SPECIAL DELIVERY: ALLOW TWO TO THREE WEEKS FOR SHIPPING . . . AND NSA BUGGING

SARAH O'DONOHUE*

I. INTRODUCTION 81
II. THE FOURTH AMENDMENT AND ELECTRONIC MONITORING 83
A. Olmsted v. United States *and* Katz v. United States 83
B. *The Third-Party Doctrine and* United States v. Jones 86
III. THE PROBLEMATIC PRECEDENT SET BY *KNOTTS* AND *KARO* 89
A. United States v. Knotts 89
B. United States v. Karo 91
IV. THE REJECTION OF *KNOTTS* AND *KARO* BY TWO STATE SUPREME COURTS 95
A. People v. Oates 95
B. State v. Kelly 97
C. *The Need for Uniformity in the Law* 99
V. WHY THE UNITED STATES SUPREME COURT SHOULD OVERTURN *KNOTTS* AND *KARO* 100
A. *A Manufacturer's Consent to the Installation of a Monitoring Device Is Invalid* 100
B. *New Electronic Monitoring Technologies Pose Greater Threats to Privacy Than Locational Tracking Devices* 104
C. *The Trespass Theory of the Fourth Amendment Has Been Liberally Construed* 105
VI. CONCLUSION 108

I. INTRODUCTION

It is widely known that the National Security Agency intercepts communications sent over the Internet, but now the agency is increasingly making use of radio technology that allows it to enter and alter data in computers that are offline.[1] Government documents leaked by former NSA contractor Edward Snowden revealed that since at least 2008, the agency has inserted special circuit boards and USB cards into approximately 100,000 computers manufac-

* Attorney, Alston & Bird LLP; J.D., Emory University School of Law, 2014; B.A., Political Science and Classical Studies, Vanderbilt University, 2010. I would like to thank Professor Morgan Cloud for his invaluable assistance while I was writing this Article and for his support and mentoring throughout my law school career.

[1] David E. Sanger & Thom Shanker, *N.S.A. Devises Radio Pathway into Computers*, N.Y. TIMES, Jan. 15, 2014, at A1.

tured by Cisco, Dell, and Hewlett-Packard before the computers are delivered to consumers worldwide.[2] The hardware is implanted by government agents either while the computers are still in the factory or after they have been diverted to a "load station" during shipment.[3] These devices transmit radio waves to a portable relay station that can be set up as far away as eight miles from the target computer and allow surveillance to continue "even while the computer's user enjoys the false confidence that being walled off from the Internet constitutes real protection."[4] The agency insists that its "activities are focused and specifically deployed against—and only against—valid foreign intelligence targets in response to intelligence requirements."[5] The NSA further claims that this surveillance is being conducted to "serve as an early warning system for cyberattacks directed at the United States."[6] *The New York Times* reports that so far "[t]here is no evidence that the NSA has implanted its software or used its radio frequency technology inside the United States."[7] But if law enforcement and intelligence officials do in fact use such technology in the United States, is it constitutional under the Fourth Amendment?

This Article explains that the NSA's practice of installing spyware in personal computers is constitutional under the trespass theory of the Fourth Amendment set forth in *United States v. Knotts*[8] and *United States v. Karo*[9] because the computers are not consumers' "effects" until they are delivered. Courts evaluating Fourth Amendment claims brought against the NSA will therefore be forced to resort to the reasonable-expectation-of-privacy test adopted in *Katz v. United States*.[10] However, this Article argues that the *Katz* test is insufficient in the face of new technologies. Thus, rather than forcing defendants and courts to apply the problematic *Katz* test, this Article contends that the precedent set by *Knotts* and *Karo* should be overturned. Part II of this Article begins by providing an overview of Fourth Amendment jurisprudence with a focus on electronic monitoring. Part III reviews *Knotts* and *Karo*, and then Part IV describes their almost-immediate rejection by two state supreme courts. Finally, Part V sets forth the bases for this Article's conclusion that *Knotts* and *Karo* should no longer be considered good law.

---

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.*

[8] United States v. Knotts, 460 U.S. 276, 277 (1983).

[9] United States v. Karo, 468 U.S. 705, 707 (1984).

[10] Katz v. United States, 389 U.S. 347 (1967).

II. The Fourth Amendment and Electronic Monitoring

A. Olmsted v. United States *and* Katz v. United States

Thirty years ago, the electronic beeper, another type of "radio transmitter . . . [that] emits periodic signals that can be picked up by a radio receiver" from a short distance away, raised Fourth Amendment concerns when employed by law enforcement agents to monitor criminal suspects.[11] Before detailing the evolution of government spy tools from electronic beepers, to GPS tracking units, to the circuit boards and USB cards currently used by the NSA and their treatment in various invasion of privacy cases, this Article sets the stage with an overview of Fourth Amendment jurisprudence. 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."[12] A search or seizure is considered "unreasonable" when the government does not possess a warrant supported by probable cause.[13] To claim the Fourth Amendment's protections, a person must have a legitimate expectation of privacy in the place searched or the items seized.[14] The Supreme Court has defined such an expectation of privacy as one "that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."[15] Indeed, the constitutional right to privacy was traditionally interpreted as protecting against government invasion of an individual's property interest, and thus only physical trespasses into "material things—the person, the house, his papers or his effects"—constituted searches.[16]

The purely property-based conception of the Fourth Amendment began to change with *Olmstead v. United States*.[17] In that case, the Supreme Court considered whether government interception of the defendants' private conversations using wiretaps placed on public telephone lines outside their homes and offices violated the Fourth Amendment.[18] The Court held that because the telephone lines were "not part of [the defendants'] house[s] or office[s] any more than . . . the highways along which they are stretched," there was no physical trespass or infringement upon their property interests and, therefore, no search.[19] Rather, "the evidence was secured by the use of the sense of hearing

---

[11] United States v. Knotts, 460 U.S. 276, 277 (1983).

[12] U.S. Const. amend. IV.

[13] *Id.*

[14] Minnesota v. Carter, 525 U.S. 83, 88 (1998).

[15] *Id.*

[16] Olmstead v. United States, 277 U.S. 438, 463–64 (1928).

[17] *Id.* at 438.

[18] *Id.* at 455.

[19] *Id.* at 465. *But cf.* Silverman v. United States, 365 U.S. 505, 509, 512 (1961) (holding that the government's insertion of a microphone into a heating duct in the defendant's house was "an unauthorized physical penetration" that violated the Fourth Amendment).

and that only."[20] Similarly, there was no seizure because the Fourth Amendment only applies to tangible property and not to the intangible spoken words of the defendants' conversations.[21]

In his famous dissent, Justice Brandeis argued that such a literal reading of the Fourth Amendment failed to recognize that conceptions of privacy must evolve in tandem with technology.[22] Echoing the introduction to his and Samuel Warren's seminal law review article *The Right to Privacy*,[23] Justice Brandeis stated, "[T]ime works changes [and] brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government" which threaten to cause "disclosure in court of what is whispered in the closet."[24] Furthermore, because "[t]he progress of science in furnishing the government with means of espionage is not likely to stop with wiretapping," Justice Brandeis criticized the limited scope of the Fourth Amendment protection adopted by the majority.[25] Even the inner sanctum of the home—an area specifically mentioned in the text of the Constitution—could lose its Fourth Amendment protection if the government developed ways to reproduce private papers in court "without removing [them] from secret drawers," thereby "expos[ing] to a jury the most intimate occurrences of the home."[26] Justice Brandeis proposed that the Fourth Amendment should instead be interpreted to encompass changes in technology so that new developments would not eviscerate the most traditional notions of privacy.[27] When applying the Constitution, he argued, the Court must consider not only "what

---

[20] *Olmstead,* 277 U.S. at 464–65; *accord* Goldman v. United States, 316 U.S. 129, 135 (1942) (concluding that no search occurred where a "detectaphone" was placed on the outer wall of the defendant's office for the purpose of overhearing conversations held within the room).

[21] Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology, and the Fourth Amendment*, 72 MISS. L.J. 5, 16 (2002).

[22] *Olmstead*, 277 U.S. at 472–73, 476 (Brandeis, J., dissenting) ("Clauses guaranteeing to the individual protection against specific abuses of power[ ] must have a . . . capacity of adaptation to a changing world.").

[23] The following statement in Justice Brandeis's dissent bears striking resemblance to the law review article he co-authored 38 years earlier: "The makers of our Constitution . . . knew that only a part of the pain, pleasure, and satisfactions of life are to be found in material things. They sought to protect Americans in their beliefs, their thoughts, their emotions, and their sensations. They conferred, as against the government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men." *Id.* at 478. *Compare with* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).

[24] *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

[25] *Id.* at 474.

[26] *Id.* at 473.

[27] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 580 (2009).

has been, but [also] what may be."[28] Accordingly, to protect the defendants' constitutional right to privacy, Justice Brandeis would have excluded the evidence obtained by wiretapping.[29] He contended that it was necessary to move away from the property-based theory of the Fourth Amendment because the invention of the telephone had changed the way that private communications were conducted, the societal conception of privacy, and, inevitably, the notion of "trespass."[30]

Justice Brandeis's view of the Fourth Amendment was vindicated in *Katz v. United States*, where the use of wiretaps was again at issue.[31] In that case, the government placed wiretaps on a telephone in a public booth in order to listen to and record the defendant's conversations.[32] Following the Supreme Court's decision in *Olmstead*, the Court of Appeals in *Katz* held that the recordings were not obtained in violation of the Fourth Amendment because there was no physical entrance into an area occupied by the defendant.[33] The Supreme Court, however, began its analysis by announcing that "the Fourth Amendment protects people, not places."[34] The Court then overruled *Olmsted*, reasoning that the constitutional right to privacy "cannot turn on the presence or absence of a physical intrusion into any given enclosure."[35] The Court explained that "the 'trespass' doctrine [ ] enunciated [in *Olmstead*] can no longer be regarded as controlling";[36] instead, for Fourth Amendment claims the inquiry is whether the defendant sought to preserve the privacy of his communications—even those made in a "public" place.[37] When Charles Katz occupied the telephone booth, he shut the door behind him and paid the toll to place a call, so "surely [he was] entitled to assume that the words he utter[ed] into the mouthpiece [would] not be broadcast to the world."[38]

However, *Katz* is best known for the statements made by Justice Harlan in his concurring opinion, which clarified that a person's intention to preserve the privacy of his "objects, activities, or statements" is determined by a two-pronged test.[39] First, the person must "have exhibited an actual (subjective) expec-

---

[28] *Olmstead*, 277 U.S. at 474 (Brandeis, J., dissenting).

[29] *Id.* at 478–79.

[30] *Id.* at 479 (declaring that the location of the physical connection of telephone wires leading into the defendants' homes and offices is immaterial to the Fourth Amendment analysis).

[31] Katz v. United States, 389 U.S. 347 (1967).

[32] *Id.* at 348.

[33] *Id.* at 348–49.

[34] *Id.* at 351.

[35] *Id.* at 353.

[36] *Id.*

[37] *Id.* at 351.

[38] *Id.* at 352.

[39] *Id.* at 361 (Harlan, J., concurring).

tation of privacy."[40] Second, that expectation must "be one that society is prepared to recognize as 'reasonable.'"[41] This test was later adopted by the majority in *Smith v. Maryland* as the method for determining whether the government has invaded a person's constitutional right to privacy.[42] Like Justice Brandeis nearly forty years earlier, the Court in *Katz* recognized the important role that technology plays in privacy law by holding that the government's wiretapping constituted a search and seizure within the meaning of the Fourth Amendment.[43] The fact that the electronic device did not penetrate the wall of the telephone booth had no constitutional significance because "[t]o read the Constitution more narrowly [would be] to ignore the vital role that the public telephone has come to play in private communication."[44]

B. *The Third-Party Doctrine and* United States v. Jones

Although the *Katz* Court broadened Fourth Amendment protection by holding that private communications conducted in a public place can receive Fourth Amendment protection, the Court made clear that a privacy expectation is no longer reasonable when an individual discloses the item or information in question to a third party. According to the third-party doctrine, "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[45] Nine years later, the Court applied this principle in *United States v. Miller* and found no constitutional right to privacy in bank records that were not in the defendant's sole possession.[46] Justice Blackmun's statement in *Smith v. Maryland* that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" articulates the third-party doctrine as it stands today.[47] In the context of computers—the latest technology to play a "vital role . . . in private communication"[48]—courts have held that because of the third-party doctrine, "a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any measures to protect [it]."[49]

---

[40] *Id.*

[41] *Id.*

[42] Smith v. Maryland, 442 U.S. 735, 740 (1979).

[43] *Katz*, 389 U.S. at 353.

[44] *Id.* at 352–53.

[45] *Id.* at 351. This statement echoed the *Olmstead* Court's view "that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and [thus] the wires beyond his house, and the messages while passing over them, are not within the protection of the Fourth Amendment." Olmstead v. United States, 277 U.S. 438, 456–66 (1928).

[46] United States v. Miller, 425 U.S. 435, 440, 442 (1976).

[47] *Smith*, 442 U.S. at 743–44.

[48] *Katz*, 389 U.S. at 352–53.

[49] United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002).

The legitimacy of the third-party doctrine and the viability of the trespass theory of the Fourth Amendment were recently addressed by the Supreme Court in *United States v. Jones*.[50] Officers installed a GPS tracking device on the undercarriage of Antoine Jones's vehicle as part of an investigation of his suspected narcotics trafficking.[51] The device tracked the vehicle's movements and communicated its location to a government computer, generating over 2,000 pages of data over the 28-day monitoring period.[52] Jones moved to suppress this evidence, but the district court held that the majority of the data was admissible because, under the third-party doctrine, Jones had no reasonable expectation of privacy in the locations and movements of his vehicle on public roads that were visible to all.[53] Based on the evidence obtained through the GPS device, Jones was convicted of various drug-related crimes.[54]

Justice Scalia began the Supreme Court's majority opinion by asserting that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[55] As a result, *Katz* in no way eroded the principle that, without a warrant, a physical intrusion by the government into a constitutionally protected area violates the Fourth Amendment.[56] Justice Scalia explained that *Katz* merely established that "property rights are not the sole measure of Fourth Amendment violations"; it did not "snuf[f] out the previously recognized protection for property."[57] At a minimum, the Court must "assure[ ] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted,"[58] and Jones's vehicle is undeniably an "effect" as that term was used in the Constitution.[59] Therefore, the warrantless installation of the GPS device—a physical intrusion on private property—was an unreasonable search, and Jones's conviction was overturned.[60]

The concurring opinions by Justices Sotomayor and Alito raised critical Fourth Amendment issues that *Jones* majority left unresolved. Justice Sotomayor pointed out that the type of physical intrusion at issue in *Jones*—government installation of a monitoring device on a vehicle owned and regularly used by a criminal suspect—will soon be unnecessary in order to conduct surveillance.[61] Rather, "[w]ith increasing regularity, the Government will be

---

[50] United States v. Jones, 132 S. Ct. 945 (2012).

[51] *Id.* at 948.

[52] *Id.*

[53] *Id.*

[54] *Id.*

[55] *Id.* at 951.

[56] *Id.* at 950, 952.

[57] Soldal v. Cook Cnty., 506 U.S. 56, 64 (1992).

[58] Kyllo v. United States, 533 U.S. 27, 34 (2001).

[59] *Jones*, 132 S. Ct. at 949.

[60] *Id.* at 949, 954.

[61] *Id.* at 955 (Sotomayor, J., concurring).

capable of duplicating the monitoring undertaken in this case" without trespassing on an effect already in the suspect's possession "by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones."[62] Like Justice Brandeis in his *Olmstead* dissent, Justice Sotomayor cautioned that such electronic surveillance techniques are especially problematic because they are cheap and, by design, "proceed[ ] surreptitiously" and "evade[ ] the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'"[63] Furthermore, she noted that the third-party doctrine will not be helpful in resolving these types of technologically advanced monitoring cases because the 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."[64]

Justice Alito likewise explained that under the trespass theory of the Fourth Amendment, "if long-term monitoring can be accomplished without committing a . . . trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car"—then the future owner of the car would have no constitutional protection.[65] In fact, the Fourth Amendment only applied in *Jones* "because the officers installed the GPS device *after* [Jones]'s wife, to whom the car was registered, turned it over to [him] for his exclusive use. . . . [I]f the GPS device had been installed *before* [Jones]'s wife gave him the keys, [he] would have had no . . . Fourth Amendment claim . . . ."[66] Indeed, because of two Supreme Court cases from the 1980s involving electronic beepers—the precursor to GPS devices—the trespass theory Justice Scalia advocated in *Jones* provides a criminal defendant no recourse in cases where officers activate "a stolen vehicle detection system that came with the car when it was purchased."[67]

In *United States v. Knotts*,[68] the Court held that the installation of a beeper was not a trespass because it "had been placed in the container [later delivered to the defendant] before it came into [his] possession, with the consent of the then-owner," the manufacturer.[69] As the Court made clear one year later in *United States v. Karo*,[70] the government's use of such electronic surveillance is permissible because "[the defendant] accepted the container as it came to him, beeper and all, and was therefore not entitled to object to the beeper's presence, even though it was used to [track his] . . . location."[71] If the precedent set by

---

[62] *Id.*

[63] *Id.* at 956 (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004)).

[64] *Id.* at 957.

[65] *Id.* at 961 (Alito, J., concurring).

[66] *Id.* (emphases added).

[67] *Id.* at 962.

[68] United States v. Knotts, 460 U.S. 276 (1983).

[69] *Jones*, 132 S. Ct. at 952 (majority opinion).

[70] U.S. v. Karo, 468 U.S. 705, 707 (1984).

[71] *Jones*, 132 S. Ct. at 952 (majority opinion).

Knotts and *Karo* makes the trespass theory inapplicable to the electronic monitoring described by Justices Sotomayor and Alito, then courts will be forced to resort to the *Katz* reasonable-expectation-of-privacy test when evaluating Fourth Amendment claims.[72] The *Katz* test not only raises third-party doctrine questions but also "involves a degree of circularity, and judges are apt to confuse their own expectations of privacy with those of the hypothetical person to which the . . . test looks."[73] In addition, this hypothetical reasonable person does not have a well-developed and stable set of privacy expectations; rather, his expectations change along with new technological developments.[74]

This Article argues that the NSA's latest surveillance program is the equivalent of the government activity that Justices Sotomayor and Alito feared. But instead of working with auto manufacturers to install GPS tracking devices, the agency is teaming up with major computer companies to install spyware in products that criminal suspects have ordered. Such investigatory techniques are constitutional under the trespass theory of the Fourth Amendment because the computers are not the consumers' "effects" until they are delivered. The concurring opinions in *Jones* identified that this poses a critical problem for search and seizure law. As discussed below, rather than turning to the untenable *Katz* test, the problematic precedent set by *Knotts* and *Karo* should be overturned.

III. THE PROBLEMATIC PRECEDENT SET BY *KNOTTS* AND *KARO*

A. United States v. Knotts

Leroy Knotts and his co-defendants Tristan Armstrong and Darryl Petschen were suspected of producing illicit drugs.[75] During their investigation, Minnesota narcotics officers got word that Armstrong had stolen chemicals from his former employer and was seen purchasing similar products from another company.[76] The officers arranged for the chemical company to install an electronic beeper inside a five-gallon drum of chloroform, "one of the so-called 'precursor' chemicals used to manufacture illicit drugs."[77] The owner of the company agreed that when Armstrong next purchased chloroform, it would be placed in the drum with the beeper.[78] As planned, Armstrong made the purchase and stored the drum in his car.[79] The narcotics officers followed the car, tracking it with both visual surveillance and a radio receiver that picked up the signals sent

---

[72] *Id.* at 962 (Alito, J., concurring).
[73] *Id.*
[74] *Id.*
[75] United States v. Knotts, 460 U.S. 276, 277 (1983).
[76] *Id.* at 278.
[77] *Id.*
[78] *Id.*
[79] *Id.*

by the beeper.[80] Armstrong transferred the drum to Petschen, who then drove it in his own car to a cabin owned by Knotts.[81] During the trip to the cabin, the officers lost sight of Petschen's car and could not track the signal from the beeper.[82] After about an hour without visual or electronic surveillance, they located the cabin through a helicopter containing a second radio receiver that traced the beeper's signal to a rural town in Wisconsin.[83] The officers then obtained a search warrant based on "the location of the chloroform derived through the use of the beeper and additional information obtained during three days of intermittent visual surveillance of [Knotts]'s cabin."[84] In the search of the cabin, they discovered a drug laboratory, formulas for amphetamine and methamphetamine, and enough chemicals to produce fourteen pounds of pure amphetamine.[85] The drum of chloroform was found outside the cabin under a barrel.[86]

After being indicted for various drug-related offenses, the defendants moved to suppress the evidence obtained from the warrantless monitoring of the beeper, which they claimed violated their right to privacy guaranteed by the Fourth Amendment.[87] The district court denied the motion, and the defendants were convicted.[88] The Supreme Court upheld the conviction, concluding that "[t]he governmental surveillance conducted by means of the beeper" was not a search or seizure because it "amounted principally to the following of an automobile on public streets and highways," where, under the third-party doctrine, the driver has no reasonable expectation of privacy.[89] Claiming that if the beeper had not been used, "[v]isual surveillance from public places along Petschen's route or adjoining Knotts'[s] premises would have sufficed to reveal all of [the relevant] facts," the Court held that "[n]othing in the Fourth Amendment prohibited the police from augmenting [their] sensory faculties . . . with

---

[80] *Id.*

[81] *Id.* at 277–78.

[82] *Id.* at 278.

[83] *Id.*

[84] *Id.* at 279.

[85] *Id.*

[86] *Id.*

[87] *Id.*

[88] *Id.*

[89] *Id.* at 281–85 ("When Petschen travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was traveling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property). *See also* United States v. Barraza-Maldonado, 879 F. Supp. 2d 1022, 1029 (D. Minn. 2012) ("Because [the defendant] voluntarily conveyed his progress and route to anyone who wanted to look by driving on public roads, he could not reasonably have expected privacy in the location of his [vehicle]." (internal quotation marks omitted)).

such enhancement [provided by] science and technology."[90] Like the *Olmstead* Court over a half-century earlier, the Court insisted that just because "the beeper enabled the police to be more effective in detecting crime" did not make its use unconstitutional.[91]

But was the installation of the beeper constitutional in the first place? This question is more relevant when considering the new surveillance devices employed by the NSA that relay information to government agents even when the computers are not connected to the Internet—and thus their users are not voluntarily conveying anything to the public. In his concurrence in *Knotts*, Justice Brennan stated that "this would have been a much more difficult case if [the defendants] had challenged, not merely certain aspects of the monitoring of the beeper . . ., but also its original installation."[92] The principle of caveat emptor did not suffice because "[t]he government [was] not . . . defending against a claim for damages in an action for breach of a warranty; it [was] attempting to justify the legality of a search conducted in the course of a criminal investigation."[93] Justice Brennan opined that there is no constitutionally significant difference between installing a beeper on an object already in a criminal suspect's possession and "arranging that [the suspect] be sold an object that, unknown to him, already has a beeper installed inside it."[94]

B. United States v. Karo

One year later, in *United States v. Karo*, the Court addressed two questions left open by *Knotts*: (1) Does the installation of a beeper in a container "with the consent of the original owner constitute a search or seizure . . . when the container is delivered to a buyer having no knowledge of the presence of the beeper?" and (2) Does the monitoring of a beeper's signal implicate the Fourth Amendment "when it reveals information that could *not* have been obtained through visual surveillance?"[95] James Karo and his co-defendants had ordered fifty gallons of ether from a photo design company for use in extracting cocaine from clothing that was imported into the United States.[96] With the consent of the company's owner, Drug Enforcement Agency officers "substituted their own can of ether containing a beeper for one of the cans in the shipment and then had all 10 cans painted to give them a uniform appearance."[97] Using the beeper, the government tracked the can of ether as it was moved among various

---

[90] *Knotts*, 460 U.S. at 282.

[91] *Id.* at 284; *see also* Olmstead v. United States, 277 U.S. 438, 464–65 (1928).

[92] *Knotts*, 460 U.S. at 286 (Brennan, J., concurring).

[93] *Id.*

[94] *Id.*

[95] United States v. Karo, 468 U.S. 705, 707 (1984) (emphasis added).

[96] *Id.* at 708.

[97] *Id.*

residences and commercial storage lockers.[98] Eventually, the defendants were arrested for possession of cocaine with the intent to distribute, and before trial they moved to suppress the evidence obtained through the use of the beeper.[99] The district court granted the motion, and the Court of Appeals affirmed, "holding that a warrant was required to install the beeper in one of the 10 cans of ether and to monitor it in private dwellings and storage lockers."[100]

The Supreme Court reversed, concluding that there was no Fourth Amendment violation because "[t]he can into which the beeper was placed belonged at the time to the DEA, and by no stretch of the imagination could it be said that the [defendants] had any legitimate expectation of privacy in it."[101] Furthermore, even if the agents had placed the beeper into one of the original 10 cans of ether, those cans "belonged to, and were in the possession of," the photo design company, and therefore the owner's "consent was sufficient to validate the placement of the beeper in the can."[102] The Court of Appeals had also acknowledged that before Karo took control of the ether, the DEA and the chemical company could do whatever they liked with the cans without violating Karo's rights.[103] But where the two courts differed was that the intermediate court believed that a Fourth Amendment violation occurred when the beeper-laden can was transferred to Karo because "[a]ll individuals have a legitimate expectation of privacy that objects coming into their rightful ownership do not have electronic devices attached to them . . . that would give law enforcement agents the opportunity to monitor the locations of the objects at all times and in every place that [they] are taken."[104] The Supreme Court, on the other hand, opined that Karo accepted the container as it came to him, beeper and all and that "[t]he mere transfer . . . of a can containing an unmonitored beeper infringed no privacy interest"—"[i]t conveyed no information that Karo wished to keep private, for it conveyed no information at all."[105]

While Karo's Fourth Amendment rights were not violated by the installation of the beeper, they were violated by the use of the beeper to monitor the can's movements inside private areas that were concealed from public view.[106] The

---

[98] *Id.* at 708–10.

[99] *Id.* at 710.

[100] *Id.* (citing United States v. Karo, 710 F.2d 1433 (10th Cir. 1983)).

[101] *Id.* at 711.

[102] *Id.*

[103] United States v. Karo, 710 F.2d 1433, 1438 (10th Cir. 1983).

[104] *Id.*

[105] *Karo*, 468 U.S. at 712. *But cf.* On Lee v. United States, 343 U.S. 747, 751–52 (1952) (holding that there was no search or seizure where an informant, who was wearing a concealed microphone, was invited into the defendant's house and their conversation was recorded by the police).

[106] *Karo*, 468 U.S. at 713–14; *cf.* United States v. Knotts, 460 U.S. 276, 281–85 (1983) (holding that no Fourth Amendment violation was committed by monitoring a beeper in a chloroform drum placed in a vehicle because the movements of the vehicle and the transfer

Court admitted that "[t]he monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact about the interior of the premises that the Government is extremely interested in knowing and that it could not have otherwise obtained without a warrant"—the can's location.[107] Further explaining its point, the Court compared this case to *United States v. White*, where the government's recording of conversations using concealed radio transmitters worn by informants was deemed constitutional.[108] The Court reasoned that although a person may have no reasonable expectation that a guest in his home will not bring a bugged object, in this case none of Karo's co-conspirators consented to the placement of the beeper in the can of ether: "Surely if the Government surreptitiously plants a listening device on an unsuspecting household guest . . . and then monitors conversations with the homeowner, the homeowner could challenge the monitoring . . . regardless of the fact that he did not have power to give effective consent to the search of the visitor."[109]

However, three Justices dissented in part because they believed that Karo and his co-defendants—not the owner of the photo design company—should have been the ones with the power to consent to the search or seizure of the can of ether, and that the installation of the beeper thus violated the Fourth Amendment.[110] Earlier in the term, the Court had decided *United States v. Jacobsen*, in which it made clear that the Fourth Amendment offers two kinds of protections: one for "searches," which occur when an individual's reasonable expectation of privacy is infringed, and another for "seizures," which involve a meaningful interference with an individual's possessory interests in his property.[111] Justice Stevens, joined by Justices Brennan and Marshall, wrote separately in *Karo* to explain that while he agreed with the majority that beeper surveillance revealing the location of an object within a private residence or storage locker—a fact that could not be visually verified—constituted a search within the meaning of the Fourth Amendment, there was also a seizure at issue in *Karo*.[112] By attaching the electronic beeper to the can of ether, the government effectively seized the property because it interfered with Karo's right to exclude others and to use the can exclusively for his own purposes.[113] As de-

---

of the drum to an area *outside* of a private residence could have been observed by the naked eye).

[107] *Karo*, 468 U.S. at 715.

[108] *Id.* at 716 n.4 (citing United States v. White, 401 U.S. 745 (1971)).

[109] *Id.* (internal quotation marks omitted). Even the *White* Court recognized the substantial distinction between "[r]evelations to the Government by a party to conversations with the defendant" and monitoring those conservations without the knowledge or consent of the parties participating in them. *White*, 401 U.S. at 749.

[110] *Karo*, 468 U.S. at 729 (Stevens, J., concurring in part and dissenting in part).

[111] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

[112] *Karo*, 468 U.S. at 728 (Stevens, J., concurring in part and dissenting in part).

[113] *Id.*

scribed in *Jacobsen*, this interference was "meaningful" because "the character of the [can was] profoundly different when infected with an electronic bug than when it [was] entirely germ free."[114] Justice Stevens maintained that it was irrelevant that the beeper was installed before the cans that Karo purchased were delivered to him: "Once the delivery had been effected, the container was [the defendants'] property from which they had the right to exclude all the world. It was at that point that the infringement of this constitutionally protected interest began."[115]

Although "[a]s a general matter, the private citizen is entitled to assume, and in fact does assume, that his possessions are not infected with concealed electronic devices," in this case the government asserted dominion and control over the can of ether by covertly installing a beeper inside, thereby seizing the property "in the most basic sense of the term."[116] Just as the officers in *Silverman v. United States* were only able to overhear the defendants' conversations by inserting a microphone into the heating duct of their apartment building,[117] "[h]ere too, by attaching a monitoring device to [the defendants'] property, the agents usurped a part of [the] property."[118] This seizure of the can of ether led to a search when Karo brought the object into his house and concealed it from public view.[119] While the third-party doctrine makes clear that the Fourth Amendment does not protect what is exposed to the public, those who take steps to conceal an item's possession and location have a reasonable expectation that it will remain private.[120] When the DEA agents installed the beeper in the can of ether and relied on that device to track the can as it made its way into storage lockers and private residences, they violated the protections guaranteed by the Fourth Amendment.[121] Whereas in *Knotts*, "the agents already saw the codefendant take possession of [the] chloroform," learned nothing about the interior of Knotts's cabin, and accomplished no more than they would have without the aid electronic surveillance, "the agents [in *Karo*] learned who had the container and where it was only through the use of the beeper."[122]

---

[114] *Id.*

[115] *Id.* at 728 n.2. The other six Justices believed that the Fourth Amendment was first implicated in this case when the beeper was activated, not when it was transferred in the can to the defendants.

[116] *Id.* at 730, 735.

[117] Silverman v. United States, 365 U.S. 505 (1961).

[118] *Karo*, 468 U.S. at 730 (Stevens, J., concurring in part and dissenting in part).

[119] *Id.* at 735.

[120] *Id.* at 735 n.8.

[121] *Id.* at 734–35.

[122] *Id.* at 733 (Stevens, J., concurring in part and dissenting in part).

IV. THE REJECTION OF *KNOTTS* AND *KARO* BY TWO STATE SUPREME COURTS

Less than a year after the Supreme Court decided *Karo*, the high courts in Colorado and Hawaii considered cases with very similar facts and asserted they were "not content, as was the Court in *Karo*, to view the actual installation of the beeper as constitutionally insignificant apart from [the] subsequent monitoring."[123] To better protect their citizens from governmental invasion of privacy, these courts determined that the search and seizure provisions in their state constitutions prohibited the warrantless installation of an electronic tracking device in an item that an individual has paid for but not yet taken possession of.[124]

A. People v. Oates

In *People v. Oates*, the defendants were charged with manufacturing and possessing controlled substances.[125] During the investigation leading to the charges, the DEA received a tip from the general manager of a Texas chemical company that two men had placed an order and partially paid for a 110-pound drum of phenyl-acetic acid, which is used to produce methamphetamines.[126] With the manager's consent, a DEA agent installed a beeper in the drum of chemicals.[127] After one of the defendants paid the balance on his order and picked up the drum, the agents used the beeper to follow the men to an amphetamine lab in Colorado where they were later arrested.[128] Before trial, the defendants moved to suppress the evidence obtained as a result of the warrantless installation and monitoring of the beeper, arguing that it violated their rights under both the Fourth Amendment to the U.S. Constitution and a related provision in the Colorado Constitution.[129] The district court granted the motion with respect to the installation, but concluded that based on *Knotts* the subsequent monitoring of the beeper was not a search under the federal or state constitution.[130] The Colorado Supreme Court affirmed the district court's ruling, holding that a defendant who pays for and takes possession of a drum containing a beeper possesses a "legitimate expectation of privacy in that drum, and that the warrantless installation and continued presence of the beeper constituted an illegal intrusion upon that expectation of privacy under article II, section 7 of the Colorado Constitution."[131] The court acknowledged that under *Karo*, the in-

---

[123] People v. Oates, 698 P.2d 811, 818 (Colo. 1985).
[124] *Id.* at 814–16.
[125] *Id.* at 812.
[126] *Id.* at 813, 816.
[127] *Id.* at 813.
[128] *Id.*
[129] *Id.* at 813–14.
[130] *Id.* at 813 n.4.
[131] *Id.* at 814.

stallation and presence of the beeper in this case was not a search within the meaning of the Fourth Amendment, but explained that in interpreting the Colorado Constitution it was not bound by the decisions of the U.S. Supreme Court that construe the federal Constitution.[132]

The court declined to follow the reasoning in *Karo* because it believed that the search and seizure provision in the Colorado Constitution encompasses "a broader definition of what constitutes" a reasonable expectation of privacy—namely that "purchased commercial goods will be free of government surveillance devices."[133] Echoing Justice Stevens's opinion in *Karo*, the Colorado Supreme Court explained that at the time the beeper was installed, not only had one of the defendants partially paid for the drum of chemicals, but when he took possession of the drum he did not have the exclusive power to use and dispose of the item as he saw fit.[134] When the DEA agents installed the beeper, they violated the purchaser's expectation of privacy, and this violation continued through the time he took possession of the product.[135] Furthermore, the consent of a seller or lessor of goods does not validate the invasion that occurs when the product is transferred to the purchaser or lessee.[136] Just as a previous owner of a suitcase cannot consent to the police periodically opening and searching the bag after it comes under the ownership of another, neither can one owner's agreement to have a beeper installed in an item suffice once that item belongs to someone else.[137] This type of violation is not merely a "technical trespass," but an actual one that "significantly impairs the privacy associated with privately-owned goods."[138] Despite its decisions in *Knotts* and *Karo*, the Supreme Court's holding in *Alderman v. United States* indicates that "[t]he crucial invasion of privacy occurs when entry is effected for the purpose of making a search; it is not necessary that the entry produce information in order to violate the sense of security protected by [the Fourth Amendment]."[139] The homeowner in *Alderman* was allowed to challenge the installation of a listening device in his residence despite the fact that he was not present during any conversation that was monitored by the police.[140] Justice Stevens made a similar argument in his *Karo* opinion that even the entry of a blindfolded intruder is an

---

[132] *Id.* at 815.

[133] *Id.* at 815–16.

[134] *Id.* at 816. *But see* United States v. Hufford, 539 F.2d 32 (9th Cir. 1976) (holding that partial payment for a drum of chemicals did not establish a defendant's reasonable expectation of privacy in it).

[135] *Id.* at 816–17.

[136] *Id.* at 817 n.6.

[137] *Id.*

[138] *Id.* at 817.

[139] *Id.* at 818; Alderman v. United States, 394 U.S. 165, 179–80 (1967).

[140] *Alderman*, 394 U.S. at 179–80.

invasion of privacy.[141]

Because the beeper served as a surrogate for actual police presence and converted the drum of chemicals into a covert broadcasting station, its capacity to impart information was enough to violate the Colorado Constitution—even before the monitoring began.[142] Therefore, the state supreme court held that "the legitimate privacy expectation of one with a proprietary or possessory interest in a commercially-purchased item is violated under . . . the Colorado Constitution whenever the item contains a government-installed beeper."[143] In addition, it noted that *Karo* was correct in stating that "one lacking any expectation of privacy in the drum itself"—i.e., someone who did not purchase or possess it—"may nonetheless suffer an invasion of privacy through law enforcement monitoring of the beeper if the beeper enters his residence or otherwise monitors information that he reasonably would expect to remain private."[144]

B. State v. Kelly

A few months after the Colorado Supreme Court decided *Oates*, the Hawaii Supreme Court considered *State v. Kelly*.[145] Patrick Kelly was convicted for cocaine possession based on evidence from a photo album located in his residence.[146] Kelly appealed the trial court's denial of his motion to suppress such evidence, arguing that the warrantless installation of a beeper in the back cover of the photo album violated his rights under both the Fourth Amendment and a similar provision in the Hawaii Constitution.[147] The installation of the beeper in *Kelly* is of particular relevance to the topic of NSA bugging discussed in this Article because the beeper was implanted when the government intercepted a package that was being shipped to the defendant. A drug dog at the Hawaii airport detected contraband in a box from Peru that was addressed to Kelly.[148] Customs officers opened the package and discovered a photo album with cocaine stored in the front and back covers.[149] They notified the DEA, and ten days later, federal agents replaced four of the packets in the album with fake cocaine.[150] The agents also installed a beeper in the back cover of the album "which would enable [them] to monitor the location of the package and to learn

---

[141] United States v. Karo, 468 U.S. at 705, 735 n.10 (1984) (Stevens, J., concurring in part and dissenting in part).

[142] *See* United States v. Butts, 710 F.2d 1139, 1149 (5th Cir. 1983).

[143] *Oates*, 698 P.2d at 818.

[144] *Karo*, 468 U.S. at 714–17; *Oates*, 698 P.2d at 819.

[145] State v. Kelly, 708 P.2d 820, 820–21 (Haw. 1985).

[146] *Id.* at 821.

[147] *Id.*

[148] *Id.*

[149] *Id.* at 822.

[150] *Id.*

when the back cover . . . was being opened."[151] That same day, the package was delivered to Kelly at the University of Hawaii School of Business.[152] Kelly then took the album to his residence, and officers followed him using the beeper's signals.[153] When "the signals from the beeper changed to a droning tone indicating that the back cover of the album had been opened," two officers knocked on the door and asked to speak to Kelly.[154] Kelly's roommate told the officers that Kelly was not home, but upon hearing the sounds of fast footsteps and the toilet flushing, the officers entered the house, observed Kelly in the bathroom holding the open album over the toilet, and arrested him.[155]

Reversing the trial court's denial of Kelly's motion to suppress, the Hawaii Supreme Court went further than the *Oates* court by deciding that the case involved a violation of *both* the state and U.S. Constitutions.[156] The court determined that the material facts of *Kelly* were distinguishable from the facts of *Knotts and Karo* and held that "the warrantless seizure of the album for ten days for the purpose of installing the beeper in the back cover . . . constituted an unreasonable seizure of property violating the Fourth Amendment of the [U.S.] Constitution," as well as article I, section 7 of the Hawaii Constitution.[157] The beepers in *Knotts* and *Karo* were installed in drums of chemicals while "government agents had full control, dominion, and possessory interest . . . before the defendants obtained possession of the drums through a purchase." Kelly, on the other hand, had a possessory interest in the photo album while it was in the mail and had a "reasonable expectation that [such] possessory interest . . . would not be tampered or interfered with by anyone."[158] As a result, the seizure of the album, the installation and monitoring of the beeper, and the subsequent search of Kelly's residence were unreasonable, and the cocaine and other incriminating evidence accordingly must be suppressed.[159] Because the NSA installs its spyware in computers both before they leave the factory and while they are being shipped to consumers, this reasoning in *Kelly* would be only moderately helpful to defendants bringing constitutional invasion of privacy claims against the agency. As discussed below, the better solution is to overturn *Knotts* and *Karo* as they relate to the trespass theory of the Fourth Amendment.

---

[151] *Id.*

[152] *Id.*

[153] *Id.*

[154] *Id.*

[155] *Id.*

[156] *Id.* at 823–24.

[157] *Id.* at 821.

[158] *Id.* at 823.

[159] *Id.* at 823–24.

C. *The Need for Uniformity in the Law*

The dissenting opinions in *Oates* argued that the Colorado Supreme Court should not have departed from *Knotts* and *Karo* in interpreting its state constitution because of the need for uniformity in the law.[160] That argument bears exploration in this Article, but for exactly the opposite reason: *Knotts* and *Karo* should be overturned so that courts like those in Colorado and Hawaii are not forced to resort to interpreting state constitutions and finding facts that distinguish a case from the Supreme Court precedent. One dissenting judge in *Oates* explained that the facts of the case—namely, that the investigation began in Texas and the defendants were arrested in Colorado—"demonstrate [that] the manufacturing and distribution of illegal narcotics presents a problem of federal dimension."[161] Like the NSA, the DEA is a federal agency that monitors activities taking place in all fifty states and numerous foreign countries.[162] Under the current system, "[a] beeper lawfully installed in one jurisdiction without a warrant may ultimately be traced to another jurisdiction where a warrant is required."[163] Federal agents cannot and should not be expected to know the constitutional requirements of every state or to predict whether the situation in a given case differs enough from that in *Knotts* or *Karo*; rather, there must be uniformity in the law.[164] The other dissenting judge in *Oates* pointed out the absurdity of different interpretations of state and federal constitutional provisions that contain almost identical language.[165] Especially with an area of the law like search and seizure, state and federal law should be parallel because "[i]t is important to our judicial system, and to society, that certainty exist in the ground rules . . . and in the application of the exclusionary rule."[166] However, unlike these judges, this Article maintains that the solution is not deference to the decisions of the Supreme Court, but rather eliminating the problematic precedent they set.

The Colorado and Hawaii high courts were not the only ones questioning *Knotts* and *Karo* in 1985. In a law review article published the same year entitled *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo, *and the Questions Still Unanswered*, Professor Clifford S. Fishman criticized "[t]he broad sweep of the Court's discussion of consensual installations and sales in *Karo*[, which] appears on its face to be applicable to all such installations and transfers, regardless of the sophistication of the beeper and regardless

---

[160] People v. Oates, 698 P.2d 811, 822, 825 (Colo. 1985) (Ericson, C.J., dissenting and Rovira, J., dissenting) (citing People v. Disbrow, 545 P.2d 272, 284 (1976)).

[161] *Id.* at 822 (Ericson, C.J., dissenting).

[162] *Id.* at 823.

[163] *Id.*

[164] *Id.* at 825; Disbrow, 545 P.2d. at 248.

[165] *Oates*, 698 P.2d at 822–25 (Rovira, J., dissenting).

[166] *Id.* at 825.

of where the beeper is being installed."[167] Although few such cases had been reported at the time, Fishman predicted that issues "far more delicate than those before the Court in *Karo*" could arise with the use of more sophisticated surveillance tools or by the installation of tracking devices "into objects significantly more 'private' than a container of chemicals."[168] The advanced spyware being used by the NSA to infiltrate the private contents of personal computers is just the sort of problem to which Professor Fishman was referring.

Indeed, after the revelation of the NSA's latest surveillance methods, federal law can no longer hold that it is neither a search nor a seizure for law enforcement or intelligence officials, acting with the consent of the manufacturer, to install an electronic monitoring device on a product that will be delivered to the target of an investigation. *Knotts* and *Karo* were bad decisions when they came down in the early 1980s, and the technological developments since that time have only reinforced their negative impact on Fourth Amendment jurisprudence and their need to be overturned. As discussed below, the NSA's installation of electronic devices that not only track the location of personal computers but also extract from them data that has been concealed from public view (i.e., that has not been voluntarily conveyed to others over the Internet) should be considered unconstitutional for three reasons. First, a computer is the purchaser's "effect" at the time of the installation, and therefore the manufacturer's consent to the bugging is invalid. Second, the devices the NSA employs do much more than monitor a computer's location and allow the government to make inferences about a suspect's activity—they extract the computer's private contents and directly provide evidence for an investigation. Finally, using technology to electronically intercept private information is equivalent to a physical trespass on property and should be treated the same way under the law.

V. WHY THE UNITED STATES SUPREME COURT SHOULD OVERTURN *KNOTTS* AND *KARO*

A. *A Manufacturer's Consent to the Installation of a Monitoring Device Is Invalid*

As Justices Sotomayor and Alito each pointed out in their concurring opinions in *United States v. Jones*, the trespass theory of the Fourth Amendment currently offers no protection when the government enlists the help of manufacturers to install a monitoring device in a product that is not yet in the suspect's possession.[169] In his treatise on the Fourth Amendment, Wayne R. LaFave discussed the problem with allowing sellers of goods to surrender the

---

[167] Clifford S. Fishman, *Electronic Tracking Devices and the Fourth Amendment:* Knotts, Karo, *and the Questions Still Unanswered*, 34 CATH. U.L. REV. 277, 308–09 (1985).

[168] *Id.* at 309.

[169] United States v. Jones, 132 S. Ct. 945, 955, 961 (2012) (Sotomayor, J., concurring and Alito, J., concurring).

privacy rights of buyers.[170] Just as the telephone company in *Katz v. United States* could not have sanctioned the installation of the recording device on the telephone booth, "[a]t least when there has been a lawful sale of goods, the fact [that] the seller consented to putting the beeper in the goods should not itself legitimate the later monitoring of the beeper."[171] Our society should not require a buyer—even one who intends to use a product for an unlawful objective—to assume the risk that the seller has arranged for the subsequent movements of the product to be monitored: "A citizen is entitled to assume the property he buys does not contain an electronic spy."[172] Many courts deciding cases with analogous facts seem to agree with this principle, but because of the precedent set by *Knotts*, *Karo*, and now *Jones*, they have had to strain to achieve what they consider the "right" result.

For example, in *People v. LeFlore* an Illinois appellate court considered the Fourth Amendment protections available not to the purchaser of a vehicle but to someone who borrowed it.[173] After being convicted of aggravated robbery, robbery, and burglary, LeFlore appealed his conviction, arguing that the trial court erred in denying his motion to suppress evidence obtained through the use of a GPS tracking device installed on a vehicle belonging to his roommate that he regularly drove.[174] The Illinois police officers did not have a warrant, and LeFlore contended that the installation and use of the GPS device constituted an unlawful search in violation of the Fourth Amendment.[175] The police decided to conduct electronic surveillance on the car because LeFlore's roommate informed them that LeFlore would sometimes drive her car and that she often gave him rides.[176] The facts in *LeFlore* differed from those in *Jones* insofar as the defendant was the exclusive driver of a car registered to his wife.[177] Thus, although the court in *LeFlore* felt it could not deem the car LeFlore's "effect," it decided that "[t]he essence of the *Jones* trespass test is whether the government physically occupies private property for the purpose of obtaining information."[178] LeFlore was not in possession of the vehicle when the GPS was installed, but he later came into lawful possession by borrowing the car with his

---

[170] 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 2.7(f) (5th ed. 2013).

[171] *Id.* at 1003.

[172] *Id.* (quoting United States v. Bobisink, 415 F. Supp. 1334 (D. Mass. 1976)).

[173] People v. LeFlore, 996 N.E.2d 678, 683 (Ill. App. Ct. 2013).

[174] *Id.* at 681.

[175] *Id.*

[176] *Id.* at 681–82.

[177] United States v. Jones, 132 S. Ct. 945, 949 n.2 (2012) ("If Jones was not the owner [of the car] he had at least the property rights of a bailee. The Court of Appeals concluded that the vehicle's registration did not affect [Jones's] ability to make a Fourth Amendment objection, and the Government has not challenged that determination here. We therefore do not consider the Fourth Amendment significance of Jones's status.").

[178] *LeFlore*, 996 N.E.2d at 687.

roommate's consent—and at that point the government's trespassory act began.[179] The police's GPS tracking of the vehicle constituted a continuing trespass, and therefore LeFlore had standing to challenge the use of the tracking device.[180]

Just as the *LeFlore* court struggled to define the property rights of the borrower of a vehicle, the U.S. Court of Appeals for the Fourth Circuit recently wrestled with whether the purchaser of a vehicle could object to its search during the delivery process.[181] In *United States v. Castellanos*, a commercial car carrier was transporting a vehicle to North Carolina.[182] According to shipping documents, the owner of the vehicle was a man named Wilmer Castenada.[183] Texas police spotted the vehicle while it was in transit and became suspicious because there was a dealership placard instead of a regular license plate.[184] Upon investigation, officers were unable to find anyone named Wilmer Castenada in North Carolina and accordingly asked the driver of the commercial car carrier for permission to search the vehicle.[185] The driver agreed, and the search uncovered approximately $3 million of cocaine stored in the vehicle's gas tank.[186] When a man claiming to be Wilmer Casteneda called the carrier service to inquire about the delayed delivery of the car, a police officer posing as a wrecking service employee told him that the driver had been arrested and his cargo impounded; as a result, Castenada would need to claim the vehicle in Texas.[187] A man named Arturo Castellanos arrived to claim the car, and the police detained him.[188] At this time, Castellanos held the title to the car and the tracking number from the carrier service.[189] He informed the police that he was in the process of purchasing the vehicle from Castenada and was planning to pick up the car in North Carolina and then drive it back to his home in California.[190] Castellanos was indicted in North Carolina for conspiracy to distribute cocaine.[191] Prior to trial, he moved to suppress the cocaine

---

[179] *Id.* at 686–87.

[180] *Id.* at 678. *But compare* United States v. Barraza-Maldonado, 879 F. Supp. 2d 1022, 1027–28 (D. Minn. 2012) ("[W]hen a defendant takes possession of a piece of property on which a GPS device has already been installed, the continued monitoring of that device is . . . not a trespass on the property of the defendant, and therefore is not a search of the defendant for the purposes of the trespassory test.").

[181] United States v. Castellanos, 716 F.3d 828 (4th Cir. 2013).

[182] *Id.* at 830.

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] *Id.* at 830–31.

[189] *Id.* at 831.

[190] *Id.*

[191] *Id.*

found in the vehicle's gas tank, but "[n]otably . . . did not introduce any evidence"—including the title document he brought to Texas—"to show that he owned the [vehicle] at the time [the police] conducted the warrantless search or [even that he] had permission to use [or possess] the vehicle."[192] The district court therefore denied the motion, and Castellanos appealed.[193]

The Fourth Circuit affirmed, but its opinion offers several points that are relevant to the discussion in this Article.[194] The court explained that

[w]hen attempting to determine whether a defendant has a reasonable expectation of privacy in property [at a time when it] is held by another, we consider such factors as whether that person claims an ownership or possessory interest in the property, and whether he has established a right or taken precautions to exclude others from the property.[195]

While the court determined that Castellanos's assertion that he was purchasing the car was unsubstantiated, it indicated that a defendant who had evidence of the title to the car, a bill of sale, or even his Division of Motor Vehicles registration could have brought a successful Fourth Amendment challenge.[196] The dissenting judge believed, however, that the undisputed facts of the case sufficiently established that Castellanos "had a right to possession, coupled with constructive dominion and control over the vehicle at the time [the police] searched it, such that, as a matter of law, he enjoyed an objectively reasonable expectation of privacy in the vehicle."[197] Specifically, the dissenting opinion noted that at one point, Castellanos had the title and shipment tracking information for the vehicle, had called the common carrier several times to check on the status of the transport, and had visited the towing company that he was told was expecting the vehicle's delivery.[198] Therefore, the dissenting judge would have vacated the judgment and reversed the district court's ruling.[199]

Finally, it is important to consider an individual's rights in property that has neither been transferred to him as in *LeFlore* or to a common carrier as in *Castellanos*. Like the police officers and DEA agents in *Knotts* and *Karo*, NSA operatives install spyware in computers while they are still held by the manufacturers.[200] To successfully invoke the *Jones* majority's trespassory test and claim the Fourth Amendment's protections, a defendant must be able to establish that he had some type of property interest in the product at the time of

---

[192] *Id.*

[193] *Id.* at 831–32.

[194] *Id.* at 833.

[195] *Id.* at 833–34 (internal quotation marks omitted).

[196] *Id.* at 834.

[197] *Id.* at 848, 850 (Davis, J., dissenting).

[198] *Id.* at 848.

[199] *Id.* at 851.

[200] Sanger & Shanker, *supra* note 1.

the installation.[201] An analogy to the Racketeer Influenced and Corrupt Organizations ("RICO") Act is helpful for demonstrating why purchasers do indeed have property rights in the products they have ordered. Section 1963(c) of the Act provides that "[a]ll right, title, and interest in property [constituting or derived from any proceeds obtained from racketeering activity] vests in the United States upon the commission of the act giving rise to the forfeiture."[202] This statute sets out the relation back doctrine, and it gives the government an equitable interest in property as soon as a defendant commits a RICO violation, even though legal title does not transfer until there is a conviction or guilty plea.[203] This property interest "prevent[s] defendants from escaping the impact of forfeiture by giving their assets to third parties."[204] Likewise, a purchaser has at least an equitable interest in a product that he has ordered and paid for. As a result, he should be able to challenge the warrantless search or seizure of this property by government officials.

B. *New Electronic Monitoring Technologies Pose Greater Threats to Privacy Than Locational Tracking Devices*

In his 1985 law review article, Professor Fishman perceptively asked what would happen if, for example, the DEA agents in *Karo* had installed "not merely a locational [tracking device], but an eavesdropping device."[205] The answer: "As the *Karo* opinion is written, the same result would be reached—[t]he pre-transfer installation of the device would not be a 'search' . . . ."[206] The technological developments of the past thirty years have only made that statement more problematic. In her concurrence in *Jones*, Justice Sotomayor described the

unique attributes of GPS surveillance . . . [that] require particular attention[:] GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations . . . . [that] [t]he Government can store . . . and efficiently mine . . . for information years into the future.[207]

---

[201] *See, e.g.*, United States v. Barraza-Maldonado, 879 F. Supp. 2d 1022, 1028 (D. Minn. 2012).

[202] 18 U.S.C. § 1963(c).

[203] Heather J. Garretson, *Federal Criminal Forfeiture: A Royal Pain in the Assets*, 18 REV. L. & SOC. JUST. 45, 63 (2008).

[204] *Id.*

[205] Fishman, *supra* note 167, at 309 n.123.

[206] Fishman, *supra* note 167, at 309 n.123.

[207] United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring) (citing People v. Weaver, 909 N.E.2d 1195, 1199 (2009) ("Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.").

Indeed, Jones's movements were tracked 24 hours a day for 28 days, and the GPS relayed over 2,000 pages of data to government computers during that time period—far more intrusive monitoring than what took place in *Knotts* and *Karo*.[208] Likewise, the *LeFlore* court noted that a GPS transmits contemporaneous signals to a satellite and then to a server as frequently as every 15 seconds, thereby allowing the device's location to be read on a computer.[209] In that case, the police also set up a "geofence" for the area surrounding the defendant's apartment so that anytime the GPS tracker left the area, the police would receive notice on a cell phone.[210] The GPS allowed officers to conduct "continuous surveillance and transmission that [they] could *instantaneously* access, without having to retrieve the GPS device," and the geofence provided "access information on the [target] vehicle's *contemporaneous* movements."[211]

While beepers and their twenty-first century counterpart, the GPS, allow government officers to discover the totality and pattern of a suspect's movements from place to place and to "reconstruct 'a virtual mosaic of [t]he person's life,'" NSA spyware provides this information directly.[212] Tools such as the USB cards and circuit boards revealed by Snowden are also far more dangerous than the surveillance methods employed in *Knotts* and *Jones* because they extract private data from computers that are not connected to the Internet. Because the information was not "voluntarily" conveyed to the public, the third-party doctrine is not implicated. Thus, the user should be allowed to retain his reasonable expectation of privacy in the content of his personal computer.

C. *The Trespass Theory of the Fourth Amendment Has Been Liberally Construed*

Having explained why the purchaser has a property interest in a computer that he has ordered and in the privacy of the information the NSA can directly obtain using its spyware, this final section clarifies why *Knotts* and *Karo* were not justified in distinguishing the beeper installation from a physical trespass. In *Kyllo v. United States*, a government agent performed a thermal image scan of Danny Kyllo's home from a vehicle parked on the public street outside.[213] The agent concluded from the scan that Kyllo was using high-intensity lamps to grow marijuana in his house, and with this evidence he obtained a search warrant for the home.[214] The Court in *Silverman v. United States* opined that "[a]t

---

[208] *Id.* at 948, 952 (Scalia, J.)

[209] People v. LeFlore, 996 N.E.2d 678, 681 (Ill. App. Ct. 2013).

[210] *Id.* at 692.

[211] *Id.* at 692.

[212] People v. Oates, 698 P.2d 811, 817 (Colo. 1985) (quoting People v. Sporleder, 666 P.2d 135, 142 (Colo. 1983)).

[213] Kyllo v. United States, 533 U.S. 27, 29 (2001).

[214] *Id.* at 30.

the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[215] However, under the *Katz* test, Kyllo arguably had no reasonable expectation of privacy in the temperature of the exterior walls of his house because of the third-party doctrine: "A nontrespassory measurement of some physical condition of the exterior wall could rationally be [ ] characterized as a fact knowingly exposed to the public."[216]

Therefore, Kyllo could only claim the protections of the Fourth Amendment if the government somehow committed a "trespass" when it electronically entered his home.[217] The Supreme Court held that although the government did not physically intrude into a constitutionally protected area, it exercised an unreasonable search because it used sense-enhancing technology that was "not in general public use" to obtain information about the interior of Kyllo's home that could not have been previously known without a trespass.[218] Justice Stevens dissented because he believed the test should be whether a given technology offers the government the "functional equivalent of actual presence in the area being searched," and that the holding in *Kyllo* should not be limited to the home. Justice Stevens reasoned that if surveillance equipment "provide[s] its user with the functional equivalent of access to a private place—such as, for example, the telephone booth involved in *Katz*, or an office building—the then rule should apply to such an area as well as to a home."[219]

Presumably, the USB cards and circuit boards that the NSA installs in its targets' computers are "not in general public use" because the catalog containing these surveillance tools was only released to the public in the wake of the Snowden scandal. In addition, the devices are expensive—packs of 50 units cost over $1 million.[220] Accordingly, *Kyllo* seems to apply to this type of government activity, and personal computers not connected to the Internet are arguably a "private place" equivalent to the home.

Finally, it is worth noting that the legal theory advocated in this Article is not new. In fact, it stems from one of the lesser known dissenting opinions in

---

[215] Silverman v. United States, 365 U.S. 505, 511 (1961).

[216] Cloud, *supra* note 21, at 42.

[217] *See* Cloud, *supra* note 21, at 46–48.

[218] *Kyllo*, 533 U.S. at 27 (holding that the Fourth Amendment does not regulate government use of technologies "generally available to the public").

[219] *Id.* at 47, 49 (Stevens, J., dissenting) (citing Katz v. United States, 389 U.S. 347, 351 (1967) ("The Fourth Amendment protects people, not places.")).

[220] Sara Morrison, *Yes, the NSA Can Get You Offline, Too—With Radio Waves*, WIRE (Jan. 14, 2014, 11:23 PM), http://www.thewire.com/national/2014/01/yes-nsa-can-get-you-offline-too-radio-waves/357022/ (citing Jacob Appelaum, *Shopping for Spy Gear: Catalog Advertises NSA Toolbox*, SPIEGEL ONLINE INTERNATIONAL (Dec. 29, 2013), http://www.spiegel.de/international/world/catalog-reveals-nsa-has-back-doors-for-numerous-devices-a-940994.html.

Olmstead v. United States—that of Justice Butler.[221] As the Court in *Kyllo* would conclude nearly 75 years later, Justice Butler argued that using technology to intercept a private conversation is equivalent to a physical trespass on private property and should be treated as such by the law.[222] Under Justice Butler's liberal property-based analysis of the Fourth Amendment,[223] the government in *Olmstead* committed a trespass when it placed wiretaps outside the defendants' homes and recorded their private telephone conversations.[224] The communications themselves "belong[ed] to the parties between whom they pass[ed]" and thus constituted effects.[225] Just like a consumer's purchase of a product from a manufacturer, "[t]he contracts between telephone companies and users contemplate the private use of the facilities employed in the service"—wiretapping and recording the defendants' conversations interfered with their exclusive use of the telephone wire.[226]

Justice Butler explained that an 1886 case, *Boyd v. United States*,[227] gave the *Olmstead* Court license to honor the principles upon which the Constitution was founded instead of strictly interpreting the text of the Fourth Amendment.[228] In *Boyd*, there was no search or seizure within the literal meaning of the Fourth Amendment; rather, the Court liberally construed the Constitution in order to safeguard the defendants' personal rights.[229] *Boyd* established that while "the government was entitled to search for and seize [ ] those things in which it had a legally identifiable [property] interest"—such as contraband, "imported goods on which duties had not been paid," and stolen property—its officers could assert no such claim over items like the Boyds' private business records.[230] This property rights theory was a fundamental part of Fourth Amendment doctrine for nearly a century until the Court abandoned it in *Katz* to overturn the flawed *Olmstead* decision.[231] As this Article has described, the property-based approach to the Fourth Amendment was revived in *Jones* and should be applied in the context of the NSA's ongoing surveillance program and related government activity.

---

221 Olmstead v. United States, 277 U.S. 438, 485 (1928) (Butler, J., dissenting).

222 *Id.* at 487.

223 Cloud, *supra* note 21, at 18–19 (explaining that Justice Butler's dissent could have served as the basis for "an expansive interpretive theory" of property rights that could then be utilized to "implement a broad notion of individual liberty").

224 *Olmstead*, 277 U.S. at 487.

225 *Id.*

226 *Id.*

227 Boyd v. United States, 116 U.S. 616 (1886).

228 *Olmstead*, 277 U.S. at 487–88.

229 Cloud, *supra* note 21, at 11.

230 *Id.*

231 *Id.* at 15.

VI. CONCLUSION

As one commentator has noted, "[i]t's common to check up on tracking information when you're waiting on a package, but at least occasionally, that tracking data is omitting a quick stop off at the NSA."[232] This type of monitoring by the federal government poses a serious threat to the privacy of American citizens and should be prohibited under the Fourth Amendment unless a proper warrant is obtained. This Article suggests possible ways that criminal defendants could bring a constitutional challenge. But first, the Supreme Court should seriously consider whether *Knotts* and *Karo* are still good law now that "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision"—the once feared "dragnet-type law enforcement practices"[233]—is not only possible, but regularly taking place.

---

[232] Ryan Whitwam, *The NSA Regularly Intercepts Laptop Shipments to Implant Malware, Report Says*, EXTREME TECH (Dec. 30, 2013, 4:14 PM), http://www.extremetech.com/computing/173721-the-nsa-regularly-intercepts-laptop-shipments-to-implant-malware-report-says.

[233] United States v. Knotts, 460 U.S. 276, 283–84 (1983).