2015

De-Clawing Katz: Emerging Technology and the Exclusionary Rule

Samuel C. Cole

Follow this and additional works at: https://scholar.smu.edu/scitech

Recommended Citation

This Case Note is brought to you for free and open access by the Law Journals at SMU Scholar. It has been accepted for inclusion in Science and Technology Law Review by an authorized administrator of SMU Scholar. For more information, please visit http://digitalrepository.smu.edu.
De-Clawing *Katz*: Emerging Technology and the Exclusionary Rule

*Samuel C. Cole*

I. INTRODUCTION

In *United States v. Stephens*, the Fourth Circuit Court of Appeals considered whether the exclusionary rule applied to evidence obtained from an illegal search in which police officers attached a Global Positioning System (GPS) device to a suspect’s car.1 Police arrested Henry Stephens on May 16, 2011, and a grand jury later indicted him on a federal count of possessing firearms as a convicted felon.2 Stephens filed a motion to suppress, alleging that the evidence against him was obtained through an illegal search.3 After the district court denied Stephens’s motion to suppress, Stephens pleaded guilty to the charges conditionally, pending the result of his appeal of the denial of his motion to suppress.4 The exclusionary rule allows evidence obtained through certain illegal searches to be excluded.5 The rule does not extend, however, to illegal searches “conducted in objectively reasonable reliance on binding appellate precedent.”6 The search in *Stephens* took place before the Supreme Court stated unambiguously that attaching a GPS to a vehicle constitutes a “search” under the Fourth Amendment.7 Furthermore, the Supreme Court held in 1983 that using a “beeper,” the technological precursor to a GPS, in a police operation did not constitute an illegal “search” for purposes of the Fourth Amendment.8 Thus, the Fourth Circuit ruled that the exclusionary rule did not apply because the police officers reasonably relied on binding precedent.9 While the holding in *Stephens* seems narrow at first glance, its impact is widespread and will negatively impact civil liberties. *Stephens* allows police officers or other federal agents to interpret bind-

---

2. See *id.* at 330.
3. See *id*.
6. Id. at 2423–24.
ing Fourth Amendment jurisprudence too broadly—even when it relates to the ever-changing world of technology.10

**II. THE FACTUAL BACKGROUND: STEPHENS INVOKES THE FOURTH AMENDMENT**

Stephens worked as a security guard at “Club Unite,” a nightclub in Baltimore, Maryland.11 Police heard from a registered confidential informant that Stephens was involved in drug trafficking, and that he regularly took a gun to work despite being a convicted felon.12 Without obtaining a warrant, police installed a GPS device on the exterior of Stephens’s car over two periods “from March 20 to April 12, 2011, and again from May 13 to May 16, 2011.”13 On May 16, 2011, having finally obtained “reasonable suspicion, if not probable cause” that Stephens possessed a weapon, Officer Paul Geare and another police officer followed Stephens to work.14 The officers then trailed him by monitoring the GPS.15 When Stephens arrived at work, police searched him and found an empty holster around his waist and a loaded pistol in his car.16 A grand jury promptly indicted Stephens for illegal possession of a firearm.17

After Stephens’s arrest, but before his conviction, the U.S. Supreme Court decided *United States v. Jones*.18 In *Jones*, the Supreme Court held that the warrantless installation and use of a GPS on a suspect’s vehicle constitutes a Fourth Amendment violation.19 Citing to *Jones* and relying on the exclusionary rule, Stephens moved to suppress the government’s evidence against him because it was obtained through illegally attaching a GPS to his car.20 In ruling on Stephens’s motion, the district court agreed with Stephens that, under *Jones*, the officers’ installation and use of a GPS on Stephens’s car for almost two months was indeed an illegal search.21 Nevertheless, the court held that the officers acted in objectively reasonable good faith when

---

10. The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.” U.S. Const. amend. IV.


13. *Id.* at 339 (Thacker, J., dissenting).

14. *Id.* at 330.

15. *Id.*

16. *See id.*


18. *See id.*


21. *See id.*
they conducted the search. Because the officers acted in good faith, the court ultimately held that the exclusionary rule did not apply. With no other legal options left and no hope of succeeding at trial, Stephens pleaded guilty conditionally, pending the Fourth Circuit's review of the denial of his motion to suppress.

III. THE FOURTH CIRCUIT'S DECISION: THE EXCLUSIONARY RULE DOES NOT APPLY

The Fourth Circuit assumed, without actually holding, that the search was illegal after Jones. Nevertheless, the court held that, because the officers had acted in "objectively reasonable reliance on binding appellate precedent," the exclusionary rule did not apply. This "reasonable reliance" test derives from Davis v. United States. The Supreme Court in Davis held that, when police officers within the jurisdiction of the Eleventh Circuit were acting in accordance with Eleventh Circuit precedent as it existed at the time of the search, the exclusionary rule did not apply. The court reached this holding despite the fact that the Supreme Court previously (after the search but before the appeal) reversed the Eleventh Circuit precedent that the officers had relied on. In fact, the Davis petitioner had even conceded that the search was in accordance with then-current precedent. The Davis Court explained that the exclusionary rule is a "judicially created remedy," not one mandated by the Constitution. Thus, the sole purpose of the exclusionary rule is to encourage compliance with the Fourth Amendment.

Following the Davis Court, the Stephens court had to consider whether sufficiently specific, binding precedent existed at the time of the search upon which the officers could have reasonably relied when they attached the GPS device to Stephens's car. In order to answer this question, the Stephens court surveyed the relevant mandatory and persuasive precedent as it had existed at the time of the search. First, however, the Fourth Circuit articulated

22. See id.
23. See id.
25. See id. at 334.
27. Id. (citing Davis, 131 S. Ct. at 2423–24).
28. See Davis, 131 S. Ct. at 2434.
29. See id. at 2428.
30. See id.
31. Id. at 2427 (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)).
32. See id. at 2426.
33. Id. at 2434.
the overarching definition of a “search” as provided by the Supreme Court in *Katz v. United States.* In *Katz,* the Supreme Court held that state action constitutes an illegal “search” under the Fourth Amendment if it violates “an expectation of privacy that society is prepared to consider reasonable.” After defining “search” in general terms, the *Stephens* court turned to its own binding precedent as it existed at the time of the search, as well as some persuasive authority that previously interpreted whether installing a GPS device on a car met the “reasonably expectation of privacy” definition of “search” provided by *Katz.*

First, the Fourth Circuit looked at its own precedent related to the exterior of vehicles. In *United States v. George,* for instance, the court stated in dicta that “there can be no reasonable expectation of privacy in a vehicle’s exterior,” although it is clear from context that the court was only referring to the visible exterior of a vehicle. Nevertheless, the court concluded that, under 2011 jurisprudence, vehicles generally warranted diminished Fourth Amendment protection.

Second, while acknowledging that neither the Supreme Court nor the Fourth Circuit had ever ruled on whether attaching a GPS device to a vehicle was a Fourth Amendment search, the court considered persuasive analogous jurisprudence relating to “beepers.” As the Supreme Court described in *United States v. Knotts,* “[a] beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.” In *Stephens,* the Fourth Circuit relied extensively on *Knotts.*

34. See United States v. Stephens, 764 F.3d 327, 331 (4th Cir. 2014).

35. The complex way in which courts have applied *Katz* is beyond the scope of this note. The application of the *Katz* test might shift, though, for reasons completely unrelated to emerging technology. For instance, although it was a “close question,” the Supreme Court of Connecticut held that a homeless man had a reasonable expectation of privacy in the contents of a duffel bag and cardboard box he left at his “home” under a bridge. *State v. Mooney,* 588 A.2d 145, 154 (Conn. 1991). The court noted, however, that “leaving one’s property in an area ‘readily accessible to animals, children, scavengers, snoops, and other members of the public’ may render one’s expectation of privacy less than reasonable.” *Id.* at 153 (quoting California v. Greenwood, 486 U.S. 35, 40 (1988)). In other words, context matters in cases applying the *Katz* test. Evolving technology, as a particularly mutable context, is especially likely to cause a shift in “reasonable expectations.”

36. See Stephens, 764 F.3d at 331.


38. See *id.*

39. See *id.* at 332.


41. See, e.g., Stephens, 764 F.3d at 332–33.
Knotts, police officers hid a beeper in a bottle of chloroform, suspecting that the purchasers of these chloroform bottles would use the substance to make illegal drugs.42 One of the defendants purchased the chloroform and loaded the bottle into a car.43 The two defendants proceeded to drive to Leroy Knotts’s secluded cabin that was used to manufacture controlled substances.44 The police followed, relying on the beeper.45 Knotts claimed that following him using the beeper was an illegal search under the Fourth Amendment.46 The Knotts Court disagreed, observing that following Knotts using a beeper was not much different than following Knotts otherwise, as beepers only work at close range.47 Furthermore, Knotts had no “reasonable expectation of privacy” on a public road.48 He made it known to the world where he was going.49

After examining Knotts, the Stephens court examined how the circuit courts reacted to Knotts prior to 2011.50 Many circuit courts, including the Fifth, Seventh, Eighth, and Ninth Circuits, concluded that Knotts applied directly to GPS cases.51 Only one circuit court that considered the issue, the D.C. Circuit, did not think that Knotts applied automatically to GPS cases.52 Based on these sister circuit interpretations of Knotts, the Fourth Circuit itself theorized, in dicta, that Knotts stands for the proposition that “monitoring of a beeper falls within the ambit of the Fourth Amendment when it reveals a critical fact about the interior of premises that could not have been obtained through visual surveillance.”53 Notably, however, only five circuits—the Fifth, Seventh, Eighth, Ninth, and the D.C. Circuit—had ever considered whether Knotts applied to GPS tracking cases.54

After examining all of the relevant federal precedent (some binding, some persuasive), the Fourth Circuit then turned to persuasive state court precedent.55 The Maryland state courts spoke much more directly to the issue

42. See Knotts, 460 U.S. at 278.
43. See id.
44. See id. at 278–279.
45. See id. at 278.
46. See id. at 279.
47. See id. at 281.
49. See id.
51. See id.
52. See id.
53. Id. (quoting United States v. Jones, 31 F.3d 1304, 1310 (4th Cir. 1994)).
54. See id.
55. See id. at 334. There was some question in Stephens whether Officer Geare was, in fact, bound by state court precedent for purposes of the exclusionary
of whether attaching a GPS to a vehicle constituted a search under the Fourth Amendment.56 For instance, in Stone v. State, the Maryland Court of Special Appeals stated explicitly (albeit in dicta) that “the use of [a] GPS device could not be a Fourth Amendment violation.”57 To reach this conclusion, the Maryland court relied extensively on the Supreme Court’s opinion in Knotts.58 Notably, the Maryland court found it significant that GPS technology was “simply the next generation” of tracking technology after the beeper at issue in Knotts.59 Surely, then, the court reasoned, Knotts should apply to GPS technology.60 The Maryland Court of Appeals later confirmed this dictum to have been state law prior to 2011: “before Jones, binding appellate precedent in Maryland, namely Knotts, authorized the GPS tracking of a vehicle on public roads.”61 Thus, although Maryland case law is only persuasive authority for the federal system, it was clear that before Jones, four federal circuits and the Maryland state courts believed that Knotts did indeed apply to GPS tracking cases.

Based on the foregoing precedent, the Fourth Circuit held that the police officers in Stephens could have reasonably relied on Knotts when they attached the GPS device to Stephens’s car.62 Thus, the district court was correct in holding that the exclusionary rule did not apply. Even assuming, arguendo, that the Davis Court required reliance on binding precedent (as it said that it did), the Fourth Circuit concluded that Knotts was sufficiently on point: “it is the legal principle of Knotts, rather than the precise factual circumstances, that matters.”63 The manner in which other federal circuit courts and the Maryland state courts interpreted Knotts before Jones significantly bolsters this argument, the court reasoned.64

rule. Id. at 338. Geare was a federal agent, but he was also a Baltimore City police officer. See id. Furthermore, the investigation into Stephens was a joint, federal-and-state operation. See id. The court, however, essentially assumed, arguendo, that Officer Geare was not bound by state court precedent. See id. Regardless, this issue is beyond the scope of this note because the note objects more to the court’s overbroad reasoning than to its specific holding. Moreover, it is worth noting that the dissent disagreed with the majority despite the fact that Maryland precedent was unambiguous. See id. at 342–43 (Thacker, J., dissenting).

56. See id.
58. See Stephens, 764 F.3d at 334.
59. Id. (quoting Stone, 941 A.2d at 1250).
60. See id.
61. Id. (quoting Kelly v. State, 82 A.3d 205, 216 (Md. 2013)).
62. See id. at 338.
63. Id.
64. See Stephens, 764 F.3d at 338.
IV. CRITIQUE OF THE DECISION: A NARROW HOLDING OR AN AFFRONT TO CIVIL LIBERTIES?

Although the holding seems narrow, Stephens sets dangerous precedent. Contrary to Stephens, courts should encourage police officers to construe cases involving emerging technology narrowly when the holding limits the scope of the Fourth Amendment. The Supreme Court implied as much. In Kyllo v. United States, the Supreme Court held that using a thermovision imaging device to look at heat patterns inside a suspect’s house was an unlawful search under the Fourth Amendment.65 In Kyllo, a federal officer suspected that Danny Kyllo was growing marijuana in his home.66 To discover whether Kyllo was in fact growing marijuana, the officer used an Agema Thermovision 210 thermal imager to scan Kyllo’s home.67 The scan revealed that parts of the house were unusually hot from heat lamps used to grow marijuana.68 After obtaining a warrant, federal officers searched Kyllo’s home and found that he was, indeed, growing marijuana.69 Kyllo entered a conditional guilty plea pending the appeal of his unsuccessful motion to suppress.70

In addition to discussing the enhanced expectation of privacy inside one’s home, the Kyllo Court discussed the intersection of emerging technology and the Fourth Amendment.71 “It would be foolish,” noted the Court, “to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology.”72 Surveillance technology is growing more invasive of spheres formerly regarded as private.73 The Court was concerned lest the ever-increasing invasiveness of technology continue to “erode the privacy guaranteed by the Fourth Amendment.”74 The Court rejected the Government’s argument that using Thermovision was not a search because it did not provide the officers with

66. See id. at 29.
67. Id.
68. See id. at 30.
69. See id.
70. See id.
71. See Kyllo, 533 U.S. at 33–34.
72. Id.
73. See id. at 34; see also Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 MICH. L. REV. 801, 866 (2004) (discussing the possibility of increased wiretaps due to the internet’s rising trend of encryption).
74. Kyllo, 533 U.S. at 34.
Thus, courts—and, by extension, police officers—should interpret Fourth Amendment jurisprudence related to emerging technology broadly when the courts expand Fourth Amendment protections. A logical corollary to this rule is that courts and police officers should interpret Fourth Amendment jurisprudence related to emerging technology narrowly when the courts limit Fourth Amendment protections.

Legal scholars have cautioned that courts should tread carefully when addressing Fourth Amendment protections as they apply to emerging technologies. For instance, Professor Marc McAllister argues that courts should not rely on analogies to old technology when dealing with related new technology. The problem, according to McAllister, is that "these supposed analogies are so far removed from the new forms of surveillance that analogies to them only confuse, rather than clarify, the actual analysis required by Katz." To prove this point, McAllister looks at the very line of cases at issue in Stephens. Despite the fact that four circuit courts interpreted Knotts to apply to GPS devices, five concurring Justices in Jones recognized that "an officer trailing a car turn-by-turn is far less invasive than the long-term monitoring of a vehicle by GPS" and that "the situations entail very different

75. See id. at 35.
76. Id. at 35–36 (emphasis added).
77. Id. at 36–37.
78. See Kerr, supra note 73, at 804 ("The view that the Fourth Amendment should be interpreted broadly in response to technological change has been embraced by . . . nearly everyone . . . who has written on the intersection of technology and criminal procedure.").
80. Id. at 477.
81. See id. at 478.
expectations of privacy." At least four of the five Justices in Jones who reached this conclusion did not find it necessary to overrule Knotts.

McAllister also draws support for his thesis from the line of cases originating in Smith v. Maryland. In Smith, the Supreme Court held that because most people understand that phone companies keep records of the numbers they dial, it was not a Fourth Amendment search for police to get this information from the phone company. In United States v. Forrester, the Ninth Circuit extended Smith's reasoning to apply to "computer surveillance techniques that reveal the to/from addresses of e-mail messages, the IP addresses of websites visited and the total amount of data transmitted to or from an account." Even though the analogy between the technologies at issue in Smith and Forrester is plausible, McAllister argues that this sort of broad, analogical reasoning results in a simplistic application of the Katz test.

The Internet did not exist when Smith was decided. It is very possible, then, that reasonable expectations of privacy with respect to the Internet are different from the reasonable expectations of privacy a person expected in the 1970's with telephones. After all, the Supreme Court in Smith stressed, "in applying the Katz analysis to this case, it is important to begin by specifying precisely the nature of the state activity that is challenged." The holding in Stephens encourages police officers to engage in faulty analogical reasoning that McAllister and other scholars condemn. If anything, McAllister's caution applies with extra force to the Davis rule because police officers are less equipped than courts to properly analyze precedents.

83. McAllister, supra note 79, at 478–79.
84. See United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring); see also Stephens, 764 F.3d at 342 n.4 (Thacker, J., dissenting) (A beeper and a GPS device "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. . . . In other words, with the use of a GPS device, law enforcement may simply download the data from afar at their leisure, as they did in this case.").
85. See McAllister, supra note 79, at 479–80.
87. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).
88. See McAllister, supra note 79, at 480.
89. See id.
90. See id.
91. Smith, 442 U.S. at 741 (emphasis added).
92. See, e.g., Frank Lin, Siri, Can You Keep A Secret? A Balanced Approach to Fourth Amendment Principles and Location Data, 92 Or. L. Rev. 193, 221 (2013) ("[A]s technology changes, the expectations of the hypothetical reasonable person change as well.").
The *Stephens* holding is especially inappropriate if the nexus between emerging technology jurisprudence and the Fourth Amendment is constantly in flux. As the dissent in *Stephens* pointed out, "*Davis* did not . . . answer 'the . . . question whether the exclusionary rule applies when the law governing the constitutionality of a particular search is unsettled.'" In fact, a quick review of Fourth Amendment jurisprudence reveals that it is changing rapidly with respect to emerging technologies. Aside from *Jones*, *Riley v. California* also illustrates this trend. In *Riley*, the Supreme Court held that police officers could not search data on cell phones without first obtaining a warrant, even if the search was incidental to a lawful arrest. The *Riley* Court explained in detail the differences between modern-day cell phones and prior technologies that existed even ten years ago. The Court then decisively rejected the Government’s argument that searching a cell phone is “materially indistinguishable” from searching other personal items found in the pocket of an arrestee, such as a billfold, wallet, or address book. Nevertheless, the Court implied that many of these types of items could be considered technological precursors to cell phones. The Government’s argument, though, “is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.”

It is true that *Stephens* and *Riley* involved different contexts. In *Riley*, police were searching new technology, and, in *Stephens*, police were using new technology to conduct a search. *Riley* implicates the Fourth Amendment directly, whereas *Stephens* deals with the applicability of the exclusionary rule. Nevertheless, the same type of reasoning should apply to both cases. Recognizing the fact-specific nature of Fourth Amendment jurisprudence, *Riley* warns against simplistic analogies between less-advanced and

95. See *id.* at 2484, 2489–90.
96. *Id.* at 2488–89.
97. See *id.* at 2489 (Modern cell phones “are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.”).
98. *Id.*
more-advanced technologies. Especially in cases involving emerging technologies, caution is the best policy—for courts or police officers—when interpreting precedent. Even when a court has ruled decisively that using a certain technology is not an unlawful search, the jurisprudence with respect to more advanced technology is still very much in flux. The Stephens court should have interpreted Davis in a way that, like Riley, more adequately respected this fact.

V. CONCLUSION: A BRAVE NEW WORLD OF ADVANCED SURVEILLANCE TECHNOLOGY AND LIMITED FOURTH AMENDMENT PROTECTION?

Finally, the holding of the Stephens court is likely to curtail Fourth Amendment freedoms severely in the future. For example, the Supreme Court has held that "a temporary detention for questioning in the case of an airport search" is generally "permissible" under the Fourth Amendment. Researchers at the Mayo Clinic are currently developing "thermal imaging technology that measures 'heat patterns created by [facial expressions]' that 'change dramatically [when a person lies].'" Unlike conventional lie detector tests, however, this technology could easily be adapted for efficient use at airport checkpoints. This new lie-detecting technology is arguably analogous to the airport questioning currently permitted by the Supreme Court. Under the rule set forth by the Stephens court, there is nothing to deter federal officers from using this technology based on current precedent. As technology changes, however, so do our reasonable expectations of privacy. It is true that the exclusionary rule exception in Davis is practically necessary when applied to factually-specific binding precedent. After all, as the Supreme Court noted in Davis, the exclusionary rule can have devastating effects on society. Applying the Davis rule vis-à-vis the Fourth Circuit in Stephens, however, de-claws the Fourth Amendment and leaves our right to privacy at the mercy of advances in technology.

103. See Riley, 134 S. Ct at 2494–95.
106. See id. at 220.