(DIGITAL) TRESPASS: WHAT'S OLD IS NEW AGAIN

HANNAH L. COOK†

A digital trespass theory of Fourth Amendment searches is necessary to maintain the relevance of the Supreme Court's decision in *United States v. Jones*.[1] At the time the Fourth Amendment was written, if a government official wanted to track a suspect, he needed to physically follow the suspect around to learn his whereabouts. If he wanted to read a suspect's correspondence, he needed to enter the suspect's home or office and take the physical letter. If he wanted to listen to a suspect's conversation, he needed to hide under an open window or find an informant. In 2017, these tactics are no longer necessary—we use electronics to travel, write, and speak with one another. Unfortunately, these devices can betray us without any physical interaction with law enforcement, potentially confounding a Fourth Amendment whose authors never imagined law enforcement conducting a remote search and eviscerating the progress made in *Jones*.

This article provides a solution to the problem of remote digital searches by proposing a theory of digital trespass, in which it is a search when law enforcement trespasses with technology by sending a targeted electronic signal that causes a device to take an action. This action could be sending information back to the government or changing how the device functions for the user. Part I of this article discusses early Fourth Amendment law grounded in trespass and the Supreme Court's later move away from trespass. Part II discusses the return of trespass in *United States v. Jones*, demonstrating how the expansion of the *Jones* theory to digital trespass would unify current case law. Part III briefly discusses how a digital trespass theory is consistent with the principles of *Katz v. United States*.[2]

I. FROM TRESPASS TO REASONABLE EXPECTATION OF PRIVACY: *OLMSTEAD* AND *KATZ*

In criminal law, whether a search has occurred is a critical finding: if there is no search, the defendant has no Fourth Amendment rights. During the early twentieth century, the Supreme Court's jurisprudence emphasized the need for a physical trespass in order for a law enforce-

† Law Clerk, U.S. District Court for the Northern District of Illinois. Many thanks to Kevin Benish for his helpful commentary on this article. All views expressed are strictly the author's.

1. 565 U.S. 400 (2012).
2. 389 U.S. 347 (1967).

ment action to qualify as a search under the Fourth Amendment.[3] However, in 1967 the Court rejected the trespass theory in favor of a more flexible reasonable expectation of privacy test. This section describes the early trespass test and its demise.

A. Olmstead*'s Trespass Rationale*

In *Olmstead v. United States*,[4] the Supreme Court emphasized that the Fourth Amendment protects physical things from physical trespass.[5] "The Amendment itself shows that the search is to be of material things—the person, the house, his papers or his effects," wrote Chief Justice Taft.[6] This focus on the physical objects examined led the Court to conclude that a wiretap was not a search when the tapped wires were outside the defendant's property.[7] After all, the "intervening wires are not part of [the defendant's] house or office, any more than are the highways along which they are stretched," so the defendant had no property interest in the wires and he and his effects were not searched.[8] This emphasis on trespass changed with the decision in *Katz v. United States* in 1967.

B. Katz *and Reasonable Expectations of Privacy*

In *Katz*, the government recorded the defendant's phone calls from a public phone booth using a tape recorder attached to the top of the phone booth.[9] Katz challenged the recordings as a warrantless search in violation of the Fourth Amendment, even though there had been no trespass against his private property. The Court concluded that "the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."[10] This explicit rejection of the trespass test led to the adoption of a two-part test, proposed in *Katz* by Justice Harlan. Under this test, a search occurs if "a person exhibit[s] an actual (subjective) expectation of privacy and, second, that the expectation [is] one that society is prepared to recognize as 'reasonable.'"[11] This reasonable expectation of privacy test replaced the trespass test in Fourth Amendment jurisprudence for 45 years until *Jones*.

---

3. *See* Goldman v. United States, 316 U.S. 129, 134 (1942) (holding police action could become an illegal search through "trespass or unlawful entry").

4. 277 U.S. 438 (1928).

5. *Id.* at 464.

6. *Id.* Note that in the case of digital trespass, the physical device itself is being provoked to respond and reveal information, so the focus on interaction with physical objects remains similar to that in *Olmstead*.

7. *Id.*

8. *Id.* at 465. The Court noted that a trespass was not always sufficient for a search (as in the case where two police officers snuck onto a man's land and saw him come outside and hand a bottle to a friend). *Id.* However, it appeared there could not be a search without a trespass. *See id.*

9. Katz v. United States, 389 U.S. 347, 348 (1967).

10. *Id.* at 353.

11. *Id.* at 361 (Harlan, J., concurring).

II. TO *JONES* AND BEYOND: EXPANDING PHYSICAL TRESPASS TO DIGITAL TRESPASS

The primacy of the *Katz* test was thrown into question by the Supreme Court's decision in *United States v. Jones*. Writing for the majority, Justice Scalia reinvigorated the *Olmstead* trespass doctrine, at least in so far as trespass was an independent ground on which to find a search under the Fourth Amendment.[12] This part briefly explains the Court's reasoning in *Jones* and proposes expanding *Jones* to digital trespass—trespasses that take place entirely electronically by sending a targeted signal to a suspect's device to make it take some action. Second, it discusses a sample of Fourth Amendment cases and explains how digital trespass provides a harmonizing theory.

A. Jones *Revives Trespass Doctrine—And Potentially Creates Digital Trespass*

In *Jones*, the defendant challenged the government's secret installation of a Global Positioning System (GPS) on the bottom of the car he used as a warrantless search in violation of the Fourth Amendment.[13] The GPS sent the police data tracking Jones's movements for twenty-eight days, conveying more than 2,000 pages of data.[14] Although lower courts had previously found that GPS data generated by cell phone usage[15] was not necessarily covered by the Fourth Amendment (and therefore its use was not a search),[16] the Supreme Court found that the installation and use of the GPS was a search under the Fourth Amendment.

In his majority opinion, Justice Scalia concluded that a "physical intrusion" like the installation and use of the GPS, independent of the reasonable expectation of privacy, was a sufficient basis to find a search

---

12. One caveat to this characterization is that a trespass is only a search if information is actually discovered. The mere installation of the GPS, if it had malfunctioned and not transmitted data, would likely not have been a search, especially since the main remedy for a Fourth Amendment violation is suppression of the evidence (and if the installation fails, there is no evidence to suppress). *See* United States v. Karo, 468 U.S. 705, 712 (1984) ("A holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on.").

13. United States v. Jones, 565 U.S. 400, 402–04 (2012). The police had actually received a warrant, but did not follow the terms of its installation or use, so the Court proceeded as if there was no warrant.

14. *Id.*

15. Like the GPS in *Jones*, the phone conveys its location to a satellite, which is then reported back to a computer. *See id.* at 403.

16. *See* In re the Matter of the Appl. of the United States for an Order Directing Provider of Elec. Commun. Serv. to Disclose Records to the Gov't, 620 F.3d 304, 319 (3d Cir. 2010) (holding request to company for GPS data does not require a warrant because it is not a search); *see also* In re Appl. of the United States for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) (holding GPS data disclosed by a provider is not a search).

under the Fourth Amendment.[17]Although Justice Scalia acknowledged that the Court's post-*Katz* jurisprudence had "deviated from th[e] exclusively property-based approach" used in *Olmstead*, he concluded that "*Katz* did not repudiate [the trespass-based] understanding" of the Fourth Amendment.[18] In fact, for "most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[19]

Although this trespass approach reached the reasonable result in *Jones* itself, it creates an intriguing problem noted by both concurrences—that a digital trespass may soon allow law enforcement to receive identical GPS data about a vehicle without law enforcement physically installing a GPS.[20] Many cars now come with GPS devices built into the vehicle to assist with navigation and accident response, such as the popular OnStar system (which tracks a car's location and speed by default even if the owner is not a paying OnStar customer).[21] A government agent that remotely accessed a car's GPS so that it provided location data to a government computer would never have to commit a physical trespass.

However, *Jones*'s trespass theory need not be confined to physical trespasses, and expanding it to digital trespasses provides a logical theory for current and future case law. A digital trespass takes place whenever a government agent sends a targeted signal to a user's device, causing the device to return some information or take some action.[22] Note that the requirement of a targeted signal to a device eliminates the potential for digital plain view[23] as well as the issue of dragnet surveillance. This digi-

---

17. *Jones*, 565 U.S. at 404 ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted.").

18. *Id.* at 405.

19. *Id.*

20. *See id.* at 415 (Sotomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion on property, the majority opinion's trespassory test may provide little guidance."); *id.* at 426 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.").

21. David Kravets, *OnStar Tracks Your Car Even When You Cancel Service*, WIRED (Sept. 20, 2011), http://www.wired.com/2011/09/onstar-tracks-you/.

22. For example, the device could return its location or provide a copy of all IP addresses visited by the device. *See, e.g.*, Kim Zetter, *Secrets of FBI Smartphone Surveillance Tool Revealed in Court Fight*, WIRED (Apr. 09, 2013), http://www.wired.com/2013/04/verizon-rigmaiden-aircard/all/ (explaining the use of government configured aircard to return device's location).

23. Which, for example, might have been available if the government rather than Google had accessed the unencrypted wireless traffic in *Joffe v. Google*, 746 F.3d 920 (9th Cir. 2013). The plain view exception to the Fourth Amendment has a complicated relationship with computers. *Compare United States v. Williams*, 592 F.3d 511, 521 (4th Cir. 2010) (holding plain view exception allows search of every file on a hard drive) *with United States v. Carey*, 172 F.3d 1268 (10th Cir. 1999) (holding plain view exception does not allow search of every file on a hard drive). This debate is beyond the scope of this article.

tal trespass theory is consistent with existing trespass law and existing criminal law involving computer access.

Trespass law has never been confined to when a person physically intrudes on another's private property—it is sufficient that the trespasser has physical or legal control over the intrusion. For example, at common law, a trespass by livestock was an almost strict liability tort by the livestock owner—if Smith's cow went onto Jones's property and injured Jones, Smith could be liable even if he was not negligent in confining the cow and never set foot on Jones's land.[24] Trespass cases due to pollution are common; in many of these cases the trespasser never set foot on the contaminated land.[25] If an undirected animal or cloud of pollution interacting with another's property can be a trespass, it is hard to imagine why a directed wireless signal interacting with another's property would be any less of a trespass.

Furthermore, the idea of being able to trespass digitally on a computer, and using a computer or other technology to do so, is not novel.[26] Some states have criminalized "computer trespass" by statute.[27] Although the federal Computer Fraud and Abuse Act does not use the term "trespass," it uses similar language to the state statutes.[28] While there is an active scholarly debate about whether computer crimes should be understood in terms of physical trespass or not,[29] it is clear that trespass is a viable framework for conceptualizing gaining access to, or information from, electronic devices.

Furthermore, courts have accepted the idea that one could commit a computer trespass using other technology, rather than physically sitting down at the computer and attempting to access it. For example, in *State*

---

24. *See* James L. Rigelhaupt, Jr., *Liability for Personal Injury or Death Caused by Trespassing or Intruding Livestock*, 49 A.L.R. 4th 710, § 3(a) (2012) ("the possessor of livestock may be held liable under the rule of strict liability, in actions based on a theory of trespass, for personal injuries caused by their animals while intruding on the lands of others").

25. *See* 5-17 THE LAW OF HAZARDOUS WASTE § 17.01 (2015) (collecting cases); *see also* Jill E. Evans, *See Repose Run: Setting the Boundaries of the Rule of Repose in Environmental Trespass and Nuisance Cases*, 38 WM. & MARY ENVTL. L. & POL'Y REV. 119, 132 (2013) ("As a result, a number of environmental trespass and nuisance cases involve the unseen migration of pollutants through ground soil or groundwater onto adjoining property.").

26. The difference between using a computer to trespass and trespassing on a computer is trivial, since generally there will be computer-like technology on both ends of a digital trespass.

27. *See, e.g.*, WASH. REV. CODE § 9A.52.110 (repealed 2016) ("A person is guilty of computer trespass in the first degree if the person, without authorization, intentionally gains access to a computer system . . . and . . . [t]he access is made with the intent to commit another crime[] or . . . [t]he violation involves a computer or database maintained by a government agency.").

28. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 ("Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any department or agency of the United States[] or . . . information from any protected computer . . . shall be punished as provided in subsection (c) of this section.").

29. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1618-22 (2003) (arguing trespass is an insufficient analogy for computer crime).

v. Riley,[30] the Washington Supreme Court held that the defendant had committed a computer trespass by calling a telephone company's general access number and dialing random numbers to discover access codes to the company's computer system (which allowed the defendant to make long-distance calls while charging them to other customers).[31] The defendant unsuccessfully argued that he should be charged with telephone fraud, rather than computer trespass, because he did not directly access the data on the computer—he just entered numbers on his phone and learned whether he was able to make long-distance calls after entering the numbers.[32] The court rejected this argument, noting that Riley had "accessed" the computer in violation of the statute by "approach[ing]" or "mak[ing] use of any resources of a computer."[33] A digital trespass takes a similar form—using one piece of technology (be it a computer or more specialized device such as a Stingray[34]) to make use of the resources of another piece of technology.

B. Harmonizing Precedent with Digital Trespass

Supreme Court precedent is already consistent in many ways with the digital trespass theory described above. For example, the theory is consistent with the Court's decisions in *United States v. Karo*[35] and *United States v. Knotts*.[36] *Karo* and *Knotts* are befuddling. The two cases, decided less than two years apart, come to opposite conclusions about very similar facts. Although neither could be considered a search under the digital trespass theory due to the technology at stake, the theory is consistent with the logic underlying both decisions.

In *Knotts*, the Supreme Court found it was not a search when government agents inserted a tracking beeper, which emitted radio signals that could be picked up by radio receivers, into a container of chloroform being transported by Knotts.[37] The court found there was no search because the beeper was not relaying any new information to law enforcement—the beeper was only assisting law enforcement in their visual surveillance of the suspect as he transported the chloroform.[38] This would not be a search under a digital trespass theory either. The government receiver is not sending a targeting signal—the beeper simply emits data that can be picked up by anyone, and the government does not "ping" the beeper to ask it to return data (the beeper transmits constantly). In to-

30. 846 P.2d 1365 (Wash. 1993).
31. *Id.* at 1373.
32. *Id.*
33. *Id.*
34. For a discussion of how Stingrays can be used to gather information by law enforcement, *see* United States v. Patrick, 842 F.3d 540, 547 (7th Cir. 2016) (Wood, dissenting).
35. 468 U.S. 705 (1984).
36. 460 U.S. 276 (1983).
37. *Id.* at 277.
38. *Id.* at 281 ("The governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways.").

day's terms, replacing "beeper" and "receiver" with "computer" illustrates one limitation incorporated by the digital trespass theory, which is consistent with *Knotts*—if the government can pick up information that is being freely broadcast using a standard-issue receiver, it is not a search.

In *Karo*, the government inserted a similar beeper into a can of ether and had an informant swap the beeper can with one of the cans Karo was transporting.[39] Although the Court conceded there may have been a "technical trespass," they found the beeper's installation was not a search because the informant had agreed when the can was in his possession and the government had created only the "*potential* for an invasion of privacy."[40] However, the Court held that it *was* a search to use the beeper to gain locational information once the beeper was off public roads and on the defendant's property.[41] This focus on gaining access to otherwise unavailable (at least without a warrant) information is also reflected in the digital trespass test—the government's targeted signal must be effective in inducing a response from the suspect's device. The government's mere ability to ask a device for information cannot logically constitute a search, unless it actually asks for information from a device and receives it.[42]

Digital trespass carries forward *Knotts*'s and *Karo*'s themes that the government cannot turn a person's property into an informant, while placing reasonable restrictions on what government behavior falls into that category. *Knotts* and *Karo* teach that a digital trespass requires government officials to reach out and ask a device for nonpublic information. The modern analogue to the continually transmitting beeper on public roadways in *Knotts* is information shared on an unsecured wireless network.[43] The government need not ask the device to do anything in order to gain this information, just as the officers performed no physical trespass to follow Knotts.

In addition to this outreach requirement, as the previous analogy suggests, the government must gain new information. Not only has the government failed to ask for anything in the wireless network example, it is not receiving nonpublic information—it is simply following our modern-day Karo down public information superhighways. Once the government moves to the private level of the device and has the device re-

39. *Karo*, 468 U.S. at 708.

40. *Id.* at 712.

41. *Id.* at 715.

42. This approach is also consistent with lower court approaches to GPS data. For example, the Fifth Circuit found that government's request for historical cell site data were not a search because the cell phone companies generate and keep locational data for their own business purposes and the government was not involved in their generation or retention. In re Application of the United States for Historical Cell Site Data, 724 F.3d 600, 611–12 (5th Cir. 2013).

43. *See* United States v. Stanley, 753 F.3d 114, 114 (3d Cir. 2014) (finding no search where defendant's computer was located through its connection to an unsecured wireless network).

turn information that was not being shared, the government has stepped off the highway and onto the private property (for instance, the hard drive). At that point, the government has committed a trespassing search as in *Karo*.

III. DIGITAL TRESPASS AND FOURTH AMENDMENT VALUES

Although the majority in *Jones* noted that "*Katz* did not narrow the Fourth Amendment's scope" and the *Olmstead* test provides an independent basis for finding a search,[44] the digital trespass test is consistent with the reasonable expectation of privacy test that dominated a half-century of precedent. At least one court has disagreed, finding that a defendant did not have a reasonable expectation of privacy in his devices when the government used technology to find and reprogram his aircard (a way of wirelessly accessing the internet from a laptop).[45] However, the digital trespass test is consistent with the *Katz* test. Furthermore, it protects the notice interest reflected in both statutory law and the values of *Katz*.

As discussed above, the *Katz* test requires a subjective expectation of privacy that society is prepared to recognize as reasonable.[46] Especially in an age where so many programs and apps default to sharing (consider, for example, when a PC asks if the user would like to share his or her files upon joining a wireless network or more insidious sharing defaults within social media applications), the user's decision to not broadcast certain information is good evidence of a subjective expectation of privacy.[47] Moreover, the public has expressed outrage at government monitoring of electronic devices such as computers and GPS-enabled phones. One Gallup poll found that 53% of Americans disapprove of the government "compil[ing] telephone call logs and Internet communications" while the same study found 57% would be somewhat or very concerned their privacy rights had been violated if they were surveilled electronically.[48] This concern has manifested itself in calls for greater en-

---

44. United States v. Jones, 132 S. Ct. 945, 951 (2012).

45. United States v. Rigmaiden, 2013 U.S. Dist. LEXIS 65633, at *25–26 (D. Ariz. May 8, 2013). The court's opinion is not a model of clear reasoning and includes the fact that the devices were used in an "extensive scheme of fraud" as a reason to deny a reasonable expectation of privacy. Presumably use in a crime cannot dictate the boundaries of the Fourth Amendment, because otherwise criminals would never have Fourth Amendment rights.

46. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

47. Whether unsecured file sharing or wireless networks eliminates a reasonable expectation of privacy is an undecided topic. *Compare* United States v. Ahrndt, 2013 U.S. Dist. LEXIS 7223 (D. Or. Jan. 17, 2013) (finding search despite having shared files with wireless network) *with* United States v. Stanley, 753 F.3d 114 (3d Cir. 2014) (finding no reasonable expectation of privacy in location of computer after connecting to unsecured wireless network). Under either standard, the use of a secured network and applications to prevent dissemination of information reflects a subjective expectation of privacy.

48. Frank Newport, *Americans Disapprove of Government Surveillance Programs*, GALLUP (June 12, 2013) http://www.gallup.com/poll/163043/americans-disapprove-government-surveillance-programs.aspx.

cryption of cell phones and other devices, as Representative Ted Lieu recently noted during hearings on encryption.[49] It seems clear from these statistics that the public is prepared to recognize, and believes it has, an expectation of privacy in the information collected by electronic devices. Under these circumstances, the *Katz* test is satisfied and government's technical manipulation to gain the information on these devices is a search.

Finally, the digital trespass rule protects individuals from unknown, and perhaps unknowable, searches of their electronic devices. When police perform a search under the *Katz* test, they must get a warrant (or consent), which informs the person that a search is taking place. Otherwise a person can assume that her information is safe and conduct her business accordingly. Recognizing this interest in people knowing when they are being monitored, statutes such as the Stored Communications Act (which covers electronic communications data not protected by the Fourth Amendment) require notice to the target.[50] These notice provisions are essential, as otherwise citizens might curtail their activities just in case they are being surveilled.[51]

A digital trespass theory of Fourth Amendment searches is necessary to maintain the relevance of the Supreme Court's *Jones* decision in an age of increasingly pervasive technology. Although a physical trespass may no longer be necessary to track our movements, communications, or contacts, the government is still taking a targeted action to acquire information it could not otherwise gather. Neither existing trespass law, existing criminal law, nor existing Fourth Amendment law bars the expansion of *Jones* to digital trespasses. Doing so would protect the privacy of Americans in the twenty-first century and ensure our actions remain unconstrained by the fear of secret surveillance.

---

49. Cyrus Farivar, *Irate Congressman Gives Cops Easy Rule: "Just Follow the Damn Constitution,"* WIRED (Apr. 30, 2015), http://arstechnica.com/tech-policy/2015/04/30/irate-congressman-gives-cops-easy-rule-just-follow-the-damn-constitution/.

50. This notice can be delayed up to 90 days after the surveillance if certain conditions are met. 18 U.S.C. § 2705.

51. There is evidence journalists have changed their behavior in response to the disclosure of NSA surveillance programs. *With Liberty to Monitor All: How Large Scale US Surveillance is Harming Journalism, Law, and American Democracy*, HUMAN RIGHTS WATCH (July 2014), https://www.aclu.org/sites/default/files/field_document/dem14-withlibertytomonitorall-07282014.pdf.