DOGS, DRONES, AND DEFENDANTS: THE FOURTH AMENDMENT IN THE DIGITAL AGE

Mason C. Clutter[*]

INTRODUCTION

As technology evolves and expectations of individual privacy morph, so too must the law. Unfortunately, Congress is failing to keep up with technological advances, and the courts are forced to refer to our founding document for guidance on the government's use of new technologies. The Fourth Amendment protects "persons, houses, papers, and effects, against unreasonable searches and seizures."[1] We know that a man's home is his castle and one of the most private and protected spaces under the law. But what protection do citizens have from intrusion by electronic devices and other "enhanced searching technologies" that can see, smell, and hear through walls and track one's physical location and electronic communications? Can law enforcement use these technologies against us outside of our homes? The law is always a bit stickier when we step outside of the home and into "public."

Over the past decade, the Supreme Court has started to entertain this issue, with interesting results. Key to understanding the intersection between the Fourth Amendment and technology are the Supreme Court's recent decisions in two cases involving law enforcement's use of narcotics detection dogs. Read in light of the Court's decisions on the use of GPS tracking devices and thermal imaging devices, *Florida v. Jardines*[2] and *Florida v. Harris*[3] will form the basis of Fourth Amendment jurisprudence in the digital age. In order to apply the Court's previous Fourth Amendment jurisprudence to today's tech world, one must reshape the way she thinks of searches and seizures under the law and revert to a traditional definition of what these actions mean—the ability to perceive something that is not in plain view, plain smell, plain touch, or plain hearing.

The primary vehicle for consideration of Fourth Amendment rights is the criminal case. More so than civil cases, criminal cases directly involve the interaction of government (law enforcement) with individual rights, be they the rights of a person or of a corporation. Often, these cases will effect

---

[*] Mason C. Clutter is National Security and Privacy Counsel to the National Association of Criminal Defense Lawyers ("NACDL"). The views expressed in this Essay are her own and do not reflect the views of NACDL.

1 U.S. CONST. amend. IV.

2 133 S. Ct. 1409 (2013).

3 133 S. Ct. 1050 (2013).

policy changes that affect the public at large, so they are much bigger than just the defendant whose liberty is at stake. "The police, of course, are entitled to enjoy the substantial advantages . . . technology confers. They may not, however, rely on it blindly. With the benefits of more efficient law enforcement mechanisms comes the burden of corresponding constitutional responsibilities."[4]

Defense lawyers should familiarize themselves with the dog sniff cases because the Court speaks directly to lawyers about how they should challenge not just dog sniffs but also enhanced searching technologies moving forward. Both Justice Elena Kagan and Justice Sonia Sotomayor have opened the door to new constitutional arguments against warrantless uses of sense-enhancing searching devices, and advocates should advance their fresh take on the Fourth Amendment.[5]

The public's reliance on technology has reached new heights. Today, one has a difficult time functioning in society without the use of technology, like e-mail, ATMs, and smartphones. At the same time, law enforcement's reliance on technology to conduct criminal investigations is growing at an exponential rate without adequate and standardized safeguards in place to regulate the government's use of such technology. From dog sniffs to domestic surveillance drones, from your front porch to the open road, warrantless searches are being conducted every day.

I. THE (RECENT) EVOLUTION OF THE FOURTH AMENDMENT IN LIGHT OF TECHNOLOGY

During the 2012 term, the Supreme Court went to the dogs when it considered two cases involving law enforcement's use of drug detection dogs. *Florida v. Jardines* involved the warrantless use of a drug dog to sniff the front porch of a suspected grow house,[6] while *Florida v. Harris* involved the use of a drug dog that falsely alerted to the presence of narcotics in a defendant's car.[7] *Jardines* asked whether a dog sniff of a home constitutes a search under the Fourth Amendment,[8] and *Harris* asked what amount of evidence must be shown to establish probable cause for a search based on a dog's "alert."[9] *Harris* was jokingly referred to by legal pundits as the "doggie diploma case" because the Florida Supreme Court held in favor of Mr. Harris, not Aldo the dog, finding that it is not enough for an

---

4 Arizona v. Evans, 514 U.S. 1, 17-18 (1995) (O'Connor, J., concurring).

5 *See Jardines*, 133 S. Ct. at 1418-19 (Kagan, J., concurring); United States v. Jones, 132 S. Ct. 945, 956-57 (2012) (Sotomayor, J., concurring).

6 *Jardines*, 133 S. Ct. at 1413 (majority opinion).

7 *Harris*, 133 S. Ct. at 1053-54.

8 *Jardines*, 133 S. Ct. at 1413.

9 *Harris*, 133 S. Ct. at 1053.

officer to testify that his or her dog has been trained and certified to establish the dog's reliability.[10] Instead, the Florida Supreme Court said the state must keep records of the dog and handler's training, including field performance records—especially "evidence of the dog's performance history"—and other evidence to establish the dog's reliability.[11]

Law enforcement officers have used sniffer dogs for decades. For thirty years, beginning with *United States v. Place*,[12] the Supreme Court maintained that a dog sniff was not a search because a dog simply alerts to the presence or absence of contraband, and a person has no expectation of privacy in illegal contraband.[13] In fact, the *Place* Court had no need to decide whether a dog sniff amounted a search, and it was not until *Jardines* that the Court reached the question as part of its holding.[14] Nevertheless, the Court's dicta in this area raises an interesting question about modern technology that, like a dog sniff, reveals only the presence or absence of contraband. Is such technology outside the scope of the Fourth Amendment? Further, would a court simply accept the reliability of these technologies if a law enforcement officer testifies that they are in fact reliable, without additional evidence of reliability? These questions prompted the Electronic Privacy Information Center ("EPIC") and the Cato Institute, among other civil liberties groups, to file amicus briefs in *Harris* and *Jardines*, respectively.

Both organizations raised examples of developing and existing technologies that purport to reveal only the presence or absence of contraband, including terahertz wave reflection spectroscopy to detect chemical substances; millimeter wave and backscatter X-ray (airport body scanners); and message interception software (e.g., Carnivore), which "act[s] like a commercial packet 'sniffer' product, [and] analyzes electronic communications as they travel through a network."[15] The Department of Homeland Security's Future Attribute Screening Technology project "monitors specific biologic cues to detect intent to cause harm," and its "Remote Vapor Inspec-

---

10 *See, e.g.*, Harvey Silverglate, *Man's Best Friend Is No Friend to the Fourth Amendment*, FORBES (Mar. 3, 2013, 7:30 AM), http://www.forbes.com/sites/harveysilverglate/2013/03/01/mans-best-friend-is-no-friend-to-the-fourth-amendment/ ("[T]he U.S. Supreme Court deemed the dog's tail sufficiently reliable to meet the Fourth Amendment's standard of 'probable cause' to believe that a search of the truck would produce contraband. Such is the power of a diploma.").

11 Harris v. State, 71 So. 3d 756, 769 (Fla. 2011), *rev'd*, 133 S. Ct. 1050 (2013).

12 462 U.S. 696 (1983).

13 *See, e.g.*, *id.* at 707 ("We have affirmed that a person possesses a privacy interest in the contents of personal luggage that is protected by the Fourth Amendment. A 'canine sniff' by a well-trained narcotics detection dog, however, does not . . . expose noncontraband items that otherwise would remain hidden from public view . . . ." (citation omitted)).

14 Florida v. Jardines, 133 S. Ct. 1409, 1417-18 (2013).

15 Brief of Amicus Curiae Electronic Privacy Information Center (EPIC) in Support of the Respondent at 21, 24-25, 27, Florida v. Harris, 133 S. Ct. 1050 (2013) (No.11-817) [hereinafter EPIC Amicus Brief].

tion System" detects certain particles and gases.[16] EPIC referred to these new technologies as "electronic canine sniffs," and reminded the Court that "[t]he dog sniff . . . is just one crude, old-fashioned example of the search technologies available to law enforcement."[17]

Cato argued that the dog sniff at issue in *Jardines* constituted a search because, like other technologies used to detect contraband, the dog enabled the officers to "seek out something that is otherwise concealed from view" or, in this case, smell.[18] EPIC argued that "the government should bear the burden of establishing [the] reliability" of "new investigative technique[s] . . . used in an attempt to identify a hidden substance, flag a possible threat, or gather evidence."[19] The *Harris* case, EPIC argued, "implicate[s] the use of investigative techniques that encroach on electronic privacy."[20] These arguments were not far-fetched at the time because just eight months earlier the Court ruled, 9-0, in favor of a criminal defendant against whom the government used enhanced-searching technologies to track and gather incriminating evidence.[21]

In early 2012, the Court issued a groundbreaking opinion in *United States v. Jones*[22] on law enforcement use of GPS location tracking devices. A majority of the Court found 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'" under the Fourth Amendment.[23] Particularly offensive to Justice Scalia was the fact that the government used Mr. Jones's private property for the purpose of gathering evidence against him—information that was not easily within the officers' plain view.[24]

Justice Sotomayor concurred in the majority opinion, agreeing that trespass law easily decided the case, but she went on to argue that Mr. Jones may have had a reasonable expectation of privacy in his public movements.[25] She questioned whether information shared with the public "for a limited purpose" wipes that information of Fourth Amendment protection.[26] Further, citing the kind of private information such location tracking could

---

16 Brief of Amicus Curiae Cato Institute Supporting Respondent at 8-9, Florida v. Jardines, 133 S. Ct. 1409 (2013) (No. 11-564) [hereinafter Cato Amicus Brief].

17 EPIC Amicus Brief, *supra* note 15, at 3, 20 (alteration in original) (quoting Julian Sanchez, *The Pinpoint Search*, REASON (Jan. 10, 2007, 1:02 PM), http://reason.com/archives/2007/01/10/the-pin point-search) (internal quotation marks omitted).

18 *See* Cato Amicus Brief, *supra* note 16, at 14.

19 EPIC Amicus Brief, *supra* note 15, at 3.

20 *Id.* at 2.

21 *See* United States v. Jones, 132 S. Ct. 945 (2012).

22 132 S. Ct. 945 (2012).

23 *Id.* at 949 (footnote omitted).

24 *Id.*

25 *Id.* at 954-55 (Sotomayor, J., concurring).

26 *Id.* at 957.

reveal, like "trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney,"[27] she handed privacy advocates and defense lawyers a new argument for their arsenal—that seemingly non-content information can be analyzed in such a way as to reveal content. In other words, singular movements in time can be combined to create a clear picture of a person's day-to-day life, including very private behavior. Such a search can reveal both "contraband" and private information. That information, she argues, may in fact be entitled to Fourth Amendment protections. These arguments permeate the concurring opinion in *Jardines*. Prior to *Jones*, the *Jardines* concurrence may have simply discussed the dog as a dog, not as "sense-enhancing" technology.[28]

II. THE TECHNOLOGY OF DOGS

In *Jardines*, for the first time, the Supreme Court said a dog sniff was a search—a dog sniff of a home, that is. As in *Jones*, the majority relied on traditional trespass theory to establish that a search was conducted and police engaged in a "canine forensic investigation" when they marched a dog to the front door of Mr. Jardines's home without his explicit or implicit consent.[29] Interestingly, unlike in *Jones*, we see Justice Scalia entertaining thoughts of the technological implications of this opinion. For instance, he says

> [t]he dissent would let the police do whatever they want by way of gathering evidence as long as they . . . "stick to the path that is typically used to approach a front door, such as a paved walkway." From that vantage point they can presumably peer into the house through *binoculars* with impunity. That is not the law . . . .[30]

But, as in *Jones*, Justice Scalia was reluctant to analyze the issue before the Court under the *Katz* reasonable-expectation-of-privacy test. He further found that it is unnecessary to apply or reconcile *Jardines* with *Kyllo v. United States*,[31] the Court's 2001 decision finding that the use of a thermal imaging device on a home is a search within the meaning of the Fourth Amendment.[32] He said it is unnecessary to consider *Kyllo* because there is no need to consider the technology used during a trespass.[33] Additionally, in support of his use of trespass theory to decide *Jardines*, he cited

---

27 *Id.* at 955 (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)) (internal quotation marks omitted).

28 Florida v. Jardines, 133 S. Ct. 1409, 1419 (2013) (Kagan, J., concurring).

29 *Id.* at 1416 (majority opinion).

30 *Id.* at 1416 n.3 (emphasis added) (citation omitted) (quoting *id.* at 1422 (Alito, J., dissenting)).

31 533 U.S. 27 (2001).

32 *Id.* at 40.

33 *Jardines*, 133 S. Ct. at 1417.

the Court's decision in *California v. Ciraolo*,[34] which held that law enforcement use of aerial surveillance to observe marijuana growing in a backyard of a home is not a Fourth Amendment search.[35] Specifically, he used *Ciraolo* for *Jardines*'s discussion of curtilage of a home rather than the underlying technological implications of that case.

In keeping with *Jones*, the concurring opinion in *Jardines* accepted the trespass theory to resolve the case, but it also argued that the case could be decided under the *Katz* reasonable-expectation-of-privacy test.[36] In *Katz v. United States*,[37] law enforcement agents placed a listening device on a public phone booth and listened to Mr. Katz's private conversation.[38] The majority found that Mr. Katz intended to keep his conversation private—he closed the door to the phone booth—and, therefore, the government intruded into a private conversation and could only do so with a warrant.[39] The *Katz* majority is often cited for saying

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[40]

Justice Harlan concurred in the Court's opinion and created what is now known as the *Katz* reasonable-expectation-of-privacy test.[41] Under this test, a defendant's Fourth Amendment rights may be infringed if the defendant can establish that he had a subjective expectation of privacy that society recognizes as reasonable.[42]

In *Jardines*, unlike in *Jones*, the concurrence gained two more Justices and delved further into what privacy means in the digital age.[43] Specifically, we see Justice Kagan and Justice Ruth Bader Ginsburg endorse Justice Sotomayor's thoughts from her *Jones* concurrence on privacy in the digital age generally and apply them to the facts in the dog sniff case—expanding the traditional dog sniff inquiry to an inquiry about government use of enhanced searching technologies. Justice Kagan likened the use of a drug detection dog on a front porch of a home to the use of "super-high-powered binoculars" on the front porch of a home.[44] "Here, police officers came to

---

34 476 U.S. 207 (1986).

35 *Id.* at 213-14.

36 *Jardines*, 133 S. Ct. at 1418 (Kagan, J., concurring).

37 389 U.S. 347 (1967).

38 *Id.* at 348.

39 *Id.* at 359.

40 *Id.* at 351-52 (citations omitted).

41 *See id.* at 361 (Harlan, J., concurring)

42 *Id*.

43 *See* Florida v. Jardines, 133 S. Ct. 1409, 1418 (2013) (Kagan, J., concurring).

44 *Id.*

Joelis Jardines' door with a super-sensitive instrument, which they deployed to detect things inside that they could not perceive unassisted."[45] She argued that police narcotics dogs are not your typical pets: they "are highly trained tools of law enforcement."[46] Indeed, "[t]hey are to the poodle down the street as high-powered binoculars are to a piece of plain glass. Like the binoculars, a drug-detection dog is a specialized device for discovering objects not in plain view (or plain smell)."[47]

Justice Kagan goes on to say that if the case had been decided on privacy instead of property grounds, the Court's prior decision in *Kyllo* would have easily controlled.[48] In *Kyllo*, the officers did not physically trespass on the defendant's property when they used a thermal imaging device to determine in what areas of the house the defendant was likely growing marijuana.[49] Instead, the Court found that "[w]here, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[50]

Justice Kagan argued that *Kyllo* could also govern *Jardines* because "[t]he police officers here conducted a search because they used a 'device . . . not in general public use' (a trained drug detection dog) to 'explore details of the home' (the presence of certain substances) that they would not otherwise have discovered without entering the premises."[51] She concluded by reassuring law enforcement that they can use a dog—or "the device," as she calls it—to examine a home in the future, but only by first securing a warrant based on probable cause or establishing that one of the exceptions to the Fourth Amendment applies, like exigent circumstances.[52]

III. RELIABILITY OF TECHNOLOGY TO ESTABLISH PROBABLE CAUSE TO SEARCH

Just as *Jardines* can be read expansively to address the use of sense-enhancing technologies to conduct searches, *Harris* can be read to address the reliability of such technologies to establish probable cause to search. While the *Harris* opinion comes off as a little defensive (or "pro dog")[53] and protective of law enforcement, it reminds defense lawyers, and for that

---

45 *Id.*

46 *Id.*

47 *Id.*

48 *Id.* at 1419.

49 Kyllo v. United States, 533 U.S. 27, 29-30 (2001).

50 *Id.* at 40.

51 *Jardines*, 133 S. Ct. at 1419 (Kagan, J., concurring) (alteration in original).

52 *Id.* at 1419-20.

53 No one would have thought the Justices disliked dogs, really.

matter all lawyers who cross-examine witnesses, to ask the right questions. As with most opinions that require law enforcement to abide by the Fourth Amendment (e.g., *Jardines*), the Court is quick to make sure that its rulings do not place "unnecessary burdens" on law enforcement (e.g., *Harris*). In other words, *Harris*—although it was issued before *Jardines*—signals that the Court will place a small burden on law enforcement (in *Jardines*, a warrant requirement to use dogs to sniff homes), but it will refrain from further burdening law enforcement by requiring records of the dogs' performance.[54]

Instead, the Court places the burden on the defendant—or, rather, the criminal defense lawyer—to do a competent job on cross-examination. Rather than require law enforcement officers to keep documentation of the dog's field performance and other evidence of the dog's training and experience, the Court instructs defense lawyers to be thorough in cross-examining the officer about the dog, the officer/handler's training, and the dog's field performance (i.e., hits or misses in the field).[55] The Court also encourages the defense's use of "expert witnesses" to address the quality of the dog's training and certification.[56] Read in light of *Jardines*, however, *Harris* applies much more broadly than to dog sniffs. *Harris* should be read to address the reliability of all technologies to establish probable cause to search, like the technologies mentioned previously that purport to detect only the presence or absence of contraband. Would it be enough for a law enforcement officer to simply press a button or read a computer screen to justify infringing on a person's Fourth Amendment rights?

The privacy implications of the dog or the device getting it wrong are too grave for *Harris* to stand for the proposition that anything that alerts to the existence of an illegal substance is always sufficient to establish probable cause. Unfortunately, while the Court goes on to say that the dog's reliability is based on the totality of the circumstances—the circumstances surrounding the stop, like handler cuing, and the training and certification programs that the dog attended—it also suggests that dogs may in fact be better than their field records would suggest because "[t]he dog may have detected substances that were too well hidden or present in quantities too small for the officer to locate."[57] This same logic could be applied to law enforcement's use of technological devices that claim to detect only the presence of contraband, which is why the Court's reliance on the defense lawyer's ability to raise issues on cross-examination is so critical to preserving the Fourth Amendment in the digital age.

On the other hand, maybe dogs are a little different than technology under *Harris*. It is hard to reconcile Justice Kagan's treatment of the dog as

---

54 *See* Florida v. Harris, 133 S. Ct. 1050, 1056 (2013).

55 *Id.* at 1057-58.

56 *Id.* at 1057.

57 *Id.* at 1056.

a "super sensitive instrument" in *Jardines* with her hat tip to the dog in *Harris* because, as everyone knows, instruments are fallible and need some fine tuning every now and again. It may be wise for a criminal defense lawyer to argue that *Harris* is limited to the facts in light of this discrepancy, though of course only the lawyer can make the legal and factual determinations necessary to develop a legal strategy.

Conversely, as amicus EPIC argued in its brief, "many investigative techniques do not reliably indicate the presence of a controlled substance. The Fourth Amendment protects individuals against such 'unreasonable searches and seizures,' and this Court has held that procedural requirements, such as proof of probable cause, help ensure that individual rights are not violated."[58] New investigative techniques are important for law enforcement, but the government must ensure and demonstrate that the techniques are in fact reliable, otherwise "it is an exception that threatens to swallow the rule . . . that all government searches are presumptively unreasonable unless accompanied by a warrant or covered by a particular and limited exception."[59] The result would place individual rights "at the mercy of advancing technology."[60] This cannot be what the Court intended in *Harris*.

IV. LESSONS FOR CRIMINAL DEFENSE LAWYERS

As one reads through the Court's opinions on the intersection of technology and the law over the past decade, a recurring theme develops when the Court addresses what constitutes a search under the Fourth Amendment. In *Kyllo*, Justice Scalia described the investigation as "more than naked-eye surveillance of a home" which exposed "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area.'"[61] In *Jardines*, Justice Scalia said "the officers learned what they learned only by physically intruding on Jardines' property,"[62] and Justice Kagan said the dog was used to "detect things inside that [the officers] could not perceive unassisted."[63] She also noted that the drug detection dog discovers things "not in plain view."[64] These are all roundabout ways of saying that searches occurred

---

58 EPIC Amicus Brief, *supra* note 15, at 6.

59 *Id.* at 9 (alteration in original) (quoting Cecil J. Hunt, II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable Expectations of Privacy*, 56 CASE W. RES. L. REV. 285, 336 (2005)) (internal quotation marks omitted).

60 *Id.* (quoting Kyllo v. United States, 533 U.S. 27, 35 (2001)).

61 *Kyllo*, 533 U.S. at 33-34 (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

62 Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013).

63 *Id.* at 1418 (Kagan, J., concurring).

64 *Id.*

because the officers were looking for something that they could not otherwise use their own senses to see, hear, taste, touch, or smell.

A. *The "Harper Theory" of Search and Seizure*

Jim Harper, director of information policy studies at the Cato Institute and one of the authors of Cato's amicus brief in *Jardines*, regularly makes the argument that "[a] 'search' occurs when government agents seek out that which is otherwise concealed from view, the opposite condition from what pertains when something is in 'plain view.' People maintain 'privacy' by keeping things out of others' view, exercising control over personal information using physics and law."[65] The "Harper Theory" of search and seizure encourages judges, lawyers, and law enforcement officers to revert to the "plain meaning[]" of the Fourth Amendment's use of "search" and "seizure."[66] Harper argues that the *Katz* reasonable-expectation-of-privacy test asks the wrong questions, and that courts often do not undertake the analysis required in *Katz*, particularly the subjective-expectation prong.[67] It is not about expectations of privacy as much as "[t]he physical and legal barriers people place around information [which] can answer whether people have held it close, showing at the same time when the threshold of personal security the Fourth Amendment protects has been crossed."[68]

Instead, Harper argues, the Court should look to the actual language of the Fourth Amendment and determine "factually and legally" whether a search or seizure has occurred and then ask whether it was reasonable or unreasonable to conduct the search without first securing a warrant.[69] This test, he says, will survive changes in technology.[70] He made similar arguments to the Court in *Jones* regarding seizure and the property concepts of trespass and conversion.[71] Particularly, in Justice Kagan's concurrence in *Jardines*, in addition to her application of the *Katz* reasonable-expectation-of-privacy test, we see elements of this traditionalist test coming through.

The Harper Theory is a common-sense, traditional approach to the concept of search-and-seizure law. If an officer cannot see, feel, hear, taste, or smell a substance by using his or her own senses, then that officer is searching for something. One can see how this analysis easily applies equally to the use of the dog in *Jardines* and the thermal imaging device in *Kyllo*. Because there were no exigencies or facts that established an excep-

---

65 Cato Amicus Brief, *supra* note 16, at 2.

66 *Id.* at 14.

67 *Id.* at 11.

68 *Id.* at 5-6.

69 *Id.* at 14.

70 *Id.* at 16-17.

71 *See* Brief of Amicus Curiae the Cato Institute in Support of Respondent at 1-2, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259).

tion to the Fourth Amendment, it was unreasonable for law enforcement to conduct those searches without a warrant.

This analysis does not require a court to understand the technologies that may be used by law enforcement. Rather, it simply requires a determination that the officers sought out something to which they otherwise did not have direct access through the use of their own senses. Defense lawyers should consider including the Harper Theory of search and seizure in the arguments they make under the Fourth Amendment. As with the trespass theory of search and seizure, this analysis should be considered in addition to, not to the exclusion of, the *Katz* reasonable-expectation-of-privacy test. It would be worthwhile for criminal defense lawyers to spend time reviewing Mr. Harper's briefs in *Jones* and *Jardines*.

B. *Privacy Interest in Contraband*

Similarly, Justice Kagan's comparison of drug detection dogs to technological searching devices opens the door to new arguments by criminal defense lawyers. For instance, previous Supreme Court dog sniff jurisprudence noted that a dog sniff is not a search because dogs only alert to the presence or absence of contraband, and a person has no expectation of privacy in illegal substances.[72] *Jardines* dispels this argument. *Jardines*, in essence, suggests that there may in fact be a privacy interest in contraband, which is helpful in arguing against the use of new technologies designed to detect only contraband.[73] The Government will attempt to limit the application of *Jardines* in the same way it has tried to limit the application of *Jones*—the property theory of trespass controls, and, without a physical trespass, there is no Fourth Amendment violation.

While Justice Scalia suggests that using the property theory of the Fourth Amendment "keeps easy cases easy,"[74] it remains necessary to consider both the majority and concurring opinions in *Jones* and *Jardines* in reviewing the constitutionality of government uses of surveillance technologies which do not begin with a trespass.[75] The discrepancies between the majority and concurring opinions in *Jones* and *Jardines* are currently being considered by the lower courts in their application of both cases to other search technologies, like historic cell-site location tracking.[76]

---

72 *See* United States v. Place, 462 U.S. 696, 707 (1983).

73 Florida v. Jardines, 133 S. Ct. 1409, 1417 (2013).

74 *Id.*

75 *See id.* at 1418 (Kagan, J., concurring); United States v. Jones, 132 S. Ct. 945, 954-55 (2012) (Sotomayor, J., concurring).

76 *See, e.g.*, United States v. Katzin, 732 F.3d 187, 193 n.1 (3d Cir. 2013), *reh'g en banc granted*, No. 12-2548, 2013 WL 7033666 (3d Cir. Dec. 12, 2013); United States v. Alabi, 943 F. Supp. 2d 1201, 1207 (D.N.M. 2013); United States v. Graham, 846 F. Supp. 2d 384, 389-90 (D. Md. 2012).

C. *Technology Reveals Private Information*

Also, courts are beginning to recognize and apply Justice Sotomayor's analysis in *Jones* of the kind of private information that can be revealed through law enforcement's use of a GPS tracking device or other new technologies.[77] The type of information that law enforcement may obtain through the use of enhanced searching technologies today greatly differs from the limited information considered in more antiquated case law. For instance, consider the third party doctrine, established in *Smith v. Maryland*[78] and *United States v. Miller*,[79] which provides that individuals may lose their expectations of privacy in information shared with a third party.[80] Justice Sotomayor suggested that the third party doctrine "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."[81]

The third party doctrine originally allowed the government to obtain a list of telephone numbers dialed from a particular phone and certain banking information a customer shares with his or her bank.[82] The doctrine now forms the basis for the government's warrantless use of historic cell-site location information to place defendants near the scene of crimes, the search and seizure of e-mails stored online for more than 180 days, and the National Security Agency's collection of every American's telephony metadata from private companies.[83] Criminal defense lawyers should con-

---

77 *See, e.g.*, Klayman v. Obama, No. 13-0881 (RJL), 2013 WL 6598728, at *19-22 (D.D.C. Dec. 16, 2013) (applying the rationale of Justice Sotomayor's concurring opinion in *Jones* to the National Security Agency's bulk metadata collection program).

78 442 U.S. 735 (1979).

79 425 U.S. 435 (1976).

80 *See id.* at 443 ("[T]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

81 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring); *see also* NAT'L ASS'N OF CRIMINAL DEF. LAWYERS, ELECTRONIC SURVEILLANCE & GOVERNMENT ACCESS TO THIRD PARTY RECORDS 3-4 (2012), *available at* http://www.nacdl.org/reports/thirdpartyrecords/thirdpartyrecords_pdf/.

82 *See Smith*, 442 U.S. at 743-44; *Miller*, 425 U.S. at 443.

83 *See, e.g.*, *In re* Application of the United States for Historical Cell Site Data, 724 F.3d 600, 515 (5th Cir. 2013) ("Cell site data are business records and should be analyzed under that line of Supreme Court precedent."); United States v. Weaver, 636 F. Supp. 2d 769 (C.D. Ill. 2009) ("Previously opened emails stored by Microsoft for Hotmail users are not in electronic storage, and the Government can obtain copies of such emails using a trial subpoena."); U.S. DEP'T OF JUSTICE, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 2 (2013), *available at* http://www.nytimes.com/interactive/2013/08/10/us/politics/10obama-surveillance-documents.html?_r=1& ("The telephony metadata collection program also complies with the Constitution. Supreme Court precedent makes clear that participants in telephone calls lack a reasonable expectation of privacy for purposes of the Fourth Amendment in the telephone numbers used to make and receive their calls.").

sider using Justice Sotomayor's arguments in her *Jones* concurrence to demonstrate that a broad application of the third party doctrine in the digital age would permit law enforcement to access much more than contraband, and that society may not recognize this access as reasonable. *Jardines* may also be cited in conjunction with *Jones* to support an argument that a defendant may in fact have a Fourth Amendment interest in "contraband" when other private information may be revealed through the use of sense-enhancing technologies.

D. *Cross-Examination*

While *Jones* and *Jardines* addressed the legal analysis of whether government action is a seizure or a search under the Fourth Amendment, we must also look to *Harris* to understand the obligations on defense lawyers to cross-examine law enforcement officers who use such sense-enhancing technologies. In essence, the *Harris* case said it is okay for an officer to rely on a drug detection dog to establish probable cause to search, even if the dog may be alerting to something that is not actual contraband but rather "residual odor."[84] This does not mean, however, that officers can justify infringing on a person's Fourth Amendment rights by simply testifying that their dogs are reliable. Instead, the Court put the onus on the defense lawyer to effectively cross-examine witnesses and call their own experts to challenge the reliability of a particular narcotics detection dog.[85]

Defense lawyers should follow this instruction in all suppression hearings, no matter the technology used in discovering the evidence in question. In a dog sniff case, the lawyer should "contest the adequacy of a certification or training program, . . . examine how the dog (or handler) performed in the assessments made in those settings," and introduce "evidence of the dog's (or handler's) history in the field."[86] The same is true with regard to enhanced searching technologies. Lawyers will need to cross-examine law enforcement officers to learn whether they were adequately trained in how to use the device, whether they also relied on their own senses and experiences, whether the device was calibrated and properly maintained, whether the software was up-to-date, and so on. The lawyer's obligation to raise these issues, however, does not first attach at the suppression phase of a trial. Lawyers should be considering these issues as they approach discovery as well.

---

84 Florida v. Harris, 133 S. Ct. 1050, 1056 (2013).

85 *Id.* at 1057-58.

86 *Id.* at 1057.

E. *Discovery*

In a pending criminal case in the Northern District of California involving a multi-defendant prosecution for drug trafficking and other related offenses, amici curiae American Civil Liberties Union ("ACLU") and the Electronic Frontier Foundation ("EFF") cited *Harris* for the proposition that the government must disclose information about the "reliability" of human and non-human "witnesses."[87] The ACLU and the EFF argued that the Drug Enforcement Administration may have used a recently disclosed surveillance program known as "Hemisphere" to obtain call detail records from AT&T.[88] The program allows the government to use the call detail records to track phone calling patterns to easily locate users of so-called "burner phones."[89] The amici also challenge the use of the NSA phone metadata collection program recently revealed by former NSA contractor Edward Snowden, and the use of "Stingray" devices or "cell site simulator" devices that "collect unique numeric identifiers associated with phones . . . or . . . ascertain the location of a phone."[90]

The brief argues that the Government's discovery obligations

> apply equally to dogs and the covert use of surveillance programs. A drug detecting dog's performance is relevant to assessing the dog's credibility for purposes of a suppression motion. To the extent Hemisphere or other surveillance programs served as the "confidential source . . . provid[ing] investigating agents with . . . new cellular telephone number[s]" of the targets of the investigation, so too is information about how these programs function. And just as the "circumstances surrounding a particular alert" may undermine probable cause in a dog sniff situation, the same is true of information about the "algorithm and advanced search features" used by Hemisphere "to find the new number." . . . Under *Brady* and Rule 16, the defense is entitled to information that would allow cross-examination over the reliability of these surveillance programs.[91]

As the ACLU and EFF make clear, in order to effectively cross-examine a witness, as recommended by the Court in *Harris*, a defense lawyer first needs the underlying information about the technology in question.

---

87 Brief Amici Curiae of ACLU, ACLU of Northern California & Electronic Frontier Foundation in Support of Defendants' Motion to Compel Discovery at 17, United States v. Diaz-Rivera (N.D. Cal. Oct. 15, 2013) (No. 12-cr-00030-EMC/EDL).

88 *Id.* at 5.

89 *Id.* at 5-6 (discussing how the program can identify targets of investigations who cease using one phone and acquire another).

90 *Id.* at 8 (internal quotation marks omitted).

91 *Id.* at 17-18 (first, second, third, and fourth alterations in original) (citations omitted).

CONCLUSION

Initially, lawyers should expect rulings similar to those we have seen in litigation immediately following *Jones*: that the officer relied in good faith on the law at the time of the search and that therefore the evidence will not be suppressed.[92] However, once new cases find their way into the justice system, lawyers should expect additional push back by judges who fear overburdening law enforcement by requiring them to obtain a warrant before they conduct tech-assisted searches. It is important to remember, though, that traditional Fourth Amendment jurisprudence will still apply, and existing exceptions to the Fourth Amendment will continue to remain viable. These cases will take years to make their way to the Supreme Court; however, as we saw in *Harris*, it is imperative that trial lawyers make these arguments at the outset or else the ability to raise them later will forever be waived.

---

92 *See, e.g.*, Davis v. United States, 131 S. Ct. 2419, 2434 (2011) ("We therefore hold that when the police conduct a search in objectively reasonable reliance on binding appellate precedent, the exclusionary rule does not apply."); United States v. Sparks, 711 F.3d 58, 67 (1st Cir. 2013) ("[A]t the time of the GPS surveillance in this case, settled, binding precedent . . . authorized the agents' conduct. *Davis* thus precludes suppression of the resulting evidence, even if the agents' actions violated the Fourth Amendment (which we do not decide).").