Digital Privacy in the Post-*Riley* World

by Teresa Reed (Stanford Law School '15)

I. Fourth Amendment Issues

A. GPS Tracking

1. **Physical attachment / trespass**: "We hold that the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search." *United States v. Jones*, 132 S. Ct. 945, 949 (2012). Thus, in applying *Jones*, lower courts assess the threshold question whether a defendant has Fourth Amendment standing to challenge the placement of a GPS device on the vehicle in question. If so, then the physical attachment of the device constitutes a search. On the other hand, "a defendant who does not have either a lawful ownership interest, or a possessory interest in a searched automobile at the time of the search does not possess a legitimate expectation of privacy that the Fourth Amendment will protect." *United States v. Houseal*, 2014 WL 626765, at *6 n.11 (W.D. Ky. Feb. 18, 2014) (cataloguing cases).
2. **No trespass:** Where no physical trespass occurred, courts look to Justice Alito's concurrence in *Jones*, which (together with Justice Sotomayor's concurrence) spoke for five Justices to find that GPS tracking constitutes a search based solely upon the reasonable expectation of privacy test articulated in *Katz v. United States*, 389 U.S. 347 (1967). "The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).
    a. **Long-term tracking:** "[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy." *Id.* (Alito, J., concurring); *see also id.* at 955 (Sotomayor, J., concurring) (same).
    b. **Short-term tracking:** "[R]elatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable . . . We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark." *Id.* at 964 (Alito, J., concurring)*; see also id.* at 955 (Sotomayor, J., concurring) ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention").
        i. In general, lower courts reason that monitoring periods of one week or less are allowed by Justice Alito's approval of "[r]elatively short-term monitoring." *See United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012) (three days); *United States v. Devora*, 2015 WL 1621396, at *4 (W.D. Tex. Apr. 9, 2015) ("a matter of hours"); *United States v. Ruibal*,

2014 WL 357298 (W.D. Mich. Jan. 31, 2014) (two days); *United States v. Luna-Santillanes*, 2012 WL 1019601 (E.D. Mich. Mar. 26, 2012) (one day); *People v. Barnes*, 216 Cal. App. 4th 1508, (2013) (one evening); *People v. Hall*, 2013 WL 3776340, at *5 (Cal. Ct. App. July 17, 2013) ("nearly negligible one-week use of GPS monitoring," supplemented by live surveillance).

ii. For cases noting that longer time periods implicated the concerns in *Jones*, see *United States v. White*, 2014 WL 6682645, at *5 (E.D. Mich. 2014) ("[T]he length [30 days] and breadth of the tracking here extends well beyond what any reasonable person might anticipate"); *United States v. Powell*, 943 F. Supp. 2d 759 (E.D. Mich. 2013) (same, for a monitoring period of seven months); *United States v. Lopez*, 895 F. Supp. 2d 592, 601 (D. Del. 2012) (tracking for seventeen days within a four-month period was "not so distinguishable from the timeframe detailed in *Jones* as to render [defendant's] monitoring decidedly 'short-term'").

iii. Departing from this approach, the Florida Supreme Court ruled in *Tracey v. State* that the warrantless use of cell site location information to track an individual during the course of a single day's car trip violated the Fourth Amendment. 152 So. 3d 504, 525 (2014). The court refused to tether its reasoning to the temporal length of the monitoring, which in its view was "not a workable analysis." *Id.* at 520. Rather, the court emphasized that an earlier case allowing police monitoring, *United States v. Knotts*, 460 U.S. 276 (1983), was not applicable because when *Knotts* was decided, "high tech tracking such as now occurs was not within the purview of public awareness or general availability." 152 So.3d at 525.

B. Cell Phones and Other Digital Devices

1. Without a warrant

a. Incident to arrest: *Riley v. California*, 134 S. Ct. 2473 (2014), held that the search-incident-to-arrest doctrine does not allow warrantless searches of the digital contents of cell phones incident to arrest. The Supreme Court recognized that "[c]ellphones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person." *Id.* at 2489. *Riley*, therefore, suggests that "digital is different" in the Fourth Amendment context – that is, that older cases developed in the context of physical objects should not control the Fourth Amendment's application to electronic information.

i. Cell phones and other computers: In differentiating cell phones from physical objects, *Riley* did not explicitly establish what other electronic devices might fall within its

scope. However, courts have little trouble extending *Riley*'s reasoning to other computers. *See, e.g.*, *People v. Michael E.*, 230 Cal. App. 4th 261, 277 (2014) ("[A]s the Supreme Court observed, cell phones 'are in fact minicomputers,' and the search of a computer hard drive implicates at least the same privacy concerns as those implicated by the search of a cell phone . . . ." (citing *Riley*, 134 S. Ct. at 2489)).

ii. **Cameras:** Courts disagree about whether *Riley* applies to digital cameras. *See Am. News & Info Servs., Inc. v. Gore*, 2014 WL 4681936, at *10 (S.D. Cal. Sept. 18, 2014) (video cameras "fall somewhere between the physical search of a cigarette package found in a pocket [in *United States v. Robinson*, 414 U.S. 218 (1973)] . . . and the data search of a cell phone under *Riley*"). *Compare United States v. Whiteside*, 2014 WL 4928951, at *2 (S.D.N.Y. Oct. 1, 2014) (*Riley*'s "rationale appears to be equally applicable to searching the content of digital cameras given their storage capacity and labeling (time/date/location capabilities)"), *with United States v. Miller*, 2014 WL 3671062, at *3 (E.D. Mich. July 23, 2014) ("[T]he search of Defendant's camera does not raise the same privacy concerns as a cell phone.").

iii. **GPS device:** One state appellate court applied *Riley* to the contents of a GPS device found on an arrestee's person. *State v. Clyburn*, 2015 WL 1528909, at *5 (N.C. Ct. App. Apr. 7, 2015) ("The type of data that may be found on a GPS device was specifically mentioned by the *Riley* Court in distinguishing the digital data that can be stored on a cell phone from the type of data that is typically stored in physical records found on one's person.").

iv. **Key fob:** Defendants have also argued that police use of garage openers or key fobs may require a warrant after *Riley*, though no court has yet agreed. *See United States v. Williams*, 773 F.3d 98, 104 (D.C. Cir. 2014) (defendant waived argument); *United States v. Correa*, 2015 WL 300463, at *1 (N.D. Ill. Jan. 21, 2015).

b. **Exigent circumstances:** *Riley* noted that, "case-specific exceptions may still justify a warrantless search of a particular phone." 134 S. Ct. at 2494. The exigent circumstances exception, for example, could cover "the need to prevent the imminent destruction of evidence in individual cases, to pursue a fleeing suspect, and to assist persons who are seriously injured or are threatened with imminent injury." *Id.*

i. **Encryption:** Dismissing the government's argument that remote wiping or data encryption justified routine searches of cell phones incident to arrest, the *Riley* Court

nevertheless observed that if "the potential loss of evidence" truly constitutes a " 'now or never' situation . . . [police] may be able to rely on exigent circumstances to search the phone immediately." 134 S. Ct. at 2488 (quoting *Missouri v. McNeely*, 133 S. Ct. 1552, 1562 (2013)). Lower courts read this suggestion narrowly, finding that speculative concerns about data preservation do not ordinarily implicate the exigent circumstances exception. *See United States v. Camou*, 773 F.3d 932 (9th Cir. 2014); *United States v. Alonso-Castaneda*, 2015 WL 1711989, at *7 (D. Ariz. Apr. 15, 2015) (scope of search went beyond what was permissible "to prevent the loss of call data"); *Carter v. State*, 2015 WL 1905914 (Tex. App. Apr. 27, 2015); *State v. Lacey*, 2015 WL 359249, at *2 (Iowa Ct. App. Jan. 28, 2015) (no "specific, articulable facts" to support the government's contention that a second suspect could have destroyed digital evidence while a warrant was obtained); *Oliver v. State*, 2015 WL 1933389, at *4 (Tex. App. Jan. 22, 2015) ("Appellant had no opportunity to delete data himself once the phone was seized.").

ii. **Probationer / parolee search exception:** Lower courts agree that the exceptions articulated in *United States v. Knights*, 543 U.S. 112 (2001), and *Samson v. California*, 547 U.S. 843 (2006), allowing searches of probationers and parolees without probable cause, continue to apply to cell phones after *Riley*. *See United States v. Dahl*, 2014 WL 6792676, at *5 (E.D. Pa. Dec. 3, 2014); *United States v. Martinez*, 2014 WL 3956677 (N.D. Cal. Aug. 12, 2014); *State v. Gonzalez*, 2015 WL 1913109 (N.D. Apr. 28, 2015); *People v. Purdie*, 2014 WL 4261692 (Cal. Ct. App. Aug. 29, 2014).

iii. **Other exceptions:** One lower court allowed the warrantless search of a cell phone under *Riley*'s express recognition of the exception "to pursue a fleeing suspect." *State v. Samalia*, 344 P.3d 722, 726 (Wash. Ct. App. 2015) (also finding that the state's exception to the warrant requirement for voluntarily abandoned property applied to the phone).

c. Border searches: Border searches are historically "reasonable simply by virtue of the fact that they occur at the border." *United States v. Ramsey*, 431 U.S. 606, 616 (1977). Pre-*Riley*, the Ninth Circuit excluded computers from this rule, requiring reasonable suspicion for the examination of a hard drive at the border. *United States v. Cotterman*, 709 F.3d 952 (9th Cir. 2013) (en banc).

i. Some lower courts have rejected the argument that *Riley* affected the border search exception, even as they followed *Cotterman* by requiring reasonable suspicion for digital searches at the border. *See United States v. Blue*, 2015 WL 1519159, at *2 (N.D. Ga. Apr. 1, 2015) (upholding search of computer based on reasonable suspicion, but finding "no authority" for the proposition that *Riley* changed border search law); *United States v. Saboonchi*, 48 F. Supp. 3d 815 (D. Md. 2014) (declining to reconsider prior decision, which upheld search of digital devices based on reasonable suspicion, in light of *Riley*).

ii. In contrast, the D.C. District Court has relied in part on *Riley* to suppress evidence from a laptop search at the border. The court found that, after *Riley*, "the analysis of whether the search of [the] laptop was reasonable under the Fourth Amendment does not simply end with the invocation of . . . the well-recognized border exception." *United States v. Kim*, 2015 WL 2148070, at *19 (D.D.C. May 8, 2015). Rather, "[a]pplying the *Riley* framework, the national security concerns that underlie the enforcement of export control regulations at the border must be balanced against the degree to which Kim's privacy was invaded in this instance." *Id.* at *20.

2. **With a warrant / particularity requirement:** In the briefs in *Riley*, the United States asserted that the Fourth Amendment's particularity requirement did not mean that cell phone warrants would specify which files, dates, attachments, or links could be searched. U.S. Br. 24. The *Riley* Court did not address these arguments directly, but did observe that government protocols to avoid overbroad cell phone searches were "[p]robably a good idea" – though not sufficient to eliminate possible Fourth Amendment violations in the execution of warrantless searches. 134 S. Ct. at 2491.

   a. Post-*Riley*, some lower courts have rigorously applied the Fourth Amendment's particularity requirement to cell phone warrants. *See, e.g.*, *United States v. Russian*, 2015 WL 1863333 (D. Kan. Apr. 23, 2015) (court could not conclude that warrant simply authorizing seizure of cell phones was sufficiently particular); *United States v. Winn*, 2015 WL 553286 (S.D. Ill. Feb. 9, 2015) (warrant that failed to specify the categories, characteristics, and time frame of the data for which the police had probable cause was overbroad); *State v. Henderson*, 854 N.W.2d 616, 634 (Neb. 2014) (warrant allowing search of "[a]ny and all" content did not meet particularity requirement). In particular, the District Court of Kansas has applied the particularity requirement by demanding search protocols in cell phone warrants that (1) avoid "the overseizure of data and indefinite storage of data that [the

government] lacks probable cause to seize" and (2) provide a "meaningful description of the scope of the search [the government] is requesting to be authorized." *In re Nextel Cellular Telephone*, 2014 WL 2898262 (D. Kan. June 26, 2014), at *10-13; *see also In re Cellular Telephones*, 2014 WL 7793690 (D. Kan. Dec. 30, 2014); *In re Search of Premises Known as Three Cellphones & One Micro-SD Card*, 2014 WL 3845157 (D. Kan. Aug. 4, 2014).

b. Other courts have not been so eager to mandate specific limits in warrants for digital content.

i. The Sixth Circuit recently approved a warrant that authorized "the search for any records of communication, indicia of use, ownership, or possession, including electronic calendars, address books, e-mails, and chat logs," because "[a]t the time of the seizure . . . the officers could not have known where this information was located in the phone or in what format." *United States v. Bass*, 2015 WL 1727290, at *4 (6th Cir. Apr. 15, 2015); *see also Hedgepath v. Com*, 441 S.W.3d 119, 130 (Ky. 2014) (warrant specifying "cell phones" was sufficiently particular). For a lengthier discussion, see *United States v. Garcia-Alvarez*, 2015 WL 777411, at *2-5 (S.D. Cal. Feb. 24, 2015) (rejecting defendant's arguments that warrant was insufficiently particular because it was not limited to recent data and did not specify a methodology).

ii. Some courts anticipate that *Riley* forecasts future elaboration of protocols or particularity for digital data, but nevertheless read the opinion itself quite narrowly. *See, e.g.*, *United States v. Leora*, 2014 WL 5859072, at *71 (D.N.M. Oct. 20, 2014) ("Although [*Riley*] may indicate the Supreme Court's willingness to provide greater Fourth Amendment protections in the ESI [electronically stored information] context in the future, the Court finds it difficult to conclude that such increased protections are either necessary or required under current Supreme Court precedent."); *United States v. Lustyik*, 2014 WL 4802911, at *16 (S.D.N.Y. Sept. 29, 2014) (rejecting defendants' demand for search protocols, but observing that "the threats to privacy posed by digital searches . . . may eventually make digital search protocols a Fourth Amendment necessity.").

C. Cell Site Location Information: Cell phone service providers maintain records of calls made or received by a customer and of the particular cell tower that carried the call to or from the customer. Courts thus must grapple with whether police can invoke § 2703(d) of the Stored Communication Act to obtain that cell

site location information from third-party service providers upon a mere showing of "reasonable grounds," without a warrant based upon probable cause.

1. Pre-*Riley*, many lower courts found that cell phone users had no reasonable expectation of privacy in cell site records and allowed the government to access those records without a warrant. *See In re Application of U.S. for Historical Cell Site Data*, 724 F.3d 600, 613 (5th Cir. 2013) ("Cell phone users, therefore, understand that their service providers record their location information when they use their phones at least to the same extent that landline users in *Smith* [*v. Maryland*, 442 U.S. 735 (1979)] understood that the phone company recorded the numbers they dialed."); *United States v. Moreno-Nevarez*, 2013 WL 5631017 (S.D. Cal. Oct. 2, 2013); *United States v. Graham*, 846 F. Supp. 2d 384, 404 (D. Md. 2012) (pending on appeal in the Fourth Circuit); *see also United States v. Thousand*, 558 Fed. Appx. 666, 670 (7th Cir. 2014) ("We have not found any federal appellate decision accepting [defendant]'s premise that obtaining cell-site data from telecommunications companies . . . raises a concern under the Fourth Amendment.").

- **a.** For courts holding the opposite, see *In re Application of the United States for an Order Pursuant to 18 U.S.C. § 2703(d)*, 2012 WL 3260215 (S.D. Tex. July 30, 2012); *In the Application of the United States for an Order Authorizing the Release of Historical Cell-Site Information*, 809 F. Supp. 2d 113 (E.D.N.Y. 2011); *Commonwealth v. Augustine*, 4 N.E.3d 846 (Mass. 2014).
- **b.** For an intermediate approach, see *In re Application of U.S. for an Order Directing a Provider of Electronic Communication Service to Disclose Records*, 620 F.3d 304, 320 (3d Cir. 2010) (magistrates can properly grant court orders to obtain cell tower information on a showing less than probable cause, but also have the power "to be used sparingly" to require the government to show probable cause).

2. Thus far, courts have declined to interpret *Riley* as dictating Fourth Amendment protection for cell site information. *See United States v. Davis*, 2015 WL 2058977, at *16 n.19 (11th Cir. May 5, 2015) (en banc) (dismissing defendant's argument that *Riley* applies to cell tower data because "[i]t is not helpful to lump together doctrinally unrelated cases that happen to involve similar modern technology"); *United States v. Guerrero*, 768 F.3d 351, 360 (5th Cir. 2014) (*Riley* did not disrupt the Fifth Circuit's precedent holding that cell site location data is not protected by the Fourth Amendment, although it may "one day lead the Court to treat historical cell site data in the possession of a cellphone provider differently from a pen register in the possession of a pay phone operator"); *United States v. Epstein*, 2015 WL 1646838 (D.N.J. Apr. 14, 2015) (holding that "*Riley* did not address the constitutionality of utilizing § 2703(d) to obtain historical cell site location data from *third-party* cell phone providers," and cataloguing cases that agree); *United*

States v. Dorsey, 2015 WL 847395 (C.D. Cal. Feb. 23, 2015) (district courts in the Ninth Circuit have "universally decided that historical cell site information may be obtained pursuant to a § 2703(d) order without a showing of probable cause"); *United States v. Shah*, 2015 WL 72118 (E.D.N.C. Jan. 6, 2015); *United States v. Rogers*, 2014 WL 5152543 (N.D. Ill. Oct. 9, 2014); *United States v. Giddins*, 2014 WL 4955472 (D. Md. Sept. 30, 2014); *Commonwealth v. Rosario*, 32 Mass. L. Rptr. 414 (2014) ("There is no suggestion in *Riley* that the Court intended to limit third-party doctrine in any respect."); *Ford v. State*, 444 S.W.3d 171 (Ct. App. Tex. 2014). *But see United States v. Cooper*, 2015 WL 881578, at *6 (N.D. Cal. Mar. 2, 2015) (finding that, post-*Riley*, *Smith* cannot be applied to cell site data because "the pen registers employed in 1979 bear little resemblance to their modern day counterparts," but applying the good-faith exception).

II. Fifth Amendment/Passwords

A. Written Password: Both the State and the United States argued in *Riley* that police officers need to search smart phones promptly, especially if found unlocked, because a password could kick in and permanently block access. U.S. Br. 11; Resp. Br. 34-35. Petitioner responded that this argument would only hold true if – among other things – law enforcement could not compel arrestees to disclose their passwords. Reply Br. 14 & n.8.

1. Lower courts have applied the "foregone conclusion" doctrine and find no Fifth Amendment protection for passwords "[w]here the existence and location of the [information that would be compelled is already] known to the government." *In re Boucher*, 2009 WL 424718 (D. Vt. Feb. 19, 2009) (citing *Fisher v. United States*, 425 U.S. 391, 411 (1976)); *see also United States v. Gavegnano*, 305 Fed. Appx. 954, 956 (4th Cir. 2009) ("Any self-incriminating testimony that he may have provided by revealing the password was already a 'foregone conclusion' because the Government independently proved that Gavegnano was the sole user and possessor of the computer."); *United States v. Fricosu*, 841 F. Supp. 2d 1232 (D. Colo. 2012); *Com v. Gelfgatt*, 11 N.E.3d 605 (Mass. 2014) (compelling defendant to enter encryption key does not violate Fifth Amendment); *Order Granting Ex Parte Request for Reconsideration of the United States's Application Under the All Writs Act* at 3, No. 13-M-449 (E.D. Wis. May 21, 2013).

a. For cases holding that the Fifth Amendment does apply to password disclosure or decryption, see *In re Grand Jury Subpoena Duces Tecum*, 670 F.3d 1335, 1349 (11th Cir. 2012) ("[T]he explicit and implicit factual communications associated with the decryption and production are not foregone conclusions."), and *United States v. Kirschner*, 823 F. Supp. 2d 665, 669 (E.D. Mich. 2010) ("[T]he government is . . . seeking testimony from the Defendant, requiring him to divulge through his mental processes his password.")

2. Consensus has not emerged on this issue. *See, e.g.*, *United States v. Bondo*, 2015 WL 1518987, at *6 (A.F. Ct. Crim. App. Mar 18, 2015) ("We leave as unresolved whether a properly issued warrant may compel a suspect to produce a password.").
    a. In one instance, a district court applied the All Writs Act to order a cell phone manufacturer to unlock the cell phone, disregarding the Fifth Amendment issue entirely. *In re XXX, Inc.*, 2014 WL 5510865 (S.D.N.Y. Oct. 31, 2014).
    b. In other cases, officers have obtained cell passwords merely by asking for them. *See, e.g.*, *United States v. Furman*, 2015 WL 1061956, at *2 (D. Minn. Mar. 11, 2015) ("Defendant initially refused the request, but ultimately provided the password . . . ."); *United States v. Graham*, 2014 WL 2922388 (N.D. Ga. June 27, 2014); *Riley*, Reply Br. at 14 (listing cases).

B. Fingerprints: Smart phone owners today can elect to use a fingerprint scan instead of a traditional password to unlock their phones. This prompts the question whether the Fifth Amendment applies to biometric authentication of digital devices.

1. Under current precedents, the Fifth Amendment does not protect biometric information – a fingerprint, voiceprint, or facial recognition – as testimonial. *See* John Larkin, *Compelled Production of Encrypted Data*, 14 Vand. J. Ent. & Tech. L. 253, 278 n.128 (2012) (citing Supreme Court cases disavowing Fifth Amendment protection for handwriting, voice exemplars, and blood tests); *see also Virginia v. Baust*, 2014 WL 6709960, at *3 (Va. Cir. Ct. Oct. 28, 2014) ("The fingerprint, like a key, does not require the witness to divulge anything through his mental processes.").
2. Some scholars argue that the Fifth Amendment doctrine must evolve to cover biometric identification or its constitutional protection will be unduly eroded. *See, e.g.*, Erin M. Sales, *The "Biometric Revolution": An Erosion of the Fifth Amendment Privilege to Be Free From Self-Incrimination*, 69 U. Miami L. Rev. 193, 231 (2014); Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, U. Penn. J. of Const. L. (2012).

III. Exclusionary Rule

A. Officers' Actions Consistent with Then-Binding Precedent

1. **Within same court system:** The Court in *Davis v. United States* held that "searches conducted in objectively reasonable reliance on binding appellate precedent are not subject to the exclusionary rule." 131 S. Ct. 2419, 2423 (2011). Defendants seeking to suppress digital evidence, even in the wake of recent case law that renders police action unconstitutional, must therefore overcome the argument that *Davis*'s good-faith exception applies.
2. **Within same jurisdiction but state court precedent:** Courts disagree as to whether the relevant "appellate precedent" under *Davis* must come

from the same court system. One California district court applied *Davis* based on precedent from the California Supreme Court, despite observing that "[i]t might be a different question if [the precedent] were not so squarely on-point, if the decision had been issued by an intermediate state court of appeal, or if there were contradictory authority in the Ninth Circuit that made the question . . . unsettled in California [at the time of police action]." *United States v. Garcia*, 2014 WL 4543163, at *6 (N.D. Cal. Sept. 12, 2014). The court also acknowledged that a leading treatise "suggest[s] that for *Davis* to apply, the precedent must be binding 'in the jurisdiction of ultimate prosecution.'" *Id.* (*quoting* W. LaFave, 1 Search & Seizure § 1.3(h)). *But see United States v. Eisenhour*, 2014 WL 4206884, at *3 (D. Nev. Aug. 25, 2014) (declining to apply the good-faith exception after *Riley* because "[n]o Ninth Circuit case explicitly rules that digital data on a cell phone can be searched incident to arrest").

B. General Supreme Court Precedent: Courts splinter over whether older Supreme Court cases not directly on-point can trigger the good-faith exception, or whether *Davis*' *on-point* precedent rule is the only way to trigger the exception. For a helpful discussion, see *United States v. Aguiar*, 737 F.3d 251, 260-261 (2d Cir. 2013). *See also United States v. Robinson*, 903 F. Supp. 2d 766, 784 (E.D. Miss. 2012) (reading *Davis* as expressly limited to "binding" as opposed to "generally accepted" authority, and to precedent that "specifically *authorizes* a particular police practice" (quoting *Davis*, 131 S. Ct. at 2429)); Petition for Certiorari, *Stephens v. United States*, 764 F.3d 327 (4th Cir. 2014) (No. 14-1313), 2015 WL 2062483 (reviewing varied conceptions of *Davis* in lower court opinions treating GPS tracking). In tackling this issue, courts often overlook that this Court held in *United States v. Johnson*, 457 U.S. 537, 561 (1982), that suppression is the appropriate remedy when officer make a mistake absent a third-party directive concerning an "unsettled" issue of law. Applying the exclusionary rule in these circumstances, the Court explained, provides "an incentive to err on the side of constitutional behavior." *Id.*; *see also Davis*, 131 S. Ct. at 2435 (Sotomayor, J., concurring) ("when police decide to conduct a search or seizure in the absence of case law (or other authority)" exclusion has a deterrent role to play).

1. **GPS tracking:** *United States v. Knotts*, 460 U.S. 276 (1983), rejected a Fourth Amendment challenge to police use of a beeper to monitor the defendant on public roads. *See also United States v. Karo*, 468 U.S. 705 (1984) (approving *Knotts*, though finding that beeper monitoring in a private residence violates the Fourth Amendment). Courts are split over whether *Knotts* and *Karo* justify application of the good-faith exception to pre-*Jones* GPS tracking. For courts holding that *Davis* applies, see *United States v. Katzin*, 769 F.3d 163 (3d Cir. 2014) (en banc); *United States v. Stephens*, 764 F.3d 327 (4th Cir. 2014); *United States v. Brown*, 744 F.3d 474 (7th Cir. 2014); *United States v. Aguiar*, 737 F.3d 251 (2d Cir. 2013); *United States v. Sparks*, 711 F.3d 58 (1st Cir. 2013). For courts holding the opposite, see *State v. Adams*, 763 S.E.2d 341 (S.C. 2014); *State v. Hohn*, 321 P.3d 799 (Kan. App. 2014); *State v. Mitchell*,

323 P.3d 69 (Ariz. App. 2014); *People v. LeFlore*, 996 N.E.2d 768 (Ill. App. 2013).

2. **Cell phone and computer data:** Similarly, courts are beginning to grapple with whether cell phone searches conducted before *Riley* are covered by the good-faith exception in light of *United States v. Robinson*, 414 U.S. 218 (1973), which established the broad search incident to arrest exception for physical objects. *Compare United States v. Caldwell*, 2015 WL 179583 (E.D. Tenn. Jan. 14, 2015) (*Robinson* and progeny, "in combination with the decisions of most courts to have addressed the issue of a cell phone search incident to arrest at that time . . . render the actions of Officer Patterson objectively reasonable"); *People v. Gonzales*, 2015 WL 1543511 (Cal. Ct. App. Jan. 14, 2015) (good-faith reliance on *Robinson* justifies applying *Davis* to a cell phone search conducted before binding state precedent was decided), *with United States v. Garcia*, 2014 WL 4543163, at *6 (N.D. Cal. Sept. 12, 2014) ("The purposes of, and expectations surrounding, a cigarette pack and a cell phone are so different that it cannot reasonably be said that a case permitting the search of one object 'specifically authorized' the search of the other, particularly given that cell phones were not even a glint in the eye of the courts in 1973.").
3. **Cell site location information:** Courts analyzing whether *Davis* applies to police access to cell site data might rely on *Smith v. Maryland*, which held that the installation of a pen register was not a search because callers voluntarily exposed the numbers they dialed to the third-party telephone company, 442 U.S. 742 (1979). *See United States v. Davis*, 2015 WL 2058977 (11th Cir. May 5, 2015); *People v. Moorer*, 959 N.Y.S.2d 868 (N.Y. Co. Ct. 2013) (reviewing *Karo*, *Knotts*, *Smith*, and *Jones* to determine that "the unsettled state of federal decisional law in this area" made pinging defendant's cell phone to obtain its location reasonable under *Davis*). More often, where officers acted in accordance with the Stored Communications Act, courts do not address *Davis* but instead apply the good-faith exception under *Illinois v. Krull*, which held that the exclusionary rule does not apply when officers obtain evidence in "objectively reasonable reliance on statute," 480 U.S. 340 (1987). *See, e.g.*, *United States v. McCullough*, 523 Fed. Appx. 82 (2d Cir. 2013); *United States v. Epstein*, 2015 WL 1646838 (D.N.J. Apr. 14, 2015); *United States v. Dorsey*, (C.D. Cal. Feb. 23, 2015); *United States v. Giddins*, 2014 WL 4955472 (D. Md. 2014); *United States v. Ashburn*, 2014 WL 7403851 (E.D.N.Y. 2014); *United States v. Caraballo*, 963 F. Supp. 2d 341 (D. Vt. 2013); *United States v. Booker*, 2013 WL 2903562 (N.D. Ga. June 13, 2013); *United States v. Muniz*, 2013 WL 391161 (S.D. Tex. Jan. 29, 2013).