently than other containers. The court found "no principled reason to distinguish between a cell phone found on an arrestee's person during a search incident to arrest and a cell found in the passenger compartment during a vehicular search incident to arrest." (*Nottoli, supra*, at 558.) In addition to distinguishing *Nottoli* on its facts, you could argue that it was wrongly decided.

2. Pre-*Riley* Searches: Federal District Court Cases

In the six months since *Riley* was decided on June 25, 2014, at least three federal district courts have ruled on requests to suppress evidence found during warrantless cell phone data searches performed following arrest. In these cases, the cell phones were seized from arrestees and searched prior to *Riley*. The district courts found that even if the searches of the cell phones' contents were unconstitutional under *Riley*, the incriminating photos and text messages would not be suppressed under the *Davis* good faith exception,

as the officers had relied on binding appellate authority, in effect at the time of the searches, that authorized the warrantless cell phone searches incident to arrest. (See *United States v. Spears* (July 14, 2014) 2014 WL 3407930 [N.D. Texas; the officers relied on *United States v. Finley* (5th Cir. 2007) 477 F.3d 250, binding precedent which authorized warrantless searches of cell phone contents incident to arrest]; *United States v. Peel* (August 25, 2014) 2014 WL 4230926 [E.D. Cal.; the officers reasonably relied on the California Supreme Court's decision in *People v. Diaz, supra*, 51 Cal. 4th at 501, when they searched the data on the defendant's cell phone at jail following his arrest]; *United States v. Garcia* (September 12, 2014) 2014 WL 4543163 [N.D. Cal; the officers reasonably relied on *People v. Diaz*, when they searched the text messages on the defendant's cell phone, incident to arrest, without obtaining a warrant].)[42]

B. Does the *Riley* Ruling Apply to Searches of Cell Phone Parts or to Other Electronic Devices?

1. *United States v. Lowe* (October 10, 2014) 2014 WL 5106053 [Dist. Ct., D. Nevada, Slip Opinion]: Government officials do not need a warrant to search physical parts of the cell phone for the serial number.

After the defendant was arrested in November 2013, he was taken to jail. His cell phone was among the defendant's personal effects that were lawfully seized during his booking. The phone was stored in the inventory room of the jail where the defendant was held in custody. About two and one-half months later, in February 2014, an officer obtained the cell phone. He removed the phone's back cover, its battery and possibly its memory card, and obtained the phone's serial number. The officer then obtained a warrant to search the contents of the phone. (*Lowe, supra*, at *1, *2, *5, *11,)

The district judge agreed with the magistrate's holding that the officer's actions in removing the cell phone's back cover, battery and memory card in order to get the serial number was not a search requiring a warrant. Because the cell phone was one of the defendant's personal effects, taken from him at the time of arrest, it's physical parts could

---

[42] In *Garcia*, the district court addressed the defendant's argument that unlike a decision from the United States Supreme Court or the Ninth Circuit, the California Supreme Court's *Diaz* decision was not appellate precedent *binding* the federal district court. The court concluded that *Diaz* provided "sufficient binding precedent" as it was squarely on-point and there was not contradictory authority from the Ninth Circuit. Moreover, when the officers arrested the defendant, they were investigating violations of local and state laws and likely anticipated that any prosecution arising out of their investigations would take place in the California state court. (*Garcia, supra*, at *6.)

be examined for inventory purposes. (*Id.*, at *11-*12.) According to the magistrate, *Riley* supported this ruling. In *Riley*, the Court required a warrant to search cell phone data because it contains "sensitive personal information". The cell phone's battery, serial number and the outside of its memory card "do not contain sensitive personal information which would necessitate court protection." After *Riley*, officers are permitted to examine "physical aspects of the phone" for certain purposes. (*Id*., at *12, citing *Riley, supra*, 134 S.Ct. at 2485, 2490.)

2. *United States v. Miller* (July 23, 2014) 2014 WL 3671062 [Dist. Ct., E.D. Mich, Slip Opinion]: Officers do not need a warrant to search images on a digital camera, as a camera is distinguishable from a cell phone.

The police obtained a warrant to search the defendant's residence for evidence of narcotics sales and firearms. While executing this warrant, an officer found a digital camera, turned it on and discovered images of two young girls engaged in sexual acts. These images provided probable cause for two additional warrants; the first warrant authorized a search of the residence for evidence of child pornography possession and production, and the digital camera was seized during this search. A second warrant authorized a search of the camera's contents. Additional images, similar to the first two, were discovered during a thorough search of the camera. (*Miller, supra*, at *1-*2.)

The district court denied the defendant's motion challenging the initial search of the digital camera, revealing the two pornographic images. The defendant relied on *Riley* to assert this search was unconstitutional, as the police had not initially obtained a warrant authorizing examination of the digital camera's images. The court found *Riley* distinguishable and concluded that the camera search did not raise the same privacy concerns. In contrast to cell phones, cameras are unlikely to be used on a daily basis, and "contain a limited type of data, restricted to image and video files, that do not touch the breadth or depth of information that a cell phone's data offers." (*Id.,* at *3-*4.)

3. *People v. Michael E.* (2014) 230 Cal. App. 4th 261 [1st Dist., Div. 2; opinion authored by Kline, P.J.]: The police officers' warrantless search of a flash drive containing videos from the defendant's computer was unconstitutional.

The defendant took his computer into a shop for servicing. While working on the computer, the repair person, Statham, viewed images on the hard drive which showed girls posing in a sexual manner. Believing that these images were pornographic, Statham called the police and Officer Clark responded. The officer looked at these images and concluded that because the young females were not engaging in or simulating sexual activity, the images were not pornography. But Officer Clark asked Statham if he could

"search through and look at" anything else on the computer. Statham found video files he had not previously opened. When directed by Clark to open these files, Statham was unable to do so. Statham put these unopened video files on a USB flash drive. Officer Clark took the flash drive to the police department and with the assistance of another officer, they opened and viewed the videos which depicted pornographic material. The defendant filed a motion to suppress the video files which the trial court denied.

The Court of Appeal, Division Two, reversed the trial court and concluded that the warrantless police search of the video files on the flash drive was unconstitutional. The issue was whether the officers' search of the video files exceeded the scope of the prior private search conducted by Statham when he opened and viewed the initial images. Division Two applied the rule derived from *People v. Wilkinson* (2008) 163 Cal. App. 4th 1554 and *United States v. Runyan* (5th Cir. 2001) 275 F.3d 449: The police exceed the scope of a prior private search when, without obtaining a warrant, they examine a closed container that was not opened by the private searcher, unless the police are substantially certain of what is inside the previously-unopened container before they open it. If the container's contents were viewed or rendered obvious during the private search, then the defendant's expectation of privacy in those contents have been frustrated, and there is no Fourth Amendment violation. Division Two held the officers exceeded the scope of the Statham's private search when they viewed the videos stored on the flash drive. Statham had not viewed these videos and they were not identical to the photographs found by Statham and shown to Clark. Moreover, the officers were not substantially certain of the contents of the video files before opening them. (*Michael E., supra*, at 271-72, 275.)

The trial court found that the video files placed on the flash drive were contained in the defendant's computer hard drive, the functional equivalent of a closed container. Thus, the officers' searches of the videos were simply more thorough searches of the container that Stratham, the private party, had already opened. Any expectation of privacy that the defendant had in the files stored on his hard drive had already been compromised. (*Id.*, at 275-276.) Relying on *Riley*, Division Two rejected the characterization of the computer hard drive as a mere "closed container". Like the cell phone in *Riley*, a standard computer hard drive stores an enormous quantity of personal data; it is the "digital equivalent of its owner's home, capable of holding a universe of private information." (Id., at 276-77, quoting *United States v. Mitchell* (11th Cir. 2009) 565 F.3d 1347, 1351-52.) By taking his computer in for servicing, the defendant did not relinquish his reasonable expectation of privacy in all of that information. (*Id*., at 278-79.)

PART THREE:
INTERESTING AND USEFUL QUOTATIONS

I. THE EFFECTS OF EVOLVING DIGITAL TECHNOLOGY ON INDIVIDUALS' REASONABLE EXPECTATIONS OF PRIVACY: IS THERE A NECESSARY TRADEOFF BETWEEN PRIVACY AND SECURITY, SAFETY OR EFFICIENCY?

In many of these cases, the judges or justices discuss the effects of new digital technology, specifically including smart cell phones with enormous storage capacity and GPS devices allowing accurate location tracking, on the reasonable privacy expectations of people who voluntarily use these devices or are subject to police-initiated GPS searches. Some propose that there is a necessary choice between privacy on one side, and security, safety, and efficient crime detection on the other side. (Digital device users may also face their own tradeoff between privacy and convenience). Here are some interesting quotes on this topic. As you read them, consider: Is this a choice that we, as society members, necessarily need to make? Can we have both privacy and security, safety and convenience?

In *Kyllo v. United States* (2001) 533 U.S. 27, 33-34 [holding that the use of a thermal-imaging device to detect heat emanating from a home is a search requiring a warrant], Justice Scalia stated: **"It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advances in technology."**

In *United States v. Garcia* (7th Cir. 2007) 474 F.3d 994, 998 [holding, prior to *Jones*, that placement of a GPS tracking unit on the underside of a vehicle is not a Fourth Amendment search], Judge Posner wrote:

> **"Of course the [Fourth] amendment cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than the were in the eighteenth. [citation omitted] There is a tradeoff between security and privacy, and often it favors security."**

In his concurring opinion in *United States v. Jones* (2012) 132 S.Ct. 945, 962, Justice Alito proposed that changes in technology could diminish privacy expectations:

> **"[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But dramatic technological changes may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find that tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."**

In her separate concurring opinion in *Jones, supra*, 132 S.Ct. at 957, Justice Sotomayor was not convinced that most people would welcome or accept a diminishment of privacy as the price for security or convenience. She also proposed that it may be necessary, in the digital age, to reconsider the third party doctrine – the idea that individuals relinquish any reasonable expectation of privacy in information that they voluntarily provide to third parties (i.e. cell phone or internet service providers):

> **"More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. [See, e.g. *Smith v. Maryland* (1979) 442 U.S. 735; *United States v. Miller* (1976) 425 U.S. 435.] This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. Perhaps, as Justice Alito notes, some people may find the 'tradeoff" of privacy for convenience 'worthwhile" or come to accept this 'diminution of privacy' as 'inevitable,' [citation omitted], and perhaps not. I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web-site they had visited in the last week, or month, or year. But whatever the social expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."**

In *United States v. Skinner* (6th Cir. 2012) 690 F.3d 772, 777-78 [no Fourth Amendment search occurred when the police acquired GPS information from the defendant's cell phone provider to track his movements], Judge Rogers acknowledged that cell phone and GPS technology have provided police the means for more efficient location tracking, compared to visual surveillance. These technological advances should help the police, not the criminals:

> **"There is no inherent constitutional difference between trailing a defendant and tracking him via technology. Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."**

In *Riley v. California* (2014) 134 S.Ct. 2473, 2493, Chief Justice Roberts took the opposite position. He acknowledged that protecting privacy may necessarily impede law enforcement efficiency, and this tradeoff in favor of privacy is worth the cost:

> **"We cannot deny that our decision today will have an impact on the ability of law enforcement to combat crime. Cell phones have become important tools in facilitating coordination and communication among members of criminal enterprises, and can provide valuable incriminating information about dangerous criminals. Privacy comes at a cost."**

II. THE RECOGNITION THAT GPS DEVICES AND CELL PHONES ARE DIFFERENT FROM THEIR PRE-DIGITAL ANALOGS: GPS LOCATION TRACKING IS DIFFERENT THAN VISUAL SURVEILLANCE, AND CELL PHONES ARE NOT LIKE WALLETS, ADDRESS BOOKS OR PURSES

In *United States v. Jones, supra*, 132 S.Ct. at 945, despite Justice Scalia's insistence on analogizing a GPS device hidden on the underside of the defendant's vehicle to "a constable concealing himself in the target's coach in order to track it's movements." (*Id*, at 950, fn. 3.), Justice Alito rejected both this 18th Century analog and the idea that GPS tracking is equivalent to police visual surveillance, even if aided by beepers. Alito explained that before GPS, it would not have been practical for the police to track a suspect's movements in his vehicle 24/7 for four weeks (*Id.*, at 963-64):

> **"In the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical. Traditional**

surveillance for any extended period of time was difficult and costly and therefor rarely undertaken. The surveillance at issue in this case – constant monitoring of the location of a vehicle for four weeks – would have required a large team of agents, multiple vehicles, and perhaps ariel assistance. Only an investigation of unusual importance would have justified such an expenditure of law enforcement resources. Devices like the one used in the present case, however, make long-term monitoring relatively easy and cheap."

Justice Alito then explained why GPS devices, in contrast to the more primitive beepers, make long-term location monitoring possible. The two types of devices are not equivalent, as beeper tracking must be aided by visual surveillance. (*Id.*, at 963, fn. 10):

"Even with a radio transmitter like those used in [*Knotts* and *Karo*], such long-term surveillance would have been exceptionally demanding. The beepers used in those cases merely 'emit[ted] periodic signals that [could] be picked up by a radio receiver.' [citation omitted] The signal had a limited range and could be lost if the police did not stay close enough."[43]

In her concurring opinion in *Jones, supra*, 132 S.Ct. at 955-56, Justice Sotomayor explained in detail why, unlike intermittent visual surveillance of a subject's discrete trips on public roads, the long-term location tracking made possible by GPS invades the subject's reasonable expectations of privacy. The idea behind this "mosaic theory" is that the government learns more about a person's associations, habits and beliefs by tracking their movements over time than one learns from hours or even a day of surveillance:

" GPS monitoring generates a precise, comprehensive record of a person's public movements that reflect a wealth of detail about her familial, political, professional, religious and sexual associations. 'Disclosed in [GPS] data ... will be trips the indisputably private nature [which take] little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney,

---

[43] For further discussion of why "beepers and GPS devices are not one and the same", see Judge Thacker's dissenting opinion in *United States v. Stephens* (2014) 764 F.3d 327, 342, fn. 4: "The two are of an entirely different character. A beeper tracking device requires law enforcement to at least be in proximity to the device to receive the transmitted signal, whereas a GPS device downloads location data at specific time intervals with no proximity needed."

the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on'. [citation omitted]. The government can store such records and efficiently mine them for information years into the future ... The net result is that GPS monitoring - by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the government, in its unfettered discretion, chooses to track - may 'alter the relationship between citizen and government in a way that is inimical to democratic society.' [citation omitted] I would take these attributes of GPS monitoring into account when considering the existence of one's reasonable expectation of privacy in the sum of one's public movements. I would ask whether people reasonable expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."

In *Riley v. California, supra*, 134 S.Ct. 2473, 2488, Chief Justice Roberts firmly rejected the government's claim that a cell phone is materially indistinguishable from a cigarette pack, a wallet or a purse – items found on arrestees that may be searched without a warrant, incident to arrest, because they are immediately associated with his person:

"That is like saying a ride on horseback is materially distinguishable from a flight to the moon. Both are ways of getting from Point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet or a purse."

Because of the vast amount of private information that a user stores on a modern smart phone, Roberts believed that the better analogy was to computers (*Id.*, at 2489.):

"Cell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand, many of the devices are in fact minicomputers that also happen to have the capacity to be used as a telephone."

Or perhaps, Chief Justice Roberts continued, a cell phone is more like a house, which is afforded the highest degree of Fourth Amendment protection. (*Id*., at 2491.):

> **"Indeed, a cell phone search would typically expose to the government far *more* than the most exhaustive search of a house."**

In distinguishing cell phones from conventional small containers carried on one's person, Roberts emphasized the vast amount of diverse and often personal information stored on a cell phone that can fit in the user's hand. (*Id*., at 2489.):

> **"One of the most notable distinguishing features of modern cell phone is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy. [Citation omitted] Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read - nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in *Chadwick, supra*, rather than a container the size of the cigarette package in *Robinson* ... Even the most basic phones that sell for less than $20 hold photographs, picture messages, text messages, Internet browsing history, a calendar, a thousand-entry phone book, and so on."**

In *Riley*, Chief Justice Roberts used an analysis similar to Justice Sotomayor's "mosaic theory" in *Jones*. He emphasized that viewing all of the cell phone's data files together, rather than in isolation, could reveal a great deal about the phone user's private life, interests and associations (*Id.*, at 2489.):

> **"The storage capacity of cell phones has several interrelated consequences for privacy. First, a cell phone collects in one place many distinct types of information – an address, a note, a [medical] prescription, a bank statement, a video – that reveal much more in combination than any isolated record. Second, a cell phone's capacity allows even just one type of information to convey far more than previously possible. The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on the phone can date back to the**

purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all of his communications with Mr. Jones for the past several months, as would routinely be kept on his phone."

Finally, Roberts emphasized the pervasiveness of cell phones in modern society. (*Riley, supra*, at 2490.):

"A decade ago police officers searching an arrestee might have occasionally stumbled upon a highly personal item such as a diary. But those discoveries were likely to be few and far between. Today, by contrast, it is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives – from the mundane to the intimate."

In *People v. Michael E.* (2014) 230 Cal. App. 4th 261, 276-77 [1st Dist., Div. 2], Justice Kline relied on *Riley* to reject the government's assertion that a computer hard drive was the functional equivalent of a pre-digital closed container. He noted that like a cell phone, a standard computer hard drive stores an enormous quantity of personal data, and is the "digital equivalent of the owner's home." Justice Kline commented on how traditional Fourth Amendment analysis would need to adjust to the realities of new technologies. (*Id*., at 277.):

"The Supreme Court's analysis in *Riley* highlights the dangers inherent in lawyers and judges cavalierly applying established legal theories to new technologies, without carefully exploring the factual differences between such technologies and the objects traditionally found appropriate for those theories' application. As the Tenth Circuit Court of Appeals has observed: 'Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method ... [r]elying on analogies to closed containers or file cabinets may lead courts to oversimplify a complex area of Fourth Amendment doctrines and ignore the realities of massive modern computer storage'." [citing *United States v. Carey* (10th Cir. 199) 172 F.3d 1248, 1275.]