ISSUE 16.2 FALL 2011

Where We Are with Location Tracking: A Look at the Current Technology and the Implications on Fourth Amendment Jurisprudence

Ian Herbert*

INTRODUCTION

In August 2010, the D.C. Circuit, in *United States v. Maynard*, became the first federal circuit court to decide that the use of a tracking device¹ by law enforcement to track the location of a suspect was a search protected by the Fourth Amendment, clearing the way for the Supreme

^{*} J.D. Candidate, New York University, 2012. The author would like to thank Professor Erin Murphy for her comments, guidance, and unending support, and Professors Barry Friedman, Claudia Angelos and Corey Stoughton for their mentorship throughout this process. Additional thanks to the staff of the Berkeley Journal of Criminal law, particularly Jeff Gonzalez, Jessica Ly and Jake Rasch-Chabot, for their extraordinarily helpful remarks, and to Wray Herbert, Nancy Alfano and Krista Vogt for their encouragement.

¹ It is important to clarify the terminology right from the start. The term "tracking device" or "location-tracking device" refers to the broad category of devices used to track a person's location. This broad category includes radio frequency (RF)-enabled tracking devices (commonly referred to as "beepers"), satellite-based tracking devices and cell-site tracking devices. Satellite-based tracking devices are commonly referred to as Global Positioning System (GPS) devices. Technically, the term GPS refers to a specific system of satellites, the NAVSTAR GPS system created by the United States. *See infra* notes 147-84 and accompanying text for a more in-depth explanation of the NAVSTAR GPS system. Because until very recently the GPS satellite system was the only useable system in the world, almost all satellite-based tracking devices were GPS devices. However, that is beginning to change, so in this paper, the term GPS is used only to refer to devices that exclusively use the NAVSTAR GPS satellite system. The only exception to this rule is when this paper quotes courts, who sometimes use the term GPS generally to describe satellite-based tracking devices or, even more broadly, all tracking devices.

443

2011 WHERE WE ARE WITH LOCATION TRACKING

Court to decide the issue this term.² In *Maynard*, the FBI suspected the two defendants, Jones and Maynard, of distributing narcotics. Without a valid warrant, the FBI installed a tracking device on Jones's Jeep and monitored the location of the device for four weeks.³ The D.C. Circuit, relying on a "mosaic" theory, reversed Jones's conviction because it was obtained with evidence procured in violation of the Fourth Amendment.⁴ The court's "mosaic" theory holds that "[p]rolonged surveillance reveals types of information not revealed by short-term surveillance" and may violate an individual's Fourth Amendment rights, even if the same police conduct performed for a shorter period of time would not.⁵ In granting

_

² United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259). Because Maynard did not have standing to challenge the use of the tracking device on Jones's car and because that was the only issue appealed to the Supreme Court, the case in front of the Supreme Court bears only Jones's name, even though it was known as Maynard for the trial and in the D.C. Circuit. Throughout this paper, I reference Maynard when referring to the D.C. Circuit decision and Jones when referring to the case in front of the Supreme Court.

³ *Id.* at 555. The FBI actually received a court-issued order to place a tracking device on Jones's car. However, the government conceded technical violations of the order and confined its argument to the legality of the use of the device without a court order. *Id.* at 566, n.*.

⁴ *Id.* at 562.

⁵ Id. In Maynard, the investigators placed a tracking device on Jones's car and tracked his movements for 28 days. Id. at 558. The D.C. Circuit's "mosaic" theory rests on an argument that the government often makes in the national security context. In CIA v. Sims, 471 U.S. 159 (1985), for example, the CIA withheld information from a Freedom of Information Act request by relying on \$102(d)(3) of the National Security Act of 1947, which requires the Director of Central Intelligence to protect intelligence sources. Sims, 471 U.S. at 161. Even though the information requested (the grant proposals and contracts awarded under a project with the code-name MKULTRA and the names of the institutions and individuals that had performed research for that project) did not appear to fall directly under the National Security Act, the court agreed with the government that the Director could "withhold superficially innocuous information on the ground that it might enable an observer to discover the identity of an intelligence source." Id. at 178. In Maynard, the D.C. Circuit used the Supreme Court's language in Sims that "[what] may seem trivial to the uninformed, may appear of great moment to one who has a broad view of the scene and may put the questioned item of information in its proper context" to support its conclusion that an investigator who gets a broad view of a suspect's life may learn private details that are not actually exposed to the public. Maynard, 615 F.3d at 562 ("Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

the government's writ of certiorari, the Supreme Court directed the parties to address two distinct issues: whether the use of a tracking device violates the Fourth Amendment; and whether the respondent's Fourth Amendment rights were violated by the installation of the tracking device.⁶

In addition to being the first federal appellate court to proscribe the warrantless use of tracking devices, the D.C. Circuit was also the first to use the "mosaic" theory to challenge the long-established contention that a person's movements on public streets are exposed to the public.⁷ Yet the D.C. Circuit was not a legal pioneer. A number of state courts had already decided that location tracking is a violation of their state constitution, if not the federal constitution.8 Just six years after United States v. Knotts,9 the Supreme Court's seminal case on the constitutionality of the use of tracking devices by law enforcement, the Oregon Supreme Court expressly rejected the reasonable expectation of privacy test, stating, "The phrase becomes a formula for expressing a conclusion rather than a starting point for analysis, masking the various substantive considerations that are the real bases on which Fourth Amendment searches are defined."10 The court explained, "What the provisions forbid are unreasonable searches and seizures, i.e., certain acts of the government."11

places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story. A person who knows all of another's travels can deduce whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups—and not just one such fact about a person, but all such facts." (footnote omitted)).

⁶ Brief for the United States at 1, United States v. Jones, No. 10-1259 (U.S. Aug. 11, 2011).

_

⁷ Writing for the majority of the D.C. Circuit panel, Judge Ginsburg wrote, "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil." *Maynard*, 615 F.3d at 560.

⁸ See, e.g., State v. Campbell, 759 P.2d 1040 (Or. 1988); State v. Jackson, 76 P.3d 217 (Wash. 2003); People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009).

⁹ 460 U.S. 276 (1983) (upholding the use by law enforcement of a "beeper" to track a suspect for more than 100 miles over the course of a couple hours).

¹⁰ Campbell, 759 P.2d at 1044.

¹¹ *Id.* at 1045 (quotations omitted).

2011 Where We Are with Location Tracking

445

Additionally, in the three decades since Knotts was decided, a half-dozen legislatures have prohibited the use of electronic tracking devices without prior judicial approval.¹² In California, for example, the legislature made it a misdemeanor to "use an electronic tracking device to determine the location or movement of a person."13 The legislature made an exception for "the lawful use of an electronic tracking device by a law enforcement agency," but it does not define the term lawful use.¹⁴ It did, however, "declare[] that the right to privacy is fundamental in a free and civilized society and that the increasing use of electronic surveillance devices is eroding personal liberty. The Legislature declares that

¹² See, e.g., UTAH CODE ANN. § 77-23a-15.5 (LexisNexis 2011) ("An investigative or law enforcement officer may make application to a district judge for an order authorizing or approving the installation and use of a mobile tracking device."); MINN. STAT. § 626A.35 (2010) ("Except as provided in this section, no person may install or use a pen register, trap and trace device, or mobile tracking device without first obtaining a court order under section 626A.37."); FLA. STAT. \$ 934.42 (2011) ("An investigative or law enforcement officer may make application to a judge of competent jurisdiction for an order authorizing or approving the installation and use of a mobile tracking device."); S.C. CODE ANN. § 17-30-140 (2010) ("The Attorney General or any solicitor may make application to a judge of competent jurisdiction for an order authorizing or approving the installation and use of a mobile tracking device by the South Carolina Law Enforcement Division or any law enforcement entity of a political subdivision of this State."); OKLA. STAT. tit. 13, § 177.6 (2011) ("Any magistrate may issue a search warrant authorizing the installation or use of a tracking device in any moveable item, container, vehicle or other vessel. Such warrant may authorize the use of that tracking device within the jurisdiction of the magistrate, and outside that jurisdiction if the tracking device is installed within the magistrate's jurisdiction. No such warrant shall issue unless probable cause is shown for believing that such installation or use will lead to the discovery of evidence, fruits, or instrumentalities of the commission or attempted commission of an offense."); HAW. REV. STAT. §§ 803-42, 803-44.7 (2010) (Any person who "[i]ntentionally installs or uses a mobile tracking device without first obtaining a search warrant or other order authorizing the installation and use of such device, unless the device is installed by or with consent of the owner of the property on which the device is installed" shall be guilty of a class C felony.); 18 PA. CONS. STAT. § 5761 (2011) ("An order authorizing the use of one or more mobile tracking devices may be issued to an investigative or law enforcement officer by the court of common pleas upon written application. Each application shall be by written affidavit, signed and sworn to or affirmed before the court of common pleas.").

¹³ Cal. Penal Code § 637.7(a) (West 2011).

¹⁴ CAL. PENAL CODE § 637.7(c) (West 2011).

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

electronic tracking of a person's location without that person's knowledge violates that person's reasonable expectation of privacy."¹⁵

In legal academia, professors and students have seen the Supreme Court's thirty-year absence from the field as an opportunity to critique the doctrine and suggest changes. Professor Renee McDonald Hutchins has criticized what she views as the Court's decision to "tie[] the scope of Fourth Amendment protection to the categorization of a technology as either sense augmenting or extrasensory." Numerous student notes have discussed the distinction between the "beepers" used in the *Knotts* investigation and the satellite-based tracking devices used in more recent cases. And scores of journal articles have addressed the subject since the turn of the century.

The use of tracking devices by law enforcement was recently described by the Seventh Circuit as "a Fourth Amendment frontier." Since then, the Supreme Court has granted certiorari in a location tracking case, 20 and Sen. Ron Wyden and Rep. Jason Chaffetz have introduced federal legislation that would create guidelines for how law enforcement and private citizens can legally use tracking devices. 21

 $^{^{15}}$ State v. Holden, No. IN 10-03-0545 to 0548, 2010 Del. Super. LEXIS 493 at *21 & n.40 (Del. Super. Ct. Dec. 14, 2010) (quoting 1998 Cal. Legis. Serv. ch. 449 (S.B. 1667) \S 1).

¹⁶ Renee McDonald Hutchins, *Tied up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 432 (2007) ("The Court's asymmetrical approach to intrusiveness is, however, neither necessary nor desirable.").

¹⁷ See, e.g., Ramya Shah, Note, From Beepers to GPS: Can the Fourth Amendment Keep Up with Electronic Tracking Technology?, 2009 U. ILL. J.L. TECH. & POL'Y 281 (2009); April A. Otterberg, Note, GPS Tracking Technology: The Case for Revisiting Knotts and Shifting the Supreme Court's Theory of the Public Space Under the Fourth Amendment, 46 B.C. L. REV. 661 (2005); Eva M. Dowdell, Note, You Are Here! Mapping the Boundaries of the Fourth Amendment with GPS Technology, 32 RUTGERS COMPUTER & TECH. L.J. 109 (2005). But see John S. Ganz, Comment, It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices, 95 J. CRIM. L. & CRIMINOLOGY 1325 (2005).

¹⁸ As a very crude method to obtain a sense of how often this topic has been addressed by legal academics, consider this: A search on Westlaw reveals 180 journal articles since the turn of the century that have cited *Knotts* for the propositions that a person has no reasonable expectation of privacy on public streets or that monitoring a beeper did not invade any reasonable expectation of privacy of the owner.

¹⁹ United States v. Cuevas-Perez, 640 F.3d 272, 275 (7th Cir. 2011).

²⁰ United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

²¹ Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (2011).

447

2011 WHERE WE ARE WITH LOCATION TRACKING

Yet, despite this large body of literature and the recognition that the use of tracking technology by law enforcement officers is a legal frontier, no one has attempted to analyze the specific details of current tracking devices—how they work, what they can do, and what their limitations are.²² This paper seeks to change the way courts conceptualize the Fourth Amendment issues related to location tracking. Through interviews with law enforcement officials and manufacturers of tracking devices and an inspection of government contracts and court documents, this paper seeks to provide not only a history of the advancements in tracking technology, but also a guide to the electronic surveillance devices law enforcement officers have used in investigations since *Knotts* was decided thirty years ago. Using this information, this paper proposes that, regardless of the outcome in *Knotts*, courts should move from the one-

Nevertheless, this paper is not truly comprehensive for two related reasons. First, manufacturers of tracking devices and the government agencies that use them are unsurprisingly close-lipped about the products that they make and use. To protect the integrity of their surveillance methods, government agencies have denied freedom of information requests by citing law enforcement exceptions.²³ Second, manufacturers often limit information about their products to members

size-fits-all approach that they have traditionally relied on to a more rigorous analysis based on the level of police involvement, the means of

installation, and the accuracy of the specific device at issue.

_

²² For an example of the lack of depth of judicial analysis of current tracking devices, *see* United States v. Pineda-Moreno, 591 F.3d 1212, 1217 (9th Cir. 2010) ("Over a fourmonth period, agents repeatedly monitored Pineda-Moreno's Jeep using various types of mobile tracking devices. Each device was about the size of a bar of soap and had a magnet affixed to its side, allowing it to be attached to the underside of a car."). The best analysis of current tracking technology is found in a concurring opinion from a Seventh Circuit case that was published earlier this year. *See Cuevas-Perez*, 640 F.3d at 277 (Flaum, J., concurring) ("A beeper transmits a signal that a receiver can detect. With GPS technology, the unit itself is a receiver: using a process called trilateration, the unit pieces together the geographical coordinates of its location based on its position relative to several orbiting satellites. When affixed to a vehicle, the GPS unit can either record the vehicle's movements for later downloading or transmit the information at intervals. To be sure, GPS units are far more accurate than beepers." (citation omitted)).

²³ See, e.g., infra notes 89-93 and accompanying text.

[Vol. 16:2

448

of the law enforcement community by placing the majority of their online product descriptions behind password-protected firewalls.²⁴

This lack of information is exacerbated by the approach courts have taken regarding the use of tracking devices by law enforcement. Instead of asking detailed questions about the devices that are used and the constitutionality of different technologies, courts have taken a one-size-fits-all approach to the use of tracking devices. Most courts are content to call the devices "GPS trackers" without any additional analysis of the capabilities of the particular device. Meanwhile, litigators and legislators have also been content with this level of analysis or have been unable to force the issue. 26

Courts use the term "GPS tracker" to mean any one of a number of different kinds of devices, all with varying capabilities, when in fact "GPS" has a precise meaning regarding the use of a specific satellite system, the Global Positioning System, to track the location of a device.²⁷ As this paper makes clear, some location-tracking devices reveal the target's location every second of every day, while others only provide information when asked; some devices require the investigator to approach the car to retrieve the information, while others allow the officer to retrieve the information from miles away; some devices are incredibly accurate, while others provide only general tracking information such as the direction and approximate distance of the target; some are able to alert the police when a target is moving or is outside of a certain area, while others require the police to retrieve the device from the car in order to download the information; some are powered by batteries, while others are connected to the suspect's car and draw power from its power source.²⁸

All of these factors could be relevant to the Fourth Amendment analysis. For example, devices that investigators attach to car batteries may result in an unlawful seizure of the car's battery power or violate a

²⁴ See, e.g., infra note 97 and accompanying text.

²⁵ See supra note 22 and accompanying text; infra notes 45, 50-54 and accompanying text.

²⁶ Id.

²⁷ See infra notes 147-84 for a more in-depth explanation of the NAVSTAR GPS system.

²⁸ See generally infra notes 266-301 and accompanying text.

449

2011 Where We Are with Location Tracking

protected interest in the car,²⁹ and devices that allow the investigator to access location information from anywhere in the world may reveal information that is not actually exposed to the public in the same way as devices that require additional police action.³⁰ Also, increasingly more accurate devices may violate the sanctity of the home.³¹

In Knotts, the defendant expressed concern that a rule placing tracking devices outside the protection of the Fourth Amendment would mean that "twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision."32 The Court dismissed this concern, saying it could always reconsider the issue if "such dragnet type law enforcement practices . . . should eventually occur."33 Two different schools of thought have emerged on the meaning of the Court's use of the phrase "dragnet type law enforcement." Many courts have assumed that the Court was concerned about widespread use of tracking technology catching a large number of (potentially innocent) people in a police dragnet.³⁴ However, in *Maynard*, the D.C. Circuit stated that the Supreme Court used the phrase in response to the defendant's concern that, if the Fourth Amendment did not prohibit such conduct, twenty-four hour surveillance of any single citizen would be possible.³⁵ If the D.C. Circuit's interpretation is correct, a large

²⁹ See infra notes 318-42 and accompanying text.

³⁰ See infra notes 266-301 and accompanying text. ³¹ See infra notes 302-17 and accompanying text.

³² Brief of Respondent at 9, United States v. Knotts, 460 U.S. 276 (1983) (No. 81-

³³ Knotts, 460 U.S. at 284.

³⁴ See, e.g., United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007) (discussing the different concerns with a "program of mass surveillance" such as affixing GPS tracking devices to thousands of cars at random); United States v. Marquez, 605 F.3d 604, 610 (8th Cir. 2010) (describing "wholesale surveillance" as a different, more difficult issue); United States v. Pineda-Moreno, 591 F.3d 1212, 1216 n.2 ("We, like the Seventh Circuit, believe that '[s]hould [the] government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search." (alterations in original) (quoting Garcia, 474 F.3d at 988)).

³⁵ United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010) ("Although the Government, focusing upon the term 'dragnet,' suggests *Knotts* reserved the Fourth Amendment question that would be raised by mass surveillance, not the question raised by prolonged surveillance of a single individual, that is not what happened."), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-

[Vol. 16:2

number of devices regularly used today have crossed the threshold into "dragnet-type law enforcement practices."³⁶

This paper provides a catalog of the location-tracking technology currently in use and analyzes these technologies based on their specific capabilities. Part I details the problem with the one-size-fits-all approach taken by most courts. Part II describes the history of location-tracking devices, from beepers to satellite-based trackers to cell-site devices, and explains how the devices work. Part III discusses the devices used by law enforcement today. Finally, Part IV demonstrates what a technology-specific approach would look like.

I. THE PROBLEM WITH A ONE-SIZE-FITS-ALL APPROACH TO TRACKING TECHNOLOGY

A. Courts Have Generally Been Content with Citing Knotts for the Proposition that Location Tracking Is Valid Under the Fourth Amendment

Any discussion of tracking devices must begin with the Supreme Court's decision in *United States v. Knotts*. In *Knotts*, Minnesota investigators attached an electronic "beeper" to a barrel of chloroform that they suspected would be used to manufacture narcotics.³⁷ The beeper "emitt[ed] periodic signals that [could] be picked up by a radio receiver."³⁸ By using the signal, the investigators were able to follow the defendants from a safe distance. They tracked the defendants from a chemical company in Minneapolis to a cabin near Shell Lake, Wisconsin.³⁹ After monitoring the house for three days, the investigators

1259). See also United States v. Cuevas-Perez, 640 F.3d 272, 279 (7th Cir. 2011) (Flaum, J., concurring) ("Precisely what the Court was reserving in *Knotts* is hardly clear. Ambiguity arises because the phrase 'twenty-four surveillance' is commonly used as shorthand for around-the-clock surveillance over a prolonged time period. Yet, Knotts's concern seems to have been that any person, perhaps every person, could be monitored by the government. That concern seems better characterized as mass surveillance and the concern was acknowledged by the Court's use of the word 'dragnet.' Thus, it appears that the Court recognized both concerns, but whether one or both must be present to trigger the reservation in *Knotts* is not self-evident.").

v

³⁶ See infra note 72 and accompanying text.

³⁷ Knotts, 460 U.S. 276.

³⁸ *Id.* at 277.

³⁹ Id. at 278.

451

2011 WHERE WE ARE WITH LOCATION TRACKING

secured a search warrant, which led to the discovery of a large drug lab and enough chemicals to produce fourteen pounds of pure amphetamine.⁴⁰ The defendants challenged the use of the beeper as a violation of their Fourth Amendment rights, but the Supreme Court disagreed, holding that "A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."⁴¹

Though the holding of *Knotts* has been cited to authorize all warrantless tracking on public streets, regardless of the type of device used, 42 an examination of the Court's questions during oral argument and a closer reading of the opinion indicate that the Court was actually very concerned with the capabilities of the specific device. During oral argument, the justices asked Deputy Solicitor General Andrew Frey about the range of the device, whether it was accurate if there were obstacles between the device and the receiver, whether it could reveal its location inside of the house, and even what radio frequency the device used. 43 At one point, one of the justices asked whether the tracking device used was different from planting an undercover agent in the laboratory and relying on the agent to send out information about the lab's location. 44 At another point, one of the justices asked if it could be analogized to following the device from an airplane. 45 Solicitor General Frey said it was similar, but added that "[o]f course, if you followed them closely, they would know that they were being followed, and it would

⁴⁰ *Id.* at 279.

⁴¹ *Id.* at 281.

⁴² See, e.g., United States v. Marquez, 605 F.3d 604, 609 (8th Cir. 2010) ("A person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another. When electronic monitoring does not invade upon a legitimate expectation of privacy, no search has occurred." (citation omitted)); United States v. Pineda-Moreno, 591 F.3d 1212, 1216 (9th Cir. 2010) ("[I]n Knotts, as in this case, '[t]he substitute . . . [by use of a tracking device] is for an activity, namely following a car on a public street, that is unequivocally not a search within the meaning of the amendment." (quoting Garcia, 474 F.3d at 997)).

⁴³ See generally Transcript of Oral Argument, United States v. Knotts, 460 U.S. 276 (1983) (No. 81-1802), 1982 U.S. Trans. Lexis 61.

⁴⁴ *Id.* at *19. Solicitor General Frey replied that it was different because, on the one hand, the undercover agent sees a great deal more than simply the location of the lab, but on the other hand, the agent is there with the consent of the people being investigated. *Id.*

⁴⁵ *Id.* at *10.

[Vol. 16:2

452

affect the effectiveness."⁴⁶ This sort of probing shows that the Court had a much more nuanced view of tracking technology than subsequent courts have given it credit for.⁴⁷

Some of this nuance made it into the opinion as well. The Court said, "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," and noted that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth." The court also discussed the "limited use which the government made of the signals from this particular beeper," and said there was no indication that the government was conducting "twenty four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision." 51

Even though the Court in *Knotts* was clearly concerned with the specifics of the device used, courts have subsequently abandoned that level of analysis, choosing instead to use *Knotts* as a crutch. In analyzing Fourth Amendment claims related to tracking devices, courts typically describe the device simply as a GPS tracker or an electronic monitoring device—perhaps with a sentence or two discussing some of the device's limitations—and then make a simple reference to the holding in *Knotts*. ⁵² In *United States v. Marquez*, for example, the Eighth Circuit referred to

⁴⁶ *Id*.

⁴⁷ See, e.g., United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) ("Moran had no expectation of privacy in the whereabouts of his vehicle on a public roadway. Thus, there was no search or seizure and no Fourth Amendment implications in the use of the GPS device."); United States v. Jones, 451 F. Supp. 2d 71, 88 (D.D.C. 2006) (citing *Knotts* for the proposition that a "person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another"), overruled by sub nom. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

⁴⁸ Knotts, 460 U.S. at 281.

⁴⁹ *Id.* at 282.

⁵⁰ *Id.* at 284.

⁵¹ *Id*.

⁵² See, e.g., Stone v. State, 941 A.2d 1238, 1250 (Md. Ct. Spec. App. 2008) (noting, without discussing the capabilities of the technology that, "[t]he GPS tracking device in the case at bar is simply the next generation of tracking science and technology from the radio transmitter 'beeper' in *Knotts*, to which the *Knotts* Fourth Amendment analysis directly applies").

453

2011 WHERE WE ARE WITH LOCATION TRACKING

the "GPS tracking device" throughout the opinion.⁵³ The court said the device could only reveal its location while the vehicle it was attached to was outside and noted that the investigators had to retrieve the device seven times during the course of the investigation in order to change its batteries.⁵⁴ This limited description constituted the extent of the court's discussion of the device's specific capabilities. Rather than examining the constitutional implications of the device's capabilities, the court was content to simply cite *Knotts* for the proposition that "[a] person traveling via automobile on public streets has no reasonable expectation of privacy in his movements from one locale to another."⁵⁵ Other courts have discussed tracking devices with a similar level of detail—or lack thereof.⁵⁶

In all of the cases involving constitutional questions about location tracking, only two opinions have even mentioned the name of the device used.⁵⁷ In *United States v. McIver*, the investigators used two devices.⁵⁸ The court described one device merely as "a global positioning system," but stated that the other was a Birddog 300, an "electronic transmitter that sends a weak signal or a 'beep' to an audio unit."⁵⁹ In *New York v. Weaver*, the court described the device used as a "Q-ball,"⁶⁰ though no publicly available devices fit the description of the device given by the investigator at trial.⁶¹ In a third case, *United States v. Garcia*,

⁵³ See generally United States v. Marquez, 605 F.3d 604 (8th Cir. 2010).

⁵⁵ *Id.* at 609 (citing *Knotts*, 460 U.S. at 281).

⁶⁰ People v. Weaver, 909 N.E.2d 1195 (N.Y. 2009).

⁵⁴ *Id.* at 607.

⁵⁶ See, e.g., Commonwealth v. Connolly, 913 N.E.2d 356 (Mass. 2009) (describing the device throughout the opinion as "the GPS tracking device"); Osburn v. State, 44 P.3d 523 (Nev. 2002) (discussing the use of an "electronic monitoring device"); United States v. Pineda-Moreno, 591 F.3d 1212, 1213 (9th Cir. 2010) (explaining that "[o]ver a four-month period, agents repeatedly monitored Pineda-Moreno's Jeep using various types of mobile tracking devices," but never discussing the devices used with any greater particularity).

⁵⁷ Even the concurrence in *Cuevas-Perez*, noted earlier for its attention to detail, *supra* note 22, did not discuss the name of the device used. United States v. Cuevas-Perez, 640 F.3d 272 (7th Cir. 2011).

⁵⁸ United States v. McIver, 186 F.3d 1119, 1123 (9th Cir. 1999).

⁵⁹ Id.

⁶¹ Investigator Peter Minahan of the New York State Police Special Investigation Unit described two devices used by the police: an Orion brand "live tracker," and a passive tracker commonly called a "Q-ball," which Minahan said was made by Q Electronics

[Vol. 16:2

454

Judge Posner did not discuss the exact device used, but he pointed to the TrackingKey made by LandAirSea as an example of the type of device that was used by investigators.⁶² He said the "memory tracking unit" that the police used was "pocket-sized, battery-operated, commercially available for a couple of hundred dollars" and "receives and stores satellite signals that indicate the device's location."

The cases that reference specific devices, however, are the exception. The vast majority of decisions on the legality of warrantless location tracking discuss the constitutional implications without considering the capabilities of the devices at issue.⁶⁴ Courts are able to speak generally about the technology of tracking devices because they can rely on *Knotts* and its progeny for the general proposition that a person has no expectation in the privacy of their movements on public streets.⁶⁵ But as this article will explain, this judicial shortcut has produced results that are inconsistent with Fourth Amendment doctrine.

B. Interpreting *Knotts* to Mean that All Location Tracking Is Outside the Protection of the Fourth Amendment Indicates that No Level of Suspicion Is Required to Use Such a Device, a Proposition that Courts are Reluctant to Support

On a few occasions, courts that have held that tracking is not a search have supported their conclusion by finding that the police had

Company. Testimony of Peter Minahan at 438, New York v. Weaver, 909 N.E.2d 1195 (N.Y. 2009) (No. 2009-0053). I found devices called the Q-Locator and the MiniQ, both made by Quantum, although both of those devices are real-time active and not passive trackers. For a product description of the Q-Locator, see *Q-Locator Real-Time Tracking Device*, JUSTGPSTRACKING.COM,

http://www.justgpstracking.com/q-locator-real-time-gps-tracking-device-cdma.html (last visited October 25, 2011). For the MiniQ, see *Quantum MiniQ Real-Time GPS Tracking Device*, JUSTGPSTRACKING.COM, http://www.justgpstracking.com/quantum-mini-q-real-time-gps-tracking-device-miniq.html (last visited October 25, 2011).

(

⁶² United States v. Garcia, 474 F.3d 994, 995 (7th Cir. 2007) ("So when the police later retrieved the device (presumably when the car was parked on a public street, as the defendant does not argue that the retrieval involved a trespass), they were able to learn the car's travel history since the installation of the device.")

⁶⁴ See supra notes 50-54 and accompanying text.

⁶⁵ *Id*.

455

2011 WHERE WE ARE WITH LOCATION TRACKING

some level of suspicion that was sufficient to justify the search.⁶⁶ In Marquez, for example, a tracking device installed on the defendant's truck revealed numerous trips between Des Moines and Denver. Using that information along with information they received from wiretaps and "pole cameras" that they installed in each city, investigators received a search warrant for multiple locations and uncovered hundreds of pounds of marijuana.⁶⁷ The Eighth Circuit determined that the defendant had "no reasonable expectation of privacy in his movements from one locale to another."68 "Consequently," the court wrote, "when police have reasonable suspicion that a particular vehicle is transporting drugs, a warrant is not required when, while the vehicle is parked in a public place, they install a non-invasive GPS tracking device on it for a reasonable period of time."69 However, this, of course, is not the consequence of determining that the defendant had no reasonable expectation of privacy in his movements from one locale to another. The real consequence of such a determination is that the police do not need any amount of suspicion to use a tracking device and may leave the device on an individual's car indefinitely.⁷⁰

More commonly, courts have hidden behind the Supreme Court's language in *Knotts* that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable." This passive approach by courts poses

See e a. United States v. Mar

⁶⁶ See, e.g., United States v. Marquez, 605 F.3d 604 (8th Cir. 2010); United States v. Garcia, No. 05-CR-155-C, 2006 U.S. Dist. LEXIS 29596 at *15-16 (W.D. Wis. May 10, 2006) ("In sum, the evidence establishes that the agents had significantly more than a reasonable suspicion that Garcia had returned to the meth trade and that as of May 26, 2005, his means of transportation was the Wilsons' Ford Tempo. Therefore, it was reasonable for the agents to attach a GPS device on the Tempo. This court should deny Garcia's motion to suppress.").

⁶⁷ Marquez, 605 F.3d at 607.

⁶⁸ Id. at 609.

⁶⁹ *Id.* at 609-10 (emphasis added) (citations omitted).

⁷⁰ Osburn v. State, 44 P.3d 523, 527 (Nev. 2002) (Rose, J., dissenting) ("The police will be able to place a vehicle monitor on any vehicle, for any reason, and leave it there for as long as they want. There will be no requirement that the monitor be used only when probable cause—or even a reasonable suspicion—is shown, and there will be no time limit on how long the monitor will remain.").

⁷¹ United States v. Knotts, 460 U.S. 273, 284 (1983). *See also* United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007); *Marquez*, 605 F.3d at 609.

[Vol. 16:2

456

two related problems. First, even though *Knotts* is thirty years old, until the D.C. Circuit's opinion in *Maynard*, no courts had tried to consider whether the use of tracking devices by law enforcement officers had become "dragnet-type." Second, without a warrant requirement (and without probing by the courts in every case that comes before them), determining whether law enforcement tracking devices have become "dragnet-type" is very difficult.

Has Tracking Already Become "Dragnet-Type"?

The D.C. Circuit in *Maynard* determined that the tracking devices used today have far surpassed "dragnet-type" as the *Knotts* Court used the term.⁷² The D.C. Circuit thought then-Justice Rehnquist's dicta about the possibility of dragnet searching, which quoted the defendant's concern about "twenty-four hour surveillance," referred not to mass surveillance of a large number of people but to prolonged surveillance of a single person.⁷³ If that is the proper interpretation of *Knotts*, we are long past the point where *Knotts* is controlling. As the court in *Maynard* noted, the tracking that occurred in *Knotts* consisted of the following of the defendants during a single, discrete trip—about 100 miles from Minnesota to Wisconsin.⁷⁴ Most of the tracking done by law enforcement—at least most of the tracking that is challenged in the courts—is for a much longer period of time.⁷⁵

⁷² United States v. Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) ("As we have explained, in *Knotts* the Court actually reserved the issue of prolonged surveillance. That issue is squarely presented in this case. Here the police used the GPS device not to track Jones's 'movements from one place to another,' but rather to track Jones's movements 24 hours a day for 28 days as he moved among scores of places, thereby discovering the totality and pattern of his movements from place to place to place." (quoting *Knotts*, 460 U.S. at 281)), *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

⁷³ *Id.* at 556-57 ("In reserving the 'dragnet' question, the Court was not only addressing but in part actually quoting the defendant's argument that, if a warrant is not required, then prolonged 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.' The Court avoided the question whether prolonged 'twenty-four hour surveillance' was a search by limiting its holding to the facts of the case before it, as to which it stated 'the reality hardly suggests abuse.'" (footnote omitted) (quoting *Knotts*, 460 U.S. at 283)).

⁷⁴ *Id.* at 556.

⁷⁵ See, e.g., id. (device attached for 28 days); Marquez, 605 F.3d 604 (police changed batteries seven times during investigation); United States v. Pineda-Moreno, 591 F.3d

457

2011 WHERE WE ARE WITH LOCATION TRACKING

Most courts have chosen not to interpret the Knotts warning in this manner. With the exception of the D.C. Circuit, all of the circuits that have considered the issue have held that the Knotts dicta was directed at prohibiting a programmatic scheme by the government to track the whereabouts of a large number of people.⁷⁶ In Garcia, Judge Posner, after concluding that electronic location tracking was not a search, noted, "It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment—that it could not be a search because it would merely be an efficient alternative to hiring another 10 million police officers to tail every vehicle on the nation's roads."77 Last year, the Eighth Circuit said it was "mindful of the concerns surrounding the use of electronic tracking devices."78 Citing Judge Posner, the Eighth Circuit said that the decreasing cost of tracking technology, coupled with the increased usefulness of the technology, made it imaginable "that a police unit could undertake 'wholesale surveillance' by attaching such devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity."⁷⁹ The Ninth Circuit has also expressed agreement with Judge Posner on this issue.80

But even these opinions demonstrate that there must be limits to the argument that "the [Fourth] [A]mendment cannot sensibly be read to mean that police shall be no more efficient in the twenty-first century than they were in the eighteenth."81 Therefore, all the circuits agree that

⁷⁸ Marquez, 605 F.3d at 610.

^{1212 (9}th Cir. 2010) (police installed device on seven different occasions). *But see, e.g.*, United States v. Moran, 349 F. Supp. 2d 425, 467 (N.D.N.Y. 2005) (police tracked defendant for two days).

⁷⁶ See, e.g., Garcia, 474 F.3d at 998.

⁷⁷ *Id*.

⁷⁹ *Id.* (citing *Garcia*, 474 F.3d at 998). Like the courts in *Knotts* and *Garcia*, the Eighth Circuit in *Marquez* promised that, "[s]uch an effort, if it ever occurred, would raise different concerns than the ones present here," implying that its holding here would not be controlling on such a case.

⁸⁰ *Pineda-Moreno*, 591 F.3d at 1216 n.2 ("We, like the Seventh Circuit, believe that '[s]hould [the] government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search." (alterations in original) (quoting *Garcia*, 474 F.3d at 998)).

⁸¹ Garcia, 474 F.3d at 998.

BERKELEY JOURNAL OF CRIMINAL LAW

if surveillance becomes wholesale, courts will have to step in and reconsider their position on location tracking.⁸²

2. Without a Warrant Requirement, How Will We Know if Tracking Becomes "Dragnet-Type"?

Vol. 16:2

Whatever the appropriate interpretation of the phrase, without a warrant requirement, it will continue to be difficult to know whether tracking has become "dragnet-type." Warrants have been heralded as protections against abuse because they create a record of requests and approvals.⁸³ This is the fear that drove Justice Marshall's dissent in *United States v. Murray*, which upheld a search pursuant to a proper warrant that the police received only after confirming, without a warrant, that evidence would be found.⁸⁴ Marshall argued that not requiring police to get a warrant in order to investigate—even if they were required to get one in order to use evidence at trial—"lends itself to easy abuse."⁸⁵ Judge Posner, in a recent case about location tracking, also discussed this "practical reason for requiring warrants when feasible."⁸⁶

⁸² See, e.g., id. ("One can imagine the police affixing GPS tracking devices to thousands of cars at random, recovering the devices, and using digital search techniques to identify suspicious driving patterns. One can even imagine a law requiring all new cars to come equipped with the device so that the government can keep track of all vehicular movement in the United States. It would be premature to rule that such a program of mass surveillance could not possibly raise a question under the Fourth Amendment"); Marquez, 605 F.3d at 610 ("It is imaginable that a police unit could undertake 'wholesale surveillance' by attaching such devices to thousands of random cars and then analyzing the volumes of data produced for suspicious patterns of activity. Such an effort, if it ever occurred, would raise different concerns than the ones present here." (citations omitted)); Pineda-Moreno, 591 F.3d at 1217 ("We, like the Seventh Circuit, believe that '[s]hould [the] government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search." (alterations in original) (quoting Garcia, 474 F.3d at 998)).

⁸³ Cf. William J. Stuntz, Warrants and Fourth Amendment Remedies, 77 VA. L. REV. 881, 910-18 (1991) (noting that warrants in the exclusionary rule context are important for counteracting judicial bias and police perjury).

⁸⁴ United States v. Murray, 487 U.S. 533, 551 (1988) (Marshall, J., dissenting) (claiming the Court's holding "emasculates the Warrant Clause and provides an intolerable incentive for warrantless searches").

⁸⁵ *Id.* at 550.

⁸⁶ Garcia, 474 F.3d at 996 ("[I]t forces the police to make a record before the search, rather than allowing them to conduct the search without prior investigation in the

459

2011 WHERE WE ARE WITH LOCATION TRACKING

In the area of location tracking, there are numerous examples of investigators attaching tracking devices to the cars of United States citizens without a warrant. In 2010, Yasir Afifi, a young Arab male, took his car for an oil change and found a satellite-based tracking device that turned out to belong to the FBI.87 Afifi gave the device back but brought a lawsuit against the FBI in which he alleged that "[FBI Director Robert] Mueller maintains a policy that authorizes its agents to use, without a warrant, devices similar or identical to the Tracking Device in order to collect and retain locational information pertaining to vehicles and their individual operators. This information is then used by Defendant Mueller and [the FBI's] agents to establish the associations a person maintains and otherwise reveals protected information."88 After Afifi's story went public, an animal rights activist said that she found a tracking device on her car in 2003.89 She said she knew of two Colorado residents who found devices attached to their cars in the same year and decided to check her own car after realizing that the investigators who usually followed her every move were no longer on her tail. 90 And in Weaver, the New York Court of Appeals noted, "[i]t is not clear from the record why defendant was placed under electronic surveillance."91

Finding any information about the devices used by law enforcement is incredibly difficult. In response to a written request for information, Special Agent Ann Todd of the FBI's Office of Public Affairs wrote, "Although we appreciate your interest, the information you requested is considered law enforcement sensitive and is not available to

expectation that if the search is fruitful a rationalization for it will not be difficult to construct, working backwards." (quoting United States v. Mazzone, 782 F.2d 757, 759 (7th Cir. 1986))).

j

⁸⁷ Bob Egelko, *San Jose Arab American Sues FBI Over GPS*, S.F. CHRONICLE (Mar. 3, 2011), *available at* http://articles.sfgate.com/2011-03-03/bay-area/28648677_1_gps-device-fbi-agent-fbi-director-robert-mueller.

⁸⁸ Complaint at 8, Afifi v. Holder, No. 11-CV-00460 (D.D.C. Mar. 2, 2011).

⁸⁹ Kim Zetter, *Battle Brews Over FBI's Warrantless GPS Tracking*, WIRED.COM (May 9, 2011), http://www.wired.com/threatlevel/2011/05/gps/. The activist, who was not named in the story, never returned the device to the FBI and decided to give it to Wired and iFixIt.com after reading a story about Afifi. For a step-by-step breakdown and video of iFixIt technicians disassembling the device, *see Tracking Device Teardown*, IFIXIT, http://www.ifixit.com/Teardown/Tracking-Device-Teardown/5250/1 (last visited Oct. 25, 2011).

⁹⁰ Zetter, supra note 86.

⁹¹ People v. Weaver, 909 N.E.2d 1195, 1196 (N.Y. 2009).

Herbert (442-503) Fall 2011

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

the public."92 The NYPD stated that the department does not respond to information requests from students.93 The New York State Police responded to a request with an e-mail saying, "We will respectfully decline discussing this type of technology since the technology we currently use is basically the same type of technology we have been using for many years. The discussion of our GPS surveillance and it's [sic] progression of use within our agency could possibly compromise the security and integrity of our investigative techniques."94 In response to a modified list of questions that could not compromise the investigative techniques, the State Police said, "Please let us clarify, after speaking with our Investigative and Criminal Intelligence sections, we will respectfully decline discussing any of this technology and its use."95 The New York State Office of the Inspector General also refused to divulge any information, citing the law enforcement exception to New York's Freedom of Information Law, which protects records that would "reveal criminal investigative techniques or procedures, except routine

⁹² E-mail from Ann Todd, FBI Office of Public Information, to author (May 3, 2011, 6:28 PM) (on file with author).

⁹³ When I first called the NYPD Public Information Office, I was told to e-mail the office. I sent two e-mails on March 23, 2011 and March 29, 2011, and did not receive any response. I followed up with a phone call, during which I was told that, because of the long list of requests the NYPD Public Information Office receives, student requests go to the bottom of the pile. Unfortunately, I did not record the date of these conversations or obtain the names of the people I spoke with.

⁹⁴ E-mail from Public Information Office, New York State Police, to author (Apr. 5, 2011, 2:44 PM) (on file with author).

⁹⁵ E-mail from Public Information Office, New York State Police to author (Apr. 21, 2011 11:44 AM) (on file with author) (responding to an e-mail with the following questions: "Does the New York State Police have any policies governing the use of tracking devices (GPS, infrared, or radio-frequency enabled)? If so, may I please have a copy of the policy or policies?"). The Public Information Office had previously not responded to an e-mail with the following questions, later revised so as to not compromise the integrity of investigatory techniques: "How many GPS surveillance devices does the New York State Police own? Additionally, how many radio-frequency enabled transmitters (such as the old Birddogs) does the New York State Police own? Finally, when did the State Police get its first GPS surveillance device and its first radio-frequency enabled tracking device?" Email from Public Information Office, *supra* note 91.

461

2011 WHERE WE ARE WITH LOCATION TRACKING

techniques and procedures." The Metropolitan Police Department in Washington, D.C. did not respond to requests for information.

Obtaining information from the companies that make these devices is not much easier. A commenter on the website Reddit,⁹⁷ where a photo of the device placed on Afifi's car was posted, identified it as an Orion product sold by Cobham.⁹⁸ After a half-dozen phone calls to Cobham, I was told that no one in Cobham's Tracking and Locating Division would be able to speak with me.⁹⁹ Similarly, Law Enforcement Associates (LEA) and GPS International Technologies (GPSit), both companies that sell specialized equipment, including tracking equipment, to law enforcement agencies, show only a limited selection of their products on the public portion of their website and require a verified law enforcement account to access the full selection of their products.¹⁰⁰

Litigators have also come up short, sometimes because they did not ask the right questions, and other times because they were often not given proper answers. Zahra Billoo, Afifi's lawyer, did not receive any information from the FBI about the device that was placed on Afifi's car. Similarly, Eduardo Balarezo, Jones's lawyer in the *Maynard* case, said the government filed a protective order to avoid releasing details about the device and its location on the car. 102

_

⁹⁶ Letter from Stephen Del Giacco, Records Access Officer, State of New York Office of the Inspector General, to author (June 8, 2011) (on file with author).

⁹⁷ Reddit is a website where users post content, such as links to articles or videos, and other users rate the quality of the post and post comments. The posting, comments and voting are done through anonymous usernames. *Frequently Asked Questions*, REDDIT, http://www.reddit.com/help/faq (last visited Sept. 27, 2011).

⁹⁸ Kim Zetter, *Caught Spying on Student, FBI Demands GPS Tracker Back*, WIRED.COM, (Oct. 7, 2010, 10:13 PM) http://www.wired.com/threatlevel/2010/10/fbi-tracking-device/.

⁹⁹ Telephone Interview with Monica Hallman, Senior Manager, Public Relations, Cobham (Apr. 27, 2011).

¹⁰⁰ See generally GPS Tracking, LEA CORP, http://www.leacorp.com/pages/GPS-Tracking.html (last visited Oct. 25, 2011); Law Enforcement Portal Overview, GPSIT, http://www.gpsit.com/en/portal-

overview.html?phpMyAdmin=1f2e09a0fb9200d6e3ef8410659a78f3 (last visited Oct. 25, 2011).

¹⁰¹ E-mail from Zahra Billoo, Executive Director, Council on American-Islamic Relations, to author (May 17, 2011, 6:53 PM).

 $^{^{102}}$ E-mail from Eduardo Balarezo, Balarezo Law, to author (April 15, 2011, 12:05 EST).

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

It has been similarly difficult to determine how widespread cellsite tracking is. In 2009, a Sprint/Nextel executive was secretly recorded saying that the company had received 8 million requests from law enforcement for location information from Sprint/Nextel phones in the previous thirteen months. 103 This still does not explain how often law enforcement officers use this technique, however, because, as Sprint explained, "the figure represents the number of individual 'pings' for specific location information, made to the Sprint network as part of a series of law enforcement investigations and public safety assistance requests during the past year. It's critical to note that a single case or investigation may generate thousands of individual pings to the network as the law enforcement or public safety agency attempts to track or locate an individual."104 In 2007, an FBI cell-tracking expert testified that he used cell-site data to locate fugitives nearly 150 times. 105 And in a 2007 story, The Washington Post cited an anonymous magistrate judge who said that he had denied about a dozen requests for cell-site information over the course of the previous six months, some of which had simply asserted that the evidence the investigator had was "consistent with the probable cause standard."106 The story noted, "The requests and orders are sealed at the government's request, so it is difficult to know how often the orders are issued or denied."107

The Afifi incident, the animal activist incident, the judge's statement in *Weaver* that it was unclear why the police initially attached the tracking device to the defendant's car, and the large number of police requests for cell-site data provide evidence of the widespread use of

_

¹⁰³ Kevin Bankston, Surveillance Shocker: Sprint Received 8 Million Law Enforcement Requests for GPS Location Data in the Past Year, ELECTRONIC FRONTIER FOUNDATION (Dec. 1, 2009, 1:45 PM), http://www.eff.org/deeplinks/2009/12/surveillance-shocker-sprint-received-8-million-law.

¹⁰⁴ Rich Pesce, *Sharing Location Information*, SPRINT (December 1, 2009, 3:30 PM), http://community.sprint.com/baw/community/sprintblogs/announcements/blog/2009/12/01/sharing-location-information.

¹⁰⁵ Brief of Amici Curiae Electronic Frontier Foundation et al. at 15, *In re* U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304 (3d Cir. 2010) (No. 08-4227).

¹⁰⁶ Ellen Nakashima, Cellphone Tracking Powers on Request, WASH. POST, November 23, 2007, available at http://www.washingtonpost.com/wp-dyn/content/article/2007/11/22/AR2007112201444.html.
¹⁰⁷ Id.

2011 WHERE WE ARE WITH LOCATION TRACKING

463

location tracking devices by law enforcement officers, even with little or no suspicion. But without a warrant requirement, investigators aren't "force[d] . . . to make a record before the search." All of the circuits that have considered the issue of warrantless location tracking have agreed that the courts must reconsider the issue if mass surveillance becomes the norm. But with no court records and widespread secrecy from government agencies and device manufacturers, courts have no way of knowing whether we have crossed that line. As Professor Anthony Amsterdam famously wrote, the courts have no way of "policing the police." Policing the police."

C. Legislatures Have Also Failed to Analyze Vigorously the Different Kinds of Tracking Technology

One solution could be to allow legislatures exclusive authority to regulate the use of tracking technology. At least one court has explicitly taken this approach, urging its state legislature to "consider regulating both police and private use of GPS tracking technology."¹¹¹ This may be the kind of situation where legislatures, not courts, are the appropriate vehicles for regulation. The technology is rapidly changing, and judges are not familiar with how the technology works.¹¹²

Professor Orin Kerr wrote in a well-known article on how the Fourth Amendment should govern changing technology that, when technology is in flux, "[t]he stable relationship between law enforcement conduct and privacy in traditional cases is replaced by a fluid and often counter-intuitive relationship. As a result, the task of creating rules to

-

¹⁰⁸ United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

¹⁰⁹ See supra note 79.

¹¹⁰ Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 371 (1974). *See also id.* (noting that indiscriminate searches and seizures are bad for two reasons: they expose people to unjustified intrusion by the government; and they expose citizens to the possibility of arbitrary intrusion by despotic rulers).

¹¹¹ State v. Sveum, 769 N.W.2d 53, 56 (Wis. Ct. App. 2009).

¹¹² During the Scott Weaver trial, for example, the judge seemed to think the technology was so complicated that a jury couldn't figure out how to use it during jury deliberations: "Maybe if they want to see, they will have to see it in the courtroom, because maybe the equipment is so sophisticated that it's not the kind of thing that we should let them take into the jury room and try to figure out how to use it." Testimony of Peter Minahan, *supra* note 59.

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

protect privacy becomes significantly more dynamic and complex."¹¹³ Kerr concludes that, given the constantly shifting technological landscape, as well as institutional barriers such as ex post review and limited information, "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing."¹¹⁴ Kerr advocates for "judicial caution" and believes that courts should "be wary of imposing broad privacy protections against the government's use of new technologies."¹¹⁵

Kerr's criticisms of judicial review of rapidly changing technology are valid, but legislatures face many similar problems as well. Kerr argues that statutes can be more comprehensive than judicially created rules, but that is only true if the legislature can anticipate developments in technology or is able to regularly amend its statute, which often does not happen. And during their delay, law enforcement will not hesitate to use all unregulated options to investigate citizens. Location tracking seems to be a perfect example. For years, Sen. Ron Wyden has touted the need for regulation that ensures "that law enforcement and intelligence

¹¹³ Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 865 (2004).

115 *Id.* at 888.

116 Kerr arque

_

¹¹⁴ *Id.* at 806.

protective of privacy than the judicial branch and that rules created by legislatures are often more clear and nuanced than those created by courts, which must create rules based on the specific case in front of them. *Id.* at 806. *But see* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 762-63 (2005) (arguing, *inter alia*, that the warrant requirement gives judicially created rules "a remarkable degree of flexibility" and that statutes often lack effective remedies because they don't include an exclusionary rule). ¹¹⁷ Solove, *supra* note 113, at 763 (noting, for example, that The Wiretap Act, originally enacted in 1968, does not cover silent video surveillance). "Ironically, [the Foreign Intelligence Surveillance Act] regulates video surveillance, but the [Electronic Communications Privacy Act] does not, meaning that the video surveillance of a foreign spy receives more federal statutory protection than that of a U.S. citizen." *Id.* at 764 (footnote omitted).

¹¹⁸ For a discussion on a long history of law enforcement overstepping its bounds during, for example, the Red Scare and the civil rights movement, *see* Laura Donohue, *Anglo-American Privacy and Surveillance*, 96 J. CRIM. L. & CRIMINOLOGY 1059 (2006). *See also* Nakashima, *supra* note 103 (quoting an anonymous magistrate judge as saying that some agents attach affidavits that claim only that the evidence is "consistent with the probable cause standard" of Federal Rule of Criminal Procedure 41).

2011 WHERE WE ARE WITH LOCATION TRACKING

465

agencies can take advantage of these new technologies in a way that doesn't run roughshod over every American's right to keep the records of what they do every day private." Yet Congress has not passed legislation addressing the issue and only a handful of states have done more. Even those legislators interested in placing statutory limitations on the use of tracking devices tend to care more about the broad issues than the gritty details, meaning the statutes that are passed can sometimes be vague and require interpretation by courts. 122

Rather than expecting courts to take a hands-off approach to regulating rapidly changing technology, as Kerr suggests, it makes more sense to require that both legislatures and courts engage in a more surgical inquiry into the technological capabilities of the devices in question when making difficult decisions about law enforcement's authority to track a person's location without a warrant. As Professor Sherry Colb wrote in response to Kerr, "absent some reason to think that the courts will systematically overprotect privacy, the fact that we can generally rely upon the democratic process is no reason to forego the additional protection for individual rights that the judiciary affords for those occasions when majority rule threatens to become majority tyranny." 123

II. THE TECHNOLOGICAL DEVELOPMENT OF LOCATION-TRACKING DEVICES

-

¹¹⁹ Senator Ron Wyden, Remarks as Prepared for Delivery at the Cato Institute of Policy Forum (January 26, 2011), *available at*

http://wyden.senate.gov/newsroom/press/release/?id=508ebf80-4ca8-4e47-ba5b-6146fe75dae1.

¹²⁰ For a list of state regulations, see *supra* notes 12-13.

¹²¹ See e-mail from John Dickas, staffer for Sen. Ron Wyden, to author (Mar. 31, 2011, 05:34 PM) (on file with author) (stating that his office has focused on legislation covering all different types of tracking technology rather than identifying all of the devices that are in use).

¹²² See supra notes 13-15 and accompanying text (discussing the confusion surrounding the California statute limiting location tracking, which created an exception for "the lawful use of an electronic tracking device by a law enforcement agency," but did not define the term lawful).

¹²³ Sherry Colb, A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures, 102 MICH. L. REV. 889, 903 (2004).

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

Location-tracking devices are commonly divided into four different categories: radio-frequency enabled trackers (commonly referred to as "beepers"), satellite-based tracking devices, cell-site data tracking devices, and infrared tracking devices, all of which are unique.¹²⁴

When Congress passed the Electronic Communications Protection Act in 1986,¹²⁵ it defined "electronic tracking devices" by describing a radio-frequency enabled beeper.¹²⁶ But now, the vast majority of the devices purchased by law enforcement agencies are primarily satellite-based devices, which use signals from a number of different satellites to triangulate the position of the tracking device without any effort from law enforcement officials.¹²⁷ Cell-site tracking devices have also joined the market since *Knotts* was decided in 1983. These devices use information that cell phones already send to cell phone towers, such as the strength and direction of the signal at multiple towers

¹²⁴ See, e.g., People v. Weaver, 909 N.E.2d 1195, 1199 ("Knotts involved the use of what we must now, more than a quarter of a century later, recognize to have been a very primitive tracking device."); In re U.S. for an Order Directing a Provider of Elec.
Commc'n Serv. to Disclose Records to the Gov't, 620 F.3d 304, 311 (3d Cir. 2010) (distinguishing between cell-site data and GPS data and noting that, "[t]he Government argues that it did not seek GPS information in this case"); Ramya Shah, supra note 17, at 285 (noting that beepers "are smaller and less sophisticated than GPS devices"); Otterberg, supra note 17, at 694 ("Though GPS devices and beepers can produce similar results—they both reveal the tracking device's location at any given moment—GPS devices possess much greater potential for accuracy. More importantly, GPS devices track location regardless of whether a GPS receiver, which processes the tracking device's signal to reveal location information, is in the vicinity." (footnote omitted)).
125 Electronic Communications Privacy Act of 1986 (ECPA), Pub.L. 99–508, 100 Stat. 1848.

¹²⁶ S. Rep. No. 99-541, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3564 (defining "electronic tracking devices" as "one-way radio communication devices that emit a signal on a specific radio frequency. This signal can be received by special tracking equipment and allows the user to trace the geographical location of the transponder. Such 'homing' devices are used by law enforcement personnel to keep track of the physical whereabouts of the sending unit, which might be placed in an automobile, on a person, or in some other item")

¹²⁷ See, e.g., Testimony of Solomon Bitsie at 6, United States v. Jones, 451 F. Supp. 2d 71 (D.C. 2006) (No. 05-0386) (agreeing with attorney who asked, "when you say 'tracking technology,' you're talking about GPS systems?"), overruled by sub nom. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

467

Where We Are with Location Tracking 2011

in the area and a listing of all the towers in the area. 128 Though *Knotts* has long been the seminal case for location tracking, these four technologies are drastically different in the ways they work and their degrees of accuracy. In analyzing tracking technology, it is important to have a complete understanding of the development of the technology.

Radio-Frequency Enabled Beepers

Since 1983, the legal view of location tracking has focused on the "beeper" that was used by investigators in Knotts. 129 "A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver," the Supreme Court explained in that case.¹³⁰ In Knotts, Drug Enforcement Administration (DEA) officers followed a beeper signal to a secluded cabin owned by defendant Leroy Knotts.¹³¹ During their pursuit, the officers lost the signal on multiple occasions as the driver of the car made evasive maneuvers and made repeated U-turns to see if he was being followed.¹³² The officers tracked the car 100 miles from Minnesota to Wisconsin without being detected. At the cabin, they obtained a search warrant and found a secret drug laboratory. 133

This technology was used throughout the first half of the twentieth century to assist aerial and nautical navigation, 134 but it was not until the 1970s that the technology used by law enforcement was first challenged in the courts. 135 The timing of these cases coincides with the first Birddog tracker, 136 which was the device used in *Knotts*. 137

¹³² United States v. Knotts, 662 F.2d 515, 516 (8th Cir. 1981).

¹³⁴ See infra notes 142-43 and accompanying text.

¹²⁸ See In re Pen Register, 396 F. Supp. 2d 747 (S.D. Tex. 2005).

¹²⁹ See supra note 45 and accompanying text (citing cases that rest almost entirely upon the holding in *Knotts*).

¹³⁰ United States v. Knotts, 460 U.S. 276, 277 (1983).

¹³⁵ See, e.g., United States v. Holmes, 521 F.2d 859 (5th Cir. 1975); United States v. Martyniuk, 395 F. Supp. 42 (D. Or. 1975); United States v. Carpenter, 403 F. Supp. 361 (D. Mass. 1975).

¹³⁶ See Law Enforcement Associates Reports Robust Sales of New BirddogTM GPS Tracking System, MARKETWIRE (August 23, 2007), http://www.marketwire.com/pressrelease/Law-Enforcement-Associates-Reports-Robust-Sales-of-New-Birddog-GPS-Tracking-System-AMEX-AID-763386.htm (quoting LEA President Paul Feldman saying, "[t]he original Birddog was a radio frequency (RF)-enabled tracking device

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

Stephen Hagenah, one of the investigators who followed the beeper to Knott's cabin, explained that the device emitted a signal (a beep) once every two seconds when it was stationary and as fast as two or three times per second when it was moving. According to Hagenah, the agents following the device could not tell how fast it was moving but could tell if it was moving toward them or away from them by the strength of the signal. At trial, Hagenah had the following exchange with Assistant United States Attorney Ann Montgomery:

Montgomery: Can you explain how that [the beeper] works and how you went about monitoring it?

Hagenah: We had one unit specifically built to monitor the signal from that transmitter and several other people had just regular scanner radios, which would receive the beeping signal from the transmitter in the bucket.

Montgomery: Now there is a device in here that emits a beep at periodic intervals, is that correct?

Hagenah: Yes.

Montgomery: Is it an audible beep that you could hear?

Hagenah: No, not without a radio receiver.

Montgomery: So it beeps on a frequency you can pick up with a receiver, is that correct?

Hagenah: Yes, that is correct.140

As Hagenah noted in that exchange, there were two ways to follow the device. The Minnesota Bureau of Criminal Apprehension had a receiver made specifically to follow the transmitter. That device had a needle that would move when it picked up the signal, and if it moved to the left, the investigators knew the signal had come from the right. Hagenah followed the suspect with a more rudimentary device: a simple

introduced by our AID division in the 1970s, and over time it became the most widely used covert tracking system among local and federal law enforcement agencies").

-

¹³⁷ Interview with Stephen Hagenah, Retired Investigator, Minnesota Bureau of Criminal Apprehension (April 11, 2011) (transcript on file with author).

¹³⁸ *Id*.

¹³⁹ *Id.*

¹⁴⁰ Transcript of Record at 103, United States v. Knotts, No. 3-80-CR-49 (D. Minn. 1981) (on file with author), reprinted in relevant part in Joint Appendix, United States v. Knotts, 460 U.S. 276 (1983) (No. 81-1802), 1981 U.S. Briefs 1802 at *27.

¹⁴¹ Interview with Stephen Hagenah, *supra* note 134.

2011 Where We Are with Location Tracking

469

police scanner that was tuned to the correct frequency. 142 Later versions of the Birddog product line, such as the Birddog 300 used in McIver, were equipped with "a 180 degree dial with a needle that points in the direction of the transmitter."143

The basic technology of using radio signals to navigate toward an object has been available since the beginning of the 20th century. 144 Until fairly recently, a system of radio transmitters called LORAN provided civilian and military users in the coastal waters of the continental United States and Alaska with a method of navigation accurate to 0.25 nautical miles. 145 However, in 2010, the Coast Guard published a Federal Register notice announcing its decision to terminate the LORAN signal, saying "LORAN-C has, as a result of technological advancements in the last 20 years, became [sic] an antiquated system no longer required by the armed forces, the transportation sector or the nation's security interests and is used only by a small percentage of the population."146

¹⁴² *Id*.

¹⁴³ United States v. McIver, 186 F.3d 1119, 1123 (9th Cir. 1999).

¹⁴⁴ See Waldemar Kaempffert & Car Dienstbach, What of Tomorrow's Flying? POPULAR SCIENCE MONTHLY, Oct. 1919, at 47, 49, available at

http://books.google.com/books?id=KSkDAAAAMBAJ&printsec=frontcover#v=onepage &q&f=false (noting a government plan to place radio beacons all over the country and describing a radio beacon as "[s]imply a station from which wireless waves are sent in all directions, to be picked up by the flyer lost in a fog or groping his way through the night"); Broadcast Station Can Guide Flyer, POPULAR SCIENCE, Apr. 1931, at 54, available at

http://books.google.com/books?id=8ycDAAAAMBAJ&printsec=frontcover&dq=Popul ar+Science+1931&hl=en&ei=WRWrTZrUFsyL0QGLmdn5CA&sa=X&oi=book_resul t&ct=result&resnum=4&ved=0CDoQ6AEwAw#v=onepage&q&f=false ("In parts of the country where official radio beacon stations for aircraft do not yet exist, any broadcast station can guide a plane by means of a new 'radio compass' The broadcast program, received through a set much like any standard aircraft radio, actuates a needle on a round dial beside the pilot. When the needle swings to the right or left of the center of the dial, it shows the pilot he is off his course.").

¹⁴⁵ U.S. Coast Guard Navigation Center, Loran-C User Handbook, at F2, available at http://www.navcen.uscg.gov/pdf/loran/handbook/Loran-C_Users_Handbook_entire.pdf (last visited Oct. 28, 2011).

¹⁴⁶ Loran-C General Information, U.S. COAST GUARD NAVIGATION CENTER, http://www.navcen.uscg.gov/?pageName=loranMain (last visited October 25, 2011) ("The Coast Guard understands that LORAN-C is still used by a small segment of the public and that those users will have to shift to GPS or other systems; however,

BERKELEY JOURNAL OF CRIMINAL LAW

Vol. 16:2

Like the radio-frequency navigation system LORAN, radiofrequency enabled tracking devices appear to be extinct. Some version of the Birddog product line, which was used widely during the 1970s and in the Knotts investigation, was used as late as 1997,147 and Investigator Hagenah stated that the Minnesota Bureau of Criminal Apprehension still uses the Birddog. 148 However, it appears that the old Birddog, described in a press release as "the most widely used covert tracking device by local and federal law enforcement agencies," was replaced with a satellite-based tracking device when LEA re-launched the product in 2007.149

Satellite-Based Tracking Devices

The Coast Guard terminated the LORAN signal primarily because of the widespread use of the more effective NAVSTAR Global Positioning System. 150 Over the last three decades, GPS technology, which uses signals from satellites to triangulate a target's position, ¹⁵¹ has developed from an experimental program used solely by the military to a comprehensive and accurate system widely used by civilians.

continued use of limited resources to operate LORAN-C is no longer prudent use of taxpayer funds and is not allowed under the 2010 DHS Appropriation Act.") ¹⁴⁷ McIver, 186 F.3d at 1123 ("At 3:30 a.m. on September 23, 1997, Special Agent Deist and Officer Billy Stewart placed two magnetized tracking devices on the undercarriage of the Toyota 4Runner registered to McIver. One of the devices was a global positioning system. The other was a Birddog 300 electronic transmitter that sends a weak signal or a 'beep' to an audio unit ('monitor') installed in the officer's vehicle.").

¹⁴⁸ Interview with Stephen Hagenah, *supra* note 134.

¹⁴⁹ Law Enforcement Associates Receives Orders for 15 Birddog GPS Surveillance Systems from Four Federal Agencies, MARKETWIRE (Sept. 8, 2008),

http://www.marketwire.com/press-release/Law-Enforcement-Associates-Receives-Orders-15-Birddog-GPS-Surveillance-Systems-From-AMEX-AID-897352.htm ("LEA re-launched the Birddog in the first quarter of 2007, when the company introduced an all-new tracking device based on advanced GPS technology.").

¹⁵⁰ Terminate Long Range Aids to Navigation (Loran-C) Signal, 75 Fed. Reg. 998-01 (noticed Jan. 7, 2010) ("As a result of technological advancements over the last 20 years and the emergence of the U.S. Global Positioning System (GPS), Loran-C is no longer required by the armed forces, the transportation sector, or the nation's security interests, and is used only by a small segment of the population.").

¹⁵¹ For a high-level discussion on how GPS works, see Hutchins, *supra* note 16, at 414-21.

471

2011] WHERE WE ARE WITH LOCATION TRACKING

GPS¹⁵² was conceptualized by a Joint Program Office composed of branches of the armed services and other agencies.¹⁵³ The system's satellites continuously transmit "ranging signals" on different frequencies.¹⁵⁴ The ranging signals include information about the satellite's location, the health of the satellite, and the location of other satellites.¹⁵⁵ Users compare the signals from four satellites with a usergenerated signal and calculate the distance or range to the satellite.¹⁵⁶ With the ranging information from four satellites, a user can calculate four unknowns (generally latitude, longitude, altitude and a correction to the user's clock, which is a very important piece of data for ensuring accuracy).¹⁵⁷

The satellite system was designed with twenty-four satellites to ensure that a minimum of six—and often many more—are in view at any point, allowing for the occasional satellite outage without a break in service. This design has proven to have staying power; in 1996, Bradford Parkinson, known as the father of GPS, wrote, "[t]he

 152 In this paper, the term GPS always refers to the NAVSTAR GPS system. See supranote 1.

¹⁵⁵ J.J. Spilker Jr. & Bradford W. Parkinson, *Overview of GPS Operation and Design, in* 1 GLOBAL POSITIONING SYSTEM: THEORY AND APPLICATIONS, *supra* note 150, at 32. This process requires extremely accurate clocks in both the satellites and in the user's receiver. The satellite clocks regularly receive clock time corrections from stations on the ground, *id.* at 29, and the user can estimate the error on its clock because the satellite repeats the signal every millisecond (on the Clear Acquisition Code), and the user can match the beginning of the signal to the proper millisecond. *Id.* at 34-35.

¹⁵³ Bradford W. Parkinson, *Introduction and Heritage of NAVSTAR, the Global Positioning System, in* 1 GLOBAL POSITIONING SYSTEM: THEORY AND APPLICATIONS 4, 6 (Bradford W. Parkinson & James J. Spilker, Jr. eds., Progress in Astronautics and Aeronautics Ser. No. 163, 1996) ("To increase efficiency and reduce interservice bickering, 'joint' programs were formed that forced the various services to work together. The GPS was one of the earliest examples. It was decreed to be a Joint Program, with a Joint Program Office (JPO) located at the Air Force's Space and Missile Organization and to have multiservice participation The first program director was Dr. (Col.) Bradford W. Parkinson[], supported by Deputy Program directors—eventually from the Army, Navy, Marine Corps, Defense Mapping Agency, Coast Guard, Air Logistics Command and NATO.").

¹⁵⁴ See id. at 10-11.

¹⁵⁷ Parkinson, *supra* note 150, at 10-11.

¹⁵⁸ *Id.* at 13.

[Vol. 16:2

472

Operational GPS system of today is virtually identical to the one proposed in 1973."¹⁵⁹

The satellites were launched in blocks, with the first satellite launched in 1978 and the final Block I satellite launched in 1985. 160 From the beginning, the government recognized the advantages associated with allowing civilian access to the satellite system, and in September 1983, Press Secretary Larry M. Speakes announced that President Ronald Reagan was "prepared to make available to civilian aircraft[] the facilities of its Global Positioning System when it becomes operational in 1988." 161

The final Block IIA satellite was launched in 1993, finally creating a network of 24 satellites, ¹⁶² although the system did not become fully operational until April 1995. ¹⁶³ The original presidential policy pledged to "continue to provide the GPS Standard Positioning Service for peaceful, civil, commercial and scientific use on a continuous, worldwide basis, free of direct user fees." ¹⁶⁴

Though civilians have always had access to the signals from the GPS, the civilian signal has always been separate from the military signal. The two ranging signals were broadcast at different frequencies: L1 and

¹⁵⁹ *Id.* at 10.

¹⁶⁰ *Id.* at 21 (detailing in a table all the satellites launched before the end of Block IIA in 1993).

¹⁶¹ Larry M. Speakes, Deputy Press Secretary, Statement on the Soviet Attack on a Korean Civilian Airliner (September 16, 1983), *available at* http://www.reagan.utexas.edu/archives/speeches/1983/91683c.htm.

¹⁶² Parkinson, *supra* note 150, at 21. For a table of all the satellites launched between November 26, 1990 and December 1, 2010, see Richard B. Langley, *The Almanac*, GPS WORLD (Dec. 1, 2010), http://www.gpsworld.com/gnss-system/almanac/the-almanac-4265.

¹⁶³ Rick W. Sturdevant, NAVSTAR, The Global Positioning System: A Sampling of Its Military, Civil, and Commercial Impact, in SOCIETAL IMPACT OF SPACEFLIGHT 331, 332 (Steven J. Dick & Roger D. Launius eds., 1997) (noting also the cost of \$10-\$12 billion to field the system of 24 satellites); See also GNSS Frequently Asked Questions—GPS, FAA,

http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/faq/gps/index.cfm?print=go (last visited Apr. 22, 2011).

¹⁶⁴ Press Release, Office of Science and Tech. Policy, National Security Council, Fact Sheet: U.S. Global Positioning System Policy (Mar. 29, 1996) *available at* http://clinton2.nara.gov/WH/EOP/OSTP/html/gps-factsheet.html. That language was later codified by Congress in 10 U.S.C. § 2281(b) (2009).

473

2011] WHERE WE ARE WITH LOCATION TRACKING

L2. The military encrypted the "P-Code" signal on the L2 frequency, leaving civil users with access only to the "C/A Code" signal on L1. 165 Not only is the P-Code a more precise signal, but users with access to only one signal (L1) are also unable to calibrate as effectively, so the civilian signal is less precise. 166 The civilian signal is referred to as the Standard Positioning Service (SPS), and the military signal is referred to as the Precise Positioning Service (PPS). 167 The National Executive

Darkinson subra noto 150 at

¹⁶⁵ Parkinson, *supra* note 150, at 11-12. In 1998, Vice President Al Gore announced that the United States would add two new civil signals to future GPS satellites. Press release, The White House, Vice President Gore Announces New Global Positioning System Modernization Initiative (Jan. 25, 1999), *available at*

http://clinton6.nara.gov/1999/01/1999-01-25-vice-president-gore-announces-new-global-positioning-system.html ("[T]he new signals will significantly improve the robustness and reliability of GPS for civil users, and will enable unprecedented real-time determination of highly accurate position location anywhere on Earth. This new capability will spur new applications for GPS, further expanding the rapidly growing market for GPS equipment and services worldwide."). The first satellite broadcasting the new L5 signal was launched in 2009. L5 GPS Signal Now Being Transmitted from IIR(M)-20 Satellite, GPS WORLD (Apr. 10, 2009),

http://www.gpsworld.com/defense/news/15-gps-signal-now-being-transmitted-iirm-20-satellite-7079. However, a full constellation of satellites broadcasting the L5 channel will not be available until 2018. *First of New Generation of GPS Satellites Launched into Orbit*, FAA (Apr. 7, 2009),

http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/techops/navservices/gnss/waas/news/media/FirstL5_GPS_SV_LE_040709.pdf

segments of a 200-day code) that is broadcast at ten times the rate of [the C/A Code], 10.23MHz. Because of its higher modulation bandwidth, the code ranging signal is somewhat more precise. This reduces the noise in the received signal but will not improve the inaccuracies caused by biases."). Parkinson explains that it was originally thought that the P Code would be about seven times more accurate than the C/A Code primarily because of a faster chip rate, but technology was actually able to fix the error "to the point that receiver measurement was an insignificant error source." *Id.* at 24-25. Parkinson calls the C/A Code the Clear Acquisition Code, *id.* at 12, but the

Parkinson calls the C/A Code the Clear Acquisition Code, *id.* at 12, but the Performance Standard calls the C/A Code the "coarse/acquisition" code. *See* POSITIONING, NAVIGATION, AND TIMING EXECUTIVE COMMITTEE, DEP'T OF DEFENSE, GLOBAL POSITIONING SYSTEM STANDARD POSITIONING SERVICE

PERFORMANCE STANDARD (4th ed. 2008), available at

http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf.

¹⁶⁷ See Steve Ditlea, Real Men Don't Ask Directions, POPULAR SCIENCE, March 1995, at 86. available at

http://books.google.com/books?id=q7ShNdfNiw8C&printsec=frontcover#v=onepage&q&f=false.

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

Committee for Space-Based Positioning, Navigation, and Timing has said that, at least in theory, SPS is now as accurate as PPS.¹⁶⁸ According to the organization, PPS "still gives advantages to the military beyond accuracy," but it is not clear what these advantages are.¹⁶⁹

Additionally, because of fears that the GPS would be used against the U.S. military, the government initially had the ability to introduce errors into the broadcast or intentionally desynchronize the satellite clock, a process known as Selective Availability. Selective Availability resulted in errors of up to 100 meters, though private companies quickly started developing methods of minimizing that error with a process known as Differential GPS. 172

President Clinton discontinued Selective Availability beginning May 1, 2000, saying, "Civilian users will realize a dramatic improvement in GPS accuracy," and receivers are now able to pinpoint their location up to ten times more accurately than before Selective Availability was disabled.¹⁷³ At the time of President Clinton's directive, the government had the ability to re-enable Selective Availability at any point; however, the Department of Defense announced in 2007 that it would no longer procure satellites with the ability to degrade the civilian ranging signal.¹⁷⁴

-

¹⁶⁸ Frequently Asked Questions About Selective Availability, NATIONAL EXECUTIVE COMMITTEE FOR SPACE-BASED POSITION, NAVIGATION, AND TIMING, http://www.gps.gov/systems/gps/modernization/sa/faq/ (last visited Apr. 19, 2011). ¹⁶⁹ Id.

¹⁷⁰ Sturdevant, *supra* note 160 ("To withhold full accuracy from enemies but provide GPS service to civilian users, the USAF designed the system with a protective feature called 'selective availability' (SA) that, when used, gave the U.S. military and its allies significantly more precise satellite signals than what other users received."); *See generally* Parkinson, *supra* note 150 at 12, 24 (arguing against the use of Selective Availability to combat civilian adjustments).

¹⁷¹ Parkinson, *supra* note 150, at 12

¹⁷² See Ditlea, supra note 164, at 121.

¹⁷³ Press release, The White House, Statement by the President Regarding the United States' Decision to Stop Degrading Global Positioning System Accuracy (May 1, 2000), *available at* http://gpshome.ssc.nasa.gov/content.aspx?s=press (citing as an example that "emergency teams responding to a cry for help can now determine what side of the highway they must respond to, thereby saving precious minutes").

¹⁷⁴ Press release, Department of Defense, DoD Permanently Discontinues Procurement of Global Positioning System Selective Availability (September 18, 2007), *available at* http://www.defense.gov/releases/release.aspx?releaseid=11335 (this announcement "coincide[d] with the U.S. Air Force's solicitation to purchase the next generation of GPS satellites known as GPS III").

475

2011] WHERE WE ARE WITH LOCATION TRACKING

Even without Selective Availability, GPS is not 100 percent accurate because of clock errors, atmosphere delay or receiver measurement errors.¹⁷⁵ In its report for the last quarter of 2010, the Federal Aviation Administration announced that ninety-five percent of the time the civilian signal was accurate to within a little more than two meters horizontally and a little more than five meters vertically.¹⁷⁶

People who make receivers can minimize this error in a number of ways. Differential GPS (DGPS), one widely-used method, utilizes high-quality receivers at known locations that send correction information to other receivers in the area. ¹⁷⁷ Because the error due to atmospheric conditions should be similar for two receivers relatively close to each other, a receiver can use this correction data from the higher-quality receiver to minimize its own error. ¹⁷⁸

The range for the most basic form of DGPS is 150 km,¹⁷⁹ but the U.S. government has developed a number of differential systems on a much larger scale.¹⁸⁰ Most notable is the Wide Area Augmentation System (WAAS), which consists of 38 ground stations throughout North America, all of which make corrections and send the information to GPS receivers on a GPS-like frequency.¹⁸¹ Though it was created primarily to

¹⁷⁶ GPS PRODUCT TEAM, FEDERAL AVIATION ADMINISTRATION, REPORT NO. 72, GLOBAL POSITIONING SYSTEM (GPS) STANDARD POSITIONING SERVICE (SPS) PERFORMANCE ANALYSIS REPORT, (Jan. 31, 2011), available at http://www.nstb.tc.faa.gov/REPORTS/PAN72_0111.pdf. For the most recent quarterly report and an archive of past quarterly reports, see Archived PAN Reports, FAA, http://www.nstb.tc.faa.gov/DisplayArchive.htm. The latest Performance Standard, published by the Department of Defense in 2008, had a goal of keeping the error rate under 7.8m ninety-five percent of the time. POSITION, NAVIGATION, AND TIMING

-

¹⁷⁵ Parkinson, *supra* note 150, at 17.

EXECUTIVE COMMITTEE, *supra* note 163.

177 See Bradford W. Parkinson & Per K. Enge, Differential GPS, in, 2 GLOBAL POSITIONING SYSTEM: THEORY AND APPLICATIONS 3, 3 (Bradford W. Parkinson & James J. Spilker, Jr. eds., Progress in Astronautics and Aeronautics Ser. No. 164, 1996).

178 Id.; Spilker & Parkinson, *supra* note 152, at 47.

¹⁷⁹ Parkinson & Enge, supra note 174.

¹⁸⁰ For a description of each of these systems, see *Augmentation Systems*, GPS.GOV, http://www.gps.gov/systems/augmentations/ (last visited Oct. 25, 2011).

¹⁸¹ TECHNICAL OPERATIONS, NAVIGATION SERVICES, FAA, GLOBAL POSITIONING SYSTEM WIDE AREA AUGMENTATION SYSTEM (WAAS) PERFORMANCE STANDARD 10 (2008), *available at* http://www.gps.gov/technical/ps/2008-WAAS-performance-standard.pdf. WAAS is not the only DGPS system implemented by the U.S. government. Another example of government-run DGPS is the Coast Guard Maritime

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

assist with flying, WAAS can augment any GPS device in its coverage area, resulting in one- to two-meter accuracy ninety-five percent of the time. Private companies have also created DGPS systems at various times. For example, in 1995 (before the elimination of Selective Availability), Differential Correction Inc. boasted of providing accuracy of one to ten meters, depending on the fees paid by subscribers. 183

GPS is not the only satellite navigation system in use. The Russian Global Navigation Satellite System (GLONASS) has been around nearly as long as the U.S.-operated GPS system, though it fell into disrepair in the 1990s and only recently became fully functional again. ¹⁸⁴ Europe and China are also each currently building separate satellite navigation systems. ¹⁸⁵ GPS is by far the most widely used satellite system, but in May 2011, Qualcomm announced that it would be releasing a new phone with a chipset that uses signals from both GPS and GLONASS. ¹⁸⁶ Because using both satellite systems will make the tracking devices more consistent and accurate by giving them access to more satellites, more companies will almost certainly follow Qualcomm's lead. ¹⁸⁷

Differential GPS Service, which became operational in 1999 and consists of 80 remote broadcast sites, providing 10-meter accuracy for the coasts, the Mississippi River basin, and portions of Alaska and Hawaii. *DGPS General Information*, U.S. COAST GUARD NAVIGATION CENTER, http://www.navcen.uscg.gov/?pageName=dgpsMain (last visited Oct. 25, 2011).

¹⁸² GNSS Frequently Asked Questions—GPS, supra note 160.

¹⁸³ Ditlea, *supra* note 164 at 121.

¹⁸⁴ Andrew E. Kramer, *Russia Challenges the U.S. Monopoly on Satellite Navigation*, N.Y. TIMES (Apr. 4, 2007),

http://www.nytimes.com/2007/04/04/business/worldbusiness/04gps.html. 185 $\emph{Id.}$

¹⁸⁶ Richard Wilson, *Qualcomm Adds GLONASS Positioning to Smartphones*, ELECTRONICSWEEKLY.COM (May 30, 2011),

http://www.electronicsweekly.com/Articles/2011/05/30/51150/qualcomm-add-glonass-positoning-to-smartphones.htm.

¹⁸⁷ *Id.* (quoting the vice president for project management for Qualcomm as saying, "[s]upporting both positioning technologies gives users of ZTE's latest smartphone the benefit of up to 55 different satellites when calculating their global position for navigation or any location-based application" and quoting the chief commercial officer of the cell phone manufacturer as saying, "[a]ccording to our estimates, the market of GLONASS-enabled devices will grow at high rates").

477

2011] WHERE WE ARE WITH LOCATION TRACKING

C. Cell-Site Tracking Devices

In 1996, amidst the backdrop of growing cell-phone usage, the Federal Communications Commission (FCC) began requiring cell phone companies to turn over data to 911 operators to improve emergency response. Phase I of the program, which was dubbed Enhanced 911 or E911, required the companies to turn over the phone number of the caller and the location of the cell site receiving the call. Phase II required the companies to provide longitude and latitude to a certain degree of accuracy. Cell-site information is required by the FCC to be accurate within fifty to 300 meters, depending on the technology used. Phone companies can implement this program either through cell tower triangulation or by a GPS device embedded in the phone. In 2000, the FCC modified the program to require ninety-five percent of each provider's cell phones to be compliant.

A number of the large cell phone companies missed this deadline and were fined by the FCC.¹⁹⁴ Yet this policy resulted in a large number of carriers putting GPS chips in their cell phones. Sprint-Nextel, for example, introduced more than forty new GPS-enabled handset models and distributed more than sixty million GPS-enabled handset devices by

¹⁸⁸ GAO, No. GAO-04-55, Uneven Implementation of Wireless Enhanced 911 Raises Prospect of Piecemeal Availability for Years to Come 7-8 (2003), *available at* http://www.gao.gov/new.items/d0455.pdf. ¹⁸⁹ *Id.*

_

 ¹⁹⁰ Id. See also Laurie Thomas Lee, Can Police Track Your Wireless Calls? Call Location Information and Privacy Law, 21 CARDOZO ARTS & ENT. L.J. 381, 384 (2003).
 ¹⁹¹ FCC Consumer Facts, FCC,

http://www.fcc.gov/cgb/consumerfacts/wireless911srvc.html (last visited Apr. 22, 2011). The exact requirements can be found in 47 C.F.R. § 20.18(h)(2) (2011) (requiring, for example, accuracy within 50 meters for 67 percent of calls and within 150 meters for 80 percent of the calls for handset based technologies but allowing a carrier to exclude 15 percent of counties from the 150 meter requirement due to heavy forestation).

¹⁹² See Darren Handler, Note, An Island of Chaos Surrounded by a Sea of Confusion: The E911 Wireless Device Location Initiative, 10 VA. J.L. & TECH. 1 (2005).

¹⁹³ GAO, *supra* note 185 (noting also that "[t]he most common handset solution also relies on triangulation, but uses Global Positioning System (GPS) satellites and a GPS chip inside the handset").

¹⁹⁴ Sprint, Alltel, USC Fined for Missed e911 Deadline, FIERCE WIRELESS (Aug. 31, 2007), http://www.fiercewireless.com/story/sprint-alltel-usc-fined-missed-e911-deadline/2007-08-31.

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

the end of 2005.¹⁹⁵ The last handset model Sprint-Nextel produced without a GPS capability was sold in February 2004.¹⁹⁶

Despite the inclusion of GPS in all current cell phones,¹⁹⁷ most cell phone companies also use cell-site data to track the location of their phones.¹⁹⁸ Cell-site data is a collection of a number of pieces of data "regarding the strength, angle, and timing of the caller's signal measured at two or more cell sites, as well as other system information such as a listing of all cell towers in the market area, switching technology, protocols, and network architecture."¹⁹⁹ The person who receives this data is able to pinpoint the location of the phone using a process similar to that used by a satellite-based tracking device.²⁰⁰ As the Southern District of Texas explained in 2005, "[w]hen a cell phone is powered up, it acts as a scanning radio, searching through a list of control channels for the strongest signal. The cell phone re-scans every seven seconds or when the signal strength weakens, regardless of whether a call is placed."²⁰¹

When cell phones first started becoming popular, towers served customers for miles, so the data was not particularly accurate. But there are now three times as many base stations as there were a decade ago, and

¹⁹⁵ Sprint Nextel Corporation E911 Deployment Status Report at 6, Revision of the Commission's Rules to Ensure Compatibility with Enhanced 911 Emergency Calling Systems, No. 90-102 (FCC, August 1, 2006), *available at* http://fjallfoss.fcc.gov/ecfs/document/view?id=6518415684.

-

¹⁹⁷ The last cell phone that Sprint manufactured that did not include a NAVSTAR GPS chip was discontinued in 2004. *Id.*

¹⁹⁸ EPCA Reform and the Revolution in Location Based Technologies and Services: Hearing Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on the Judiciary, 111th Cong. 12 (2010) (testimony of Matt Blaze, Associate Professor, University of Pennsylvania) [hereinafter Blaze testimony], available at http://www.judiciary.house.gov/hearings/printers/111th/111-109_57082.PDF ("GPS is actually not used by the cellular telephone network for tracking at all. And law enforcement use of GPS for surreptitious surveillance with cell phones is less important than other kinds of telephone-based tracking when we are talking in the context of wireless communication.").

¹⁹⁹ In re Pen Register, 396 F. Supp. 2d 747, 749 (S.D. Tex. 2005).

²⁰⁰ *Id.* (quoting the investigator's application in this case as saying the information "may provide the general geographic location of the Target Device and, thus, may allow investigators to identify a suspect's location").

²⁰¹ *Id.* at 750. The opinion cites to a detailed background discussion on how cell phones operate. *See* Tom Farley & Mark van der Hoek, *Cellular Telephone Basics*, PRIVATELINE (Jan. 1, 2006), http://www.privateline.com/mt_cellbasics/index.html.

479

2011 WHERE WE ARE WITH LOCATION TRACKING

in urban areas, cell towers are designed to serve specific buildings or even specific floors of buildings, making the information extremely accurate. Other advances in technology have allowed cell phone companies to locate the "angle of arrival," which reveals the phone's location within the sector, further improving its accuracy. These calculations can be made not just when a person is making a phone call but whenever the phone is turned on, depending on the company's policy. Apple's Software License Agreement, for example, explicitly allows the company to "transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone."

The ability to locate the device indoors, along with the fact that people often carry their phones with them at all times, makes cell phones advantageous to standalone satellite-based tracking devices in many respects. One potential flaw, however, is that, particularly in the morning and evening rush periods, calls can be redirected to other towers, which may make the readings inaccurate. One

²⁰² Blaze testimony, supra note 195, at 15-16.

²⁰⁵ APPLE, INC., IPHONE SOFTWARE LICENSE AGREEMENT § 4(b) (update rev. May 8, 2009), *available at* http://images.apple.com/legal/sla/docs/iphone.pdf. Apple was criticized by privacy advocacy groups in April 2011, when it was revealed that the iPhone not only recorded this information but also stored the data on the phone. *See* Charles Arthur, *iPhone Keeps Record of Everywhere You Go*, GUARDIAN (Apr. 20, 2011), http://www.guardian.co.uk/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears.

²⁰³ *Id.* at 94-95.

²⁰⁴ *Id*.

²⁰⁶ Blaze testimony, supra note 195, at 30 ("As the precision provided by cellular network-based location approaches that of GPS-based tracking technology, cellular location tracking can have significant advantages for law enforcement surveillance operations compared with traditional GPS trackers. New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cell phone location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the subject. And the 'tracking device' is now a benign object already carried by the target—his or her own telephone.").

²⁰⁷ See Anemona Hartocollis, When the Trill of a Cellphone Brings the Clang of Prison Doors, N.Y. TIMES (July 16, 2007), available at

http://www.nytimes.com/2007/07/16/nyregion/16cell.html ("[U]se [of cell-site data] in prosecutions is often challenged, for privacy reasons and for technical reasons, especially when the data comes during the morning or evening rush, when circuits are crowded

Herbert (442-503) Fall 2011

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

Cell phone companies have long had the ability to track the location of phones, and that information was used in criminal cases as far back as 1998.²⁰⁸ But beginning in 2005, courts began to see an increase in cases about cell-site data as government investigators began requesting it in orders compelling phone companies to disclose records.²⁰⁹ Courts are divided on whether to allow the government access to this information through previously enacted statutes.²¹⁰

In a 2010 case, the Third Circuit, relying on *Knotts* and *Karo*²¹¹ for the proposition that "the privacy interests at issue are confined to the interior of the home," held that the government can obtain cell-site location information under 18 U.S.C. § 2703(d), which does not require probable cause but rather "specific articulable facts showing there are

and calls can be redirected to other towers. But it is often allowed and is used by both prosecutors and defense attorneys to buttress their cases.")

²⁰⁸ Peter Wayner, *Technology That Tracks Cell Phones Draws Fire*, N.Y. TIMES (Feb. 23, 1998), *available at* http://www.nytimes.com/1998/02/23/business/technology-that-tracks-cell-phones-draws-fire.html ("A London prosecutor, Victor Temple, said that he had used data from cell phone records to convict a drug dealer of murder last year. The records showed calls converging at the scene of the murder, which helped to persuade a jury that the man's alibi was false.").

²⁰⁹ *In re* U.S. for Historical Cell Site Data, 747 F. Supp. 2d 827, 829 & n. 4 (S.D. Tex. 2010) (citing *In re* U.S. for an Order Authorizing Use of a Pen Register, 384 F. Supp. 2d 562 (E.D.N.Y. 2005), *on reconsideration*, 396 F. Supp. 2d 294 (E.D.N.Y. 2005); *In re* Pen Register, 396 F. Supp. 2d 747 (S.D. Tex. 2005); *In re* U.S. for an Order Authorizing Installation and Use of a Pen Register, 402 F. Supp. 2d 597 (D. Md. 2005); *In re* U.S. for an Order Authorizing Release of Prospective Cell Site Info., 407 F. Supp. 2d 132 (D.D.C. 2005); *In re* U.S. for an Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d 435 (S.D.N.Y. 2005)).

²¹⁰ Compare In re U.S. for an Order Authorizing the Disclosure of Prospective Cell Site Info., 412 F. Supp. 2d 947, 958 (E.D. Wis. 2006) ("If Congress intended to allow prospective cell site information to be obtained by means of the combined authority of the SCA and the Pen/Trap Statute, such intent is not at all apparent from the statutes themselves. Indeed . . . the legislative history of CALEA would suggest Congress's intent to be otherwise."), with In re U.S. for an Order for Disclosure of Telecomm. Records, 405 F. Supp. 2d at 445 ("[C]ell site or tracking information constitutes 'information' pertaining to customers or users of electronic communications services. Thus, such cell-site or tracking information comes within [18 U.S.C.] section 2703(c) and consequently is the sort of 'information' that the Government may seek pursuant to an order under section 2703(d).").

²¹¹ United States v. Karo, 468 U.S. 705 (1984) (holding, just two years after *Knotts*, that the tracking of a beeper while it was inside of a private residence did violate the Fourth Amendment).

a

2011 Where We Are with Location Tracking

reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."212

D. Infrared Tracking Devices

A fourth kind of location-tracking device is what has been described as an infrared beeper. Infrared beepers are not the subject of much litigation, 213 but they are, according to one court, "a valuable and well-accepted law enforcement tool."214 According to Investigator Hagenah, infrared tracking devices are placed on a suspect's bumper and give off a periodic signal, like an RF-enabled beeper.²¹⁵ But instead of emitting a noise, infrared tracking devices send out an infrared beam of light every couple of seconds.²¹⁶ Hagenah said the device was used regularly by the Minnesota Bureau of Criminal Apprehension and allowed officers to follow a car from a distance at night by using infrared goggles.²¹⁷ However, there is very little information about these devices.218

III. DEVICES IN USE

In Part I, this paper noted that, without the warrant requirement and without a probing inquiry by the courts, it is difficult to know what technology is in use and whether location tracking has become "dragnettype." The difficulty of obtaining information from either law enforcement or manufacturers of location-tracking devices adds to this

²¹² In re U.S. for an Order Directing a Provider of Elec. Commc'n Service to Disclose Records to the Gov't, 620 F.3d 304, 312-13 (3d Cir. 2010) (quoting 18 U.S.C. § 2703(d) (2011)).

²¹³ I found only one case that mentioned infrared tracking: *In re* U.S. for an Order Authorizing the Installation, Monitoring Maintaining, Repairing & Removing of Elec. Transmitting Devices, 155 F.R.D. 401 (D. Mass. 1994).

²¹⁴ *Id.* at 402.

²¹⁵ Interview with Stephen Hagenah, *supra* note 134.

²¹⁶ *Id*.

²¹⁷ *Id*.

²¹⁸ I found a website that references the "Firefly" infrared tracker produced by Power Plus Inc., IR Beacons, PRC68.COM http://www.prc68.com/I/IR_Beacon.shtml (last visited Oct. 28, 2011). But see In re U.S. for an Order Authorizing the Installation, Monitoring Maintaining, Repairing & Removing of Elec. Transmitting Devices, 155 F.R.D. at 402.

Herbert (442-503) Fall 2011

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

problem.²¹⁹ However, it is possible to get some sense of the products purchased and used by law enforcement through cases, newspapers and government contracts. The rest of this section details those devices.

One popular product is the Tracking Key manufactured by LandAirSea. The Tracking Key is a passive²²⁰ battery-powered satellite-based tracking device.²²¹ Procurement contracts indicate that the DEA paid LAS Systems Inc. \$13,958 for "GPS Tracking Key[s]" in 2009 and \$17,965 for "Tracking Key GPS Logger[s]" in 2010.²²² The two devices in the Tracking Key product line each cost less than \$300 per unit.²²³ LandAirSea has sold more than 250,000 passive receivers in the Tracking Key series.²²⁴ The New York Office of the State Inspector General

²²⁰ A passive tracking device is not equipped with a transmitter. It simply records its location and stores that information until the investigator physically retrieves the device from the car and downloads the data that has been stored. *See Passive GPS Tracking*, LANDAIRSEA, http://www.landairsea.com/about/gps-tracking-passive.html (last visited Oct. 21, 2011). This is in contrast to an "active" tracking device, which can transmit the data directly to the investigator at any point. *See Real-Time GPS Tracking*, LANDAIRSEA, http://www.landairsea.com/about/gps-tracking-real-time.html (last visited Oct. 21, 2011). For a more in-depth discussion of this distinction, *see infra* notes 291-96 and accompanying text. *See also* Anita Hamilton, *Why You Can't Track Your Stolen GPS*, TIME (Apr. 28, 2008),

http://www.time.com/time/business/article/0,8599,1735091,00.html? ("Car navigation devices keep you from getting lost, but their location-sensing acumen won't help you find them if they get lost or stolen. Why not? Because location and tracking are two different matters. 'The GPS calculates location for you. Communicating that location to a tracking center requires a separate service,' says Kanwar Chadha, founder and vice president of SiRF Technology, the largest supplier of GPS chips to navigation device makers.").

²¹⁹ See supra notes 89-97 and accompanying text.

²²¹ GPS Tracking Key Specifications, LANDAIRSEA, http://www.landairsea.com/gps-tracking-systems/gps-tracking-key-specifications.html (last visited Oct. 25, 2011).

²²² Purchase Order for Drug Enforcement Administration, Procurement ID No. DJD09STP0102 (Aug. 6, 2009) (.pdf on file with author), available at https://www.fpds.gov/ (search for Procurement ID No.); Purchase order for Drug Enforcement Administration, Procurement ID No. DJD10STP0129, (Aug. 12, 2010) (.pdf on file with author), available at https://www.fpds.gov/ (search for Procurement ID No.).

²²³ GPS Tracking Key Specifications, supra note 218; GPS Tracking Key Pro Specifications, LANDAIRSEA, http://www.landairsea.com/gps-tracking-systems/gps-tracking-specifications.html (last visited Oct. 25, 2011).

²²⁴ Interview with Steve Moehling, Vice President, LandAirSea (Apr. 5, 2011) (transcript of file with author). By comparison, LandAirSea, sold approximately a few

2011 Where We Are with Location Tracking

(OSIG) also uses the device.²²⁵ In a 2008 investigation of a New York State Department of Labor employee, the OSIG placed a Tracking Key on the employee's car.²²⁶ Additionally, though he did not mention what device was actually used in the investigation, Judge Posner in Garcia referred to the use of a "memory tracking unit" by investigators and included a link to the LandAirSea Tracking Key.²²⁷ LandAirSea also recently released an active device that can either be battery-powered or hard-wired.²²⁸

Another popular producer of tracking devices is Coleman Technologies, Inc., from whom the DEA purchased more than \$15,000 in GPS-related equipment in 2010.²²⁹ Coleman has a number of tracking-related products. The company's "All-in-one" series includes a General Packet Radio Services (GPRS) device, a "mini-logger," and an "RF logger." 230 Access to descriptions of these devices, however, is restricted.²³¹ The "Digital" series includes products called "Digital 1xRTT," "Digital CDMA," "Digital GPRS" and "Digital RF Log Agent," but access to this product line is also restricted. 232 Coleman has a line of receivers called "SV12," which the website describes as "an

hundred of their SilverCloud units in the first quarter of 2011. Id. However, SilverCloud is a new product, so a comparison of its sales to the popular Tracking Key series may not be as helpful.

²²⁵ Testimony of James Carroll at 264, Cunningham v. N.Y. State Dep't of Labor, 933 N.Y.S.2d 432 (N.Y. App. Div. 2011) (No. 512036).

²²⁷ See United States v. Garcia, 474 F.3d 994, 995 (7th Cir. 2007).

²²⁸ See SilverCloud Real-Time GPS Tracking System, LANDAIRSEA, http://www.landairsea.com/gps-tracking-systems/gps-tracking-silvercloud.html (last visited Oct. 25, 2011).

²²⁹ Purchase Order for Drug Enforcement Administration, Procurement ID No. DJD10HOP0258 (Aug. 18, 2010) (.pdf on file with author), available at https://www.fpds.gov/ (search for Procurement ID No.); Purchase Order for Drug Enforcement Administration, Procurement ID No. DJD10LAP0156 (Aug. 18, 2010) (.pdf on file with author), available at https://www.fpds.gov/ (search for Procurement ID No.).

²³⁰ Category Listing—Agent Advanced Generation Tracker, COLEMAN TECHNOLOGIES, https://estore.ctiusa.com/index.php?cPath=22_23 (last visited Oct. 25, 2011).

²³¹ *Product Listing*, COLEMAN TECHNOLOGIES,

https://estore.ctiusa.com/index.php?cPath=22_23_27_28 (last visited Oct. 25, 2011). ²³² *Id*.

484 BERKELEY JOURNAL OF CRIMINAL LAW

Vol. 16:2

upgrade for the Trimble SVee Eight Plus receiver module."233 These receivers appear to be passive tracking devices, but Coleman says a user can attach a radio modem or wireless connection, which indicates that they might also be capable of transmitting information.²³⁴

Testifying at the Maynard trial, Supervisor Special Agent Solomon Bitsie, who oversees the tracking technology used by the FBI, said the FBI buys products made by others and also develops products itself.²³⁵ According to Bitsie, the device used in the *Maynard* trial was an FBI-made product called CGB-1.²³⁶ It was an active satellite-based device, and it was battery-powered.²³⁷ Bitsie did not state how many similar devices the FBI had, but he said that he had used or supervised the use of GPS devices in more than 300 investigations since 1996.²³⁸

In his complaint against the FBI, Afifi alleged that the device on his car was a Guardian ST820 produced by Cobham.²³⁹ The device appeared to be similar to the one used on the car of the animal rights activist.²⁴⁰ The device she found was an active satellite-based tracking device and was battery-powered.²⁴¹ In Weaver, Investigator Minahan said the New York State Police owned an active Orion brand device in addition to the passive Q-ball that was actually used in the investigation of Weaver,²⁴² but no information about this product was available. In response to a picture of the device placed on Afifi's car, an anonymous

²³³ Commercial Vehicle Tracking, COLEMAN TECHNOLOGIES, http://ctiusa.com/electronic_systems/commerical_vehicle.php (last visited Oct. 25, 2011).

²³⁴ *Id.*

²³⁵ Testimony of Solomon Bitsie, *supra* note 124, at 15. Bitsie also said the FBI has three different types of devices that go on a car, but he was not asked to elaborate. *Id.* ²³⁶ Id.

²³⁷ Testimony of David Kirschner at 36, United States v. Jones, 451 F. Supp. 2d 71 (D.D.C. 2006) (No. 05-0386) (explaining that it then took the investigators five days to replace the batteries), overruled by sub nom. United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010), cert. granted sub nom. United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

²³⁸ Testimony of Solomon Bitsie, *supra* note 124, at 27.

²³⁹ Complaint, *supra* note 85, at 5. For a more in-depth discussion of the Afifi incident, see supra notes 84-85 and accompanying text.

²⁴⁰ Zetter, *supra* note 86. For more on the animal rights incident, see *supra* notes 86-87 and accompanying text.

²⁴¹ Tracking Device Teardown, supra note 86.

²⁴² Testimony of Peter Minahan, *supra* note 59, at 403.

485

2011 WHERE WE ARE WITH LOCATION TRACKING

commenter said Orion products are also sold by Cobham.²⁴³ However, no one from Cobham Tracking was able to answer questions about the company's tracking equipment, so it is unclear whether the company produces Guardian devices, Orion devices, or both.²⁴⁴

In 2007, the DEA paid GPSit \$37,725 for what is described as "GPS Tracking Devices." On its website, GPSit boasts that its customers include the Department of Justice (DEA, FBI, and ATF), the Department of Homeland Security, the Department of Defense, the Internal Revenue Service and "hundreds of state, county and city crime-fighting agencies." The FS1, produced by GPSit, is an active battery-powered satellite-based device, but it also uses cell-site data for improved accuracy. It is described on the company website as "the world's first and smallest fully integrated battery-powered GPS tracker using Qualcomm's patented CDMA gpsOneTM technology." gpsOne is an assisted-GPS technology that uses cell-site data to enhance the accuracy of a GPS device, particularly indoors. GPSit appears to have other products designed particularly for law enforcement, but access to those products is restricted to members of the Department of Homeland

²⁴³ Zetter, *supra* note 95 (stating that a commenter said the device placed on Afifi's car was an Orion device produced by Cobham).

_

²⁴⁴ I called Cobham multiple times but was told that no one was able to talk to me about their products. Telephone Interview with Monica Hallman, *supra* note 96; *see also supra* text accompanying note 96. A company called Orion makes GPS devices, but the devices appear to be geared toward seismic monitoring and surveying, not vehicular tracking. *See Why GPS?*, ORION MONITORING SYSTEMS,

http://www.orionmonitoring.com/technology.htm (last visited Oct. 25, 2011) ("Over the past decade, continuous GPS has been used to measure crustal deformation rates and tectonic plate velocities to better than 1 mm/yr."). I could not find the device that fits the description of the device placed on Afifi's car.

²⁴⁵ Purchase order for Drug Enforcement Administration, Procurement ID No. DJDEAHQ070303O (Sept. 24, 2007) (.pdf on file with author), *available at* https://www.fpds.gov/ (search for Procurement ID No.).

²⁴⁶ Covert Surveillance Solutions for Law Enforcement, GPSIT,

http://www.gpsit.com/en/covertsurveillance.html (last visited Oct. 25, 2011).

²⁴⁷ FS1 Battery Powered Covert GPS Tracker, GPSIT,

http://www.gpsit.com/en/gpstrackers.html?phpMyAdmin=1f2e09a0fb9200d6e3ef8410 659a78f3 (last visited Oct. 25, 2011) (emphasis omitted).

²⁴⁹ Guardian Mobile Changes Name, Intros Indoor-Locatable Beacon, GPS WORLD (Sept. 5, 2007), http://www.gpsworld.com/transportation/news/guardian-mobile-changes-name-intros-indoor-locatable-beacon-6672.

[Vol. 16:2

Security, Department of Defense, Department of Justice, and "[s]tate, county and city crime-fighting agencies." ²⁵⁰

In 2007, LEA re-launched the Birddog, the RF-enabled beeper used in *Knotts*—this time as "an all-new tracking device based on advanced GPS technology."²⁵¹ Between January and August of that year, LEA sold 90 Birddog tracking systems that LEA said had a combined value of \$625,000.²⁵² In September 2008, four federal agencies ordered a total of 15 Birddog tracking systems.²⁵³ LEA also produces a Bloodhound GPS tracking device,²⁵⁴ but that device is not available on the public portion of the LEA website.²⁵⁵ LEA reduced the price of the Bloodhound to \$3,995 in 2002,²⁵⁶ but there is no description of the product's current price or specifications. In 2009, LEA had net sales of \$11.9 million, including a \$5.9 million order from a large government agency.²⁵⁷ The percentage of sales attributable to the Birddog tracking devices is unknown. LEA, which sells electronic surveillance equipment other than tracking devices, only displays a limited selection of its products on its

²⁵⁰ Portal Introduction, GPSIT, http://www.gpsit.com/en/portal-overview.html?phpMyAdmin=1f2e09a0fb9200d6e3ef8410659a78f3 (last visited October 21, 2011) ("GPSit has developed a secure information portal for law enforcement. Within this portal, GPSit provides its law enforcement members with law enforcement [sic] only product information and guidance on successful covert tracking operations.").

²⁵¹ Law Enforcement Associates Receives Orders for 15 BirddogTM GPS Surveillance Systems from Four Federal Agencies, supra note 146.

²⁵² Law Enforcement Associates Launches Multi-City Training Series for New Birddog GPS Tracking Product, MARKETWIRE, (Aug. 29, 2007) http://www.marketwire.com/press-release/Law-Enforcement-Associates-Launches-Multi-City-Training-Series-New-Birddog-GPS-Tracking-764999.htm.

²⁵³ Law Enforcement Associates Receives Orders for 15 BirddogTM GPS Surveillance Systems from Four Federal Agencies, supra note 146.

²⁵⁴ See Law Enforcement Associates Reports Fiscal 2010 Results, Provides Operational Update, MARKETWIRE (Mar. 31, 2011), http://www.marketwire.com/press-release/Law-Enforcement-Associates-Reports-Fiscal-2010-Results-Provides-Operational-Update-1420928.htm ("Its products include the Under Vehicle Inspection System (UVIS), EDK123 (Explosive Detection Kit), Bloodhound and Birddog GPS Tracking Systems .")

²⁵⁵ See generally GPS Tracking, supra note 97.

²⁵⁶ LEA Introduces Undercover Digital Recorder, Lowers Price on BLOODHOUND GPS, Gets Contract from State of Texas, BUSINESS WIRE (Mar. 20, 2002), http://findarticles.com/p/articles/mi_m0EIN/is_2002_March_20/ai_84025029/.

²⁵⁷ Law Enforcement Associates Reports Fiscal 2010 Results, supra note 250.

487

2011 WHERE WE ARE WITH LOCATION TRACKING

generally accessible website. A password, issued only to law enforcement officers, is required to view most of their products.²⁵⁸

Another major producer of satellite-enabled tracking devices is iSECUREtrac, which sold both active and passive location-tracking devices to government agencies in 2004.259 The Central District of California, for example, which had 2,000 people awaiting federal pre-trial in 2004, paid \$4.50 per day for each of its 120 passive tracking devices and \$10 per day for each of its 20 active trackers.²⁶⁰ iSECUREtrac markets location-tracking devices to prisons and jails, which use them to keep track of suspects who are awaiting trial.²⁶¹ The company makes both an active and a passive product, both of which are battery-powered because they are designed for use on people, not cars.²⁶² iSECUREtrac also makes a hybrid device, which acts as a passive tracker unless the user commits a violation by going either outside of the inclusion zone or into an exclusion zone. After a violation, the hybrid device can switch to realtime reporting.²⁶³ Though it is difficult to know how widespread this practice is outside of California, a 2008 article by Professor Erin Murphy noted that at least 17 states had statutes authorizing some form of electronic location tracking for sexual offenders and others had "pursued implementation of such programs through either legislative enactments or executive orders."264

²⁶² iSECUREtrac Active GPS, ISECURETRAC.COM,

http://www.isecuretrac.com/GetImage.aspx?d=56 (last visited Apr. 22, 2011) (e-mail address required); *iSECUREtrac Passive GPS*, ISECURETRAC.COM,

http://www.isecuretrac.com/Library.aspx?id=57 (last visited Apr. 22, 2011) (e-mail address required).

__

²⁵⁸ See GPS Tracking, supra note 97.

²⁵⁹ Marty Whitford, *Long Arm of the Law*, GPS WORLD (Aug. 1, 2004), *available at* http://www.gpsworld.com/lbs/personal-tracking/long-arm-law-880.

²⁶⁰ *Id*.

²⁶¹ *Id.*

²⁶³ GPS: Hybrid GPS Sytems, ISECURETRAC,

http://www.isecuretrac.com/Services.aspx?p=GPS#hybrid (last visited Oct. 25, 2011). ²⁶⁴ Erin Murphy, *Paradigms of Restraint*, 57 DUKE L. J. 1321, 1333 (2008). *See also Bill Aims to Allow Use of GPS*, HERALD-TRIBUNE (Sarasota, Flor.) (Feb. 13, 2004), *available at* http://www.heraldtribune.com/article/20040213/NEWS/402130385 ("Florida has been one of the most aggressive states in using satellite technology to track criminals. The Department of Corrections uses 'active' GPS for about 400 probationers, mostly sex offenders and people who've committed violent crimes. About another 150 are monitored with 'passive' GPS which checks offenders [sic] whereabouts less often.").

BERKELEY JOURNAL OF CRIMINAL LAW

Vol. 16:2

Finally, millions of people carry tracking devices with them at all times in the form of their cell phones. Cell phones use both cell-site data and satellite-based technology to record the location of the phone.²⁶⁵ There do not appear to be location-tracking devices other than cell phones that use only cell-site tracking technology, but a number of satellite-based tracking devices use cell-site information to improve accuracy.266

The following is a table that summarizes the devices discussed above and categorizes them as active or passive and battery-powered or hard-wired. All of the devices in this table are satellite-enabled tracking devices, although the GPSit device uses cell-site data as a supplement.

Product Name	Government Use	Active or Passive	Battery- Powered or Hard-Wired
LandAirSea Tracking Key	DEA purchased nearly \$32,000 worth of devices in 2009 and 2010.	Passive	Battery-powered
Coleman	DEA purchased more than \$15,000 of Coleman tracking technology in 2010.	Unknown	Unknown
Cobham	Perhaps placed on the car of Yasir Afifi by the FBI.	Active	Battery-powered
GPSit	DEA purchased more than \$37,000 of GPSit equipment in 2007.	Active	Battery-powered
LEA Birddog	LEA sold \$625,000 worth of Birddog tracking systems in 2007 and sold to four federal agencies.	Active	Either
iSECUREtrac	The central district of California paid for 120 passive tracking devices and 20 active trackers in 2004.	Either	Battery-powered
FBI-made device	Made by the FBI for FBI use.	Active	Battery-powered

²⁶⁵ See supra notes 192-98 and accompanying text.

²⁶⁶ See, e.g., Testimony of Solomon Bitsie, supra note 124, at 13, 16 (stating that the FBI-brand location tracking devices uses two cell phone antennas to improve accuracy); FS1 Battery Powered Covert GPS Tracker, supra note 244. For a complete discussion of the FS1, see supra notes 242-46 and accompanying text.

2011 WHERE WE ARE WITH LOCATION TRACKING

489

IV. WHAT A TECHNOLOGY-SPECIFIC FOURTH AMENDMENT ANALYSIS OF LOCATION-TRACKING DEVICES MAY LOOK LIKE

The discussion in the previous parts of this paper illustrates not only that the location-tracking devices used today are substantively different than the devices that were in use the last time the Supreme Court considered this issue, but also that there is a great deal of diversity among the devices used today with regard to cost, data collection, data retrieval and power. The technology is changing so rapidly that the FBI supervisor in charge of tracking technology receives biennial updates on the new tracking technologies that are available.²⁶⁷

Courts and commentators, if they are not simply citing *Knotts* for the proposition that the use of tracking devices without a warrant is constitutional, often reach for the low-hanging fruit in their analysis by simply distinguishing the type of technology used in *Knotts* (RF-enabled beepers) from the type that is most prevalent today (satellite-based GPS tracking devices). 268 Although this distinction is important, a critical look at tracking devices reveals a number of other ways in which the devices differ, including what information is collected by the device, how that data is retrieved by law enforcement, and how long the device can operate. A cell-site tracking device, for example, may be more similar to an RF-enabled beeper in the way it collects information but more similar to a GPS device in the way it reveals that information to law enforcement officers.²⁶⁹ By taking analytical shortcuts and grouping all of these tracking devices into a single category, the courts appear to be missing key constitutional issues. The final section of this article looks at three aspects of tracking technology—level of police involvement, power supply and accuracy—that courts should consider in their constitutional analysis of current devices.

Level of Police Involvement

As tracking devices have evolved over the years, the level of police involvement needed in order to successfully track a suspect has decreased dramatically. This decrease is due primarily to a change in what information is collected. While some devices, due to technological

²⁶⁷ Testimony of Solomon Bitsie, *supra* note 124, at 8.

²⁶⁸ See supra notes 16-18, 22, 45 (citing articles, notes, and cases that take this approach).

²⁶⁹ See infra note 271-74 and accompanying text.

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

limitations, reveal their location in relation to a single mobile reference point, other devices use stationary reference points to create a more comprehensive picture. The fact that investigators can use stationary reference points to determine the location of a tracking device should change courts' constitutional analysis. This subsection first discusses that change, and then considers whether another evolution in tracking technology—the way the collected data is transmitted to the investigator—has any effect on the analysis.

1. What Information Is Collected

Satellite-based tracking devices collect a specific kind of information: the coordinates disclosing the exact location of the device on the globe at certain times.²⁷⁰ As explained in Part II, GPS devices use a number of satellites in the GPS system to triangulate the position of the device on land.²⁷¹ The devices combine the coordinates with the time to create a long list of where the device was, and when.²⁷² Cell-site tracking devices also use stationary reference points to determine the location of the device.²⁷³ Based on the cell phone tower that the device is pinging

²⁷⁰ See supra notes 147-84 and accompanying text (describing the development of GPS); see also Hutchins, supra note 16, at 414-21 (providing a layman's explanation on how the GPS system functions).

²⁷¹ See supra notes 147-84 and accompanying text. See also, Hutchins, supra note 414-21

²⁷² See, e.g., Ex. 25 at 10-15, Cunningham v. N.Y. State Dep't of Labor, 933 N.Y.S.2d 432 (N.Y. App. Div. 2011) (No. 512036) (listing the time, coordinates, and speed of the device at a number of different points each day). How thorough the data is depends on the tracking device used. LEA's Birddog, for example, records the location of the device every ten seconds. Bird Dog Hard Wired GPS – Tracking Unit, LEA CORP., http://www.leacorp.com/products.php?product=BIRD-DOG%C2%AE-Hard-Wired-GPS-%252d-Tracking-Unit%2C-Includes-1-Year-of-Service (last visited Apr. 22, 2011). The LandAirSea's TrackingKey, by contrast, records the location of the device once per second, but only when the device is moving. TRACKING KEY/TRACKING KEY PRO 2010 USER GUIDE, 13 (January 15, 2010), available at

http://www.landairsea.com/downloads/User%20Guide2.pdf. The detective in *Maynard* told the jury that if he were to print out all of the coordinates recorded by the FBI-created device used in that case, it would be thousands of pages. Testimony of David Kirschner, *supra* note 234, at 97.

²⁷³ See supra notes 185-209 and accompanying text (describing the data used for cell-site tracking).

2011 WHERE WE ARE WITH LOCATION TRACKING

and the "angle of arrival," cell-site tracking devices can determine the location of the device in relation to a nearby cell phone tower.²⁷⁴

This is in sharp contrast to RF-enabled "beepers," which are traditionally tracked using mobile receivers.²⁷⁵ Though the range of a beeper can be a couple miles on the open road, in the city that range is cut to less than a half mile,²⁷⁶ and according to Investigator Hagenah, when an investigator tried to follow the transmitter in the city, echoes often threw off the signal.²⁷⁷ In fact, because of these limitations, the investigators in *Knotts* lost the signal on multiple occasions.²⁷⁸

²⁷⁴ Blaze testimony, supra note 195, at 26.

²⁷⁸ United States v. Knotts, 662 F.2d 515, 516 (8th Cir. 1981) ("The agent following Petschen twice lost sight of Petschen's car, once purposely when Petschen, perhaps aware that he was being followed, began driving evasively. Shortly after this evasion the agent lost the beeper signal, and the drum's location was uncertain until the signal was again picked up and its source verified through the use of a helicopter."). The agents with the custom-made receiver lost the suspect early on, but Hagenah was able to follow the signal using his radio scanner. Interview with Stephen Hagenah, *supra* note 134. Hagenah lost the signal later in eastern Minnesota, picking it back up again thirty minutes later in Wisconsin. Transcript of Record, supra note 137, at 104. He lost the signal again in Wisconsin, and a helicopter with a radio receiver picked it up again about an hour later. Id. at 108-09. See also Joint Appendix, supra note 137, at *6 (transcribing testimony of Agent Hanley: "At times we lost communication for a period of time"). Losing contact seems to be a common occurrence in cases involving beepers. See, e.g., United States v. Bishop, 530 F.2d 1156, 1157 (5th Cir. 1976) ("Although at one point the signal was lost momentarily, the police were able to follow the signal out of the Shreveport city limits across the Red River into Bossier City, Louisiana. They continued to follow the signal in that city and were joined by other Shreveport police units that were following the tracking vehicle's route of travel by way of radio broadcasts."); United States v. Pretzinger, 542 F.2d 517, 519 (9th Cir. 1976) ("At 4:00 p.m. the same day, the Clark plane took off and flew to Mexico. A D.E.A. aircraft followed it but had to abandon surveillance because of darkness. The next morning the D.E.A. plane began again to search for the Clark plane. A buzzer signal was received and the Clark plane was located and followed. Another D.E.A. plane was also called in."). In United States v. Moore, the officers placed a beeper on the undercarriage of the U-Haul van used by the suspects and had another beeper in the box of chemicals the suspects had ordered. United States v. Moore, 562 F.2d 106, 108 (1st Cir. 1977). At least once, the officers lost sight of the van and lost the signals from both beepers, but they were able to spot the truck, exit the highway and catch up to the suspects a mile down the road. *Id.* (noting also that the officers relied on the beepers fifty percent of the time while tailing the suspects). In United States v. Martyniuk, the court said, "[the

²⁷⁵ Interview with Stephen Hagenah, *supra* note 134.

²⁷⁶ Transcript of Oral Argument, *supra* note 42, at *9.

²⁷⁷ Interview with Stephen Hagenah, *supra* note 134.

Herbert (442-503) Fall 2011

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

For half a century, Fourth Amendment doctrine has revolved around whether the interest being protected is one society is prepared to recognize as reasonable.²⁷⁹ Knotts was based on this principle.²⁸⁰ This change in the information a device collects from one involving police action to one independent of police action may alter the determination that a person traveling on public streets has no reasonable expectation of privacy. As the D.C. Circuit noted in Maynard, devices that record their precise location for an extended period of time may actually reveal information that is not exposed to the public.²⁸¹ In Maynard, the government argued—as it had successfully in other federal appellate courts—that the defendant's movements were exposed to the public because they took place on public streets where anyone could have seen and recorded them.²⁸² It was impossible to deny this as a factual matter. Instead, the court found that "the whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil."283

This interpretation of the Fourth Amendment is not novel. In a dissenting opinion in *Kyllo*, Justice Stevens argued that the same information revealed by the heat detector used by the police might also be noticed by a careful observer who saw that snow was melting faster on one house than another.²⁸⁴ But Justice Scalia responded: "The fact that

investigators] would have been unable to follow Hufford without using the beeper." United States v. Martyniuk, 395 F. Supp. 42, 43 (D. Or. 1975).

:..

²⁷⁹ Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'").

²⁸⁰ Knotts, 460 U.S. at 281 ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements").

²⁸¹ United States v. Maynard, 615 F.3d at 558 ("[T]he whole of one's movements over the course of a month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is effectively nil."), *cert. granted sub nom.*United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259)

²⁸² *Id.* at 556 ("The Government argues this case falls squarely within the holding in *Knotts* that '[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." (alteration in original) (quoting *Knotts*, 460 U.S. at 281)).

²⁸³ *Id.* at 558.

²⁸⁴ Kyllo v. United States, 533 U.S. 27, 43 (2001) (Stevens, J., dissenting).

493

2011 WHERE WE ARE WITH LOCATION TRACKING

equivalent information could sometimes be obtained by other means does not make lawful the use of means that violate the Fourth Amendment. The police might, for example, learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and entering to find out the same information lawful." Applied to location-tracking devices, this argument suggests that a tracking device that reveals information that would only be obtainable by twenty-four-hour surveillance is more likely to create constitutional issues than a less sophisticated device that requires much more police involvement.

The Court seems to be saying that the "reasonable expectation of privacy" test considers whether the suspect's action is exposed generally or exposed only to a person who is investigating a crime. In Bond, a border patrol agent walked down the aisle of a bus and "squeezed the soft luggage which passengers had placed in overhead storage space above the seats."286 Though the luggage was exposed to any passenger who wanted to squeeze it, Chief Justice Rehnquist, who also wrote the majority opinion in *Knotts*, said the agent's squeezing was a search protected by the Fourth Amendment because it was reasonable for the passenger to expect that other passengers would not touch the bag "in an exploratory manner."287 Even Justice Harlan, who created the reasonable expectation of privacy test in Katz, criticized the court's use of the phrase less than a decade later as "merely recit[ing] the expectations and risks without examining the desirability of saddling them upon society."288 Harlan wanted the court to consider the government's actions instead of relying solely on a suspect's conduct.²⁸⁹

_

²⁸⁵ *Id.* at 35 n.2 (majority opinion).

²⁸⁶ Bond v. United States, 529 U.S. 334, 335 (2000).

²⁸⁷ *Id.* at 338-39 ("When a bus passenger places a bag in an overhead bin, he expects that other passengers or bus employees may move it for one reason or another. Thus, a bus passenger clearly expects that his bag may be handled. He does not expect that other passengers or bus employees will, as a matter of course, feel the bag in an exploratory manner.").

²⁸⁸ United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

²⁸⁹ *Id.* ("The critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement.").

[Vol. 16:2

494

Finally, Riley and Ciraolo, seemingly the biggest hurdles to the argument that the compilation of a person's movements on public streets is not actually exposed to the public, cut in favor of requiring a warrant to conduct location tracking with minimal police involvement, as well.²⁹⁰ In Riley, the county sheriff believed Riley was growing marijuana on his property. After trying unsuccessfully to observe the marijuana from the road, the investigator flew a helicopter above the property and spotted the drugs.²⁹¹ Justice O'Connor, a necessary concurrence in the judgment in Riley, believed the relevant test was whether the police were in a place where "members of the public travel with sufficient regularity that Riley's expectation of privacy from aerial observation was not one that society is prepared to recognize as reasonable."292 A straightforward application of Riley to location tracking would indicate that, because the suspect is traveling on streets, where members of the public travel, the suspect has no reasonable expectation of privacy. However, the test in *Riley* focuses on the police officer's location. With RF-enabled beepers that require police involvement, the investigators are traveling on roads like other members of the public. Under the *Riley* test in that situation, it makes sense for a court to conclude that a suspect has no reasonable expectation to be free from government tracking when the police are traveling on public streets. However, with tracking devices that use stationary reference points and require no police involvement, the police are no longer conducting the observation where "members of the public travel with sufficient regularity."293 Instead, the investigators can be anywhere, including "sitting at home watching a football game." 294

2. How the Information Is Transmitted to the Investigator

A related consideration is how the information recorded by the tracking device is then transmitted to the investigator. Location-tracking devices can be divided into two categories based on how they transmit

-

²⁹⁰ Florida v. Riley, 488 U.S. 445 (1989); California v. Ciraolo, 476 U.S. 207 (1986).

²⁹¹ *Riley*, 488 U.S. at 448-49. The facts of *Ciraolo* are almost identical. In that case, the investigators flew a plane 1,000 feet above the property instead of flying a helicopter 400 feet above the property as they did in *Riley*. *Ciraolo*, 476 U.S. at 209.

²⁹² Riley, 488 U.S. at 454 (quotation marks omitted).

²⁹³ Id

²⁹⁴ Testimony of Peter Minahan, *supra* note 59, at 406.

information to law enforcement officers: static tracking devices, which only record and store data, and active devices, which use transmitters to send data.

A static, or passive, tracking device, also described as a "data logger," is solely a data receiver.²⁹⁵ It does not transmit any information at all. The device receives and records information about its location and oftentimes its speed. During the trial of Scott Weaver, the investigator described the Q-ball used in that investigation as "a data tracker, which will basically give you coordinate points. It won't tell you live. I can't dial that up from my home and find out where he is."²⁹⁶ A passive tracking device has to be removed by an investigator in order for the data to be retrieved.²⁹⁷

Active devices combine a typical passive satellite-based receiver with a transmitter that sends the information to a user in real-time.²⁹⁸ Whereas a passive device would require the agent to physically go under the car and remove and replace the device, an active device sends its location to the investigator either at regular intervals or at the investigator's request. As Investigator Minahan said at Scott Weaver's trial, "I could be sitting at home watching a football game and my cell phone would go off. It will be a certain tone, a certain message, that tells me that my target is moving. I dial up the laptop or turn the laptop on and dial my GPS and it will show me exactly where he's going, how fast he's going."²⁹⁹

There are also devices that fall in between. During the *Weaver* trial, the investigator said that he could simply drive by the car with the tracking device, push a button and download the data to his receiver.³⁰⁰ Though the investigator had to be in close proximity to the device to retrieve the data, he did not have to remove the device from the defendant's car.

RF-enabled tracking devices are by definition active, and cell-site tracking devices are also generally considered to be active devices because

_

²⁹⁵ Passive GPS Tracking, supra note 217.

²⁹⁶ Testimony of Peter Minahan, *supra* note 59, at 403.

²⁹⁷ Testimony of James Carroll, supra note 222 ("Somewhere from the rear tire to the bumper area.").

²⁹⁸ Real-Time GPS Tracking, supra note 217.

²⁹⁹ Testimony of Peter Minahan, *supra* note 59, at 406.

³⁰⁰ Id. at 405.

[Vol. 16:2

496

cell phones come equipped with transmitters. Yet this categorization divides satellite-based tracking devices in half. LandAirSea, for example, produces both a passive satellite-based Tracking Key device that investigators must remove from the car in order to retrieve the data it has recorded,³⁰¹ and an active satellite-based device called SilverCloud that can send real-time updates on the vehicle's location and speed via e-mail or text message.³⁰²

The active-passive distinction, however, may not be dispositive in the Fourth Amendment analysis. The beeper used in *Knotts* was an active device because it used a transmitter to send a signal to the investigator, but the Fourth Amendment does not prohibit the use of this type of device. On the other hand, a device that reveals a suspect's precise location may raise Fourth Amendment concerns, even if the data must be retrieved from the car, because, regardless of where the information is retrieved, the tracking is done from a location where members of the public are not traveling with regularity.

Yet when considered alongside the distinction about how the information is collected, the method that a device employs to transmit data can have important Fourth Amendment consequences. An active device generally allows an investigator to investigate not just from places where the public regularly travels, but from anywhere.³⁰⁴ As discussed more thoroughly in the previous subpart, the *Riley* test focuses on the location of the officer and asks if the officer is traveling in an area where members of the public frequently travel.³⁰⁵ To the extent that a transmitter allows an officer to track a suspect at all times while sitting in the comfort of his home, an active device may increase the likelihood of a Fourth Amendment violation.

³⁰¹ GPS TrackingKey Specifications, supra note 218; GPS Tracking Key Pro Specifications, supra note 220.

-

³⁰² SilverCloud Real-Time GPS Tracking System, supra note 225.

³⁰³ United States v. Knotts, 460 U.S. 276, 277 (1983) ("A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver.").

³⁰⁴ See supra note 295 and accompanying text (quoting an investigator testifying that an active device allows him to track a suspect while sitting at home watching football).

³⁰⁵ See supra notes 286-90 and accompanying text.

497

2011 WHERE WE ARE WITH LOCATION TRACKING

B. Accuracy

The natural instinct may be to say that accuracy should not be relevant to the Fourth Amendment inquiry. The reasoning behind this argument is that the government should not be punished for using more accurate tools.³⁰⁶ The Supreme Court made this point in *United States v. White*, where the Court upheld the use of evidence obtained from an informant wearing a wire by analogizing it to the already accepted technique of using an informant.³⁰⁷

But that argument only goes so far in the context of location tracking because of the strong presumption the Court has created against any investigative tactic that reveals information about the interior of a home. In *Kyllo*, the majority and dissent discussed whether the technology was "off-the-wall" or "through-the-wall," with the majority concluding that the most sophisticated thermal imaging devices continue to measure heat "off-the-wall." The *Kyllo* Court quoted *Silverman* for the proposition that "[a]t 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." In *Silverman*, the court found that even a small physical intrusion into a home—in that case, an electronic listening device that touched a heating duct of the target's house—violated the Fourth Amendment. In *Kyllo*, Justice Scalia expanded on this principle, stating that "there is certainly no exception to

³⁰⁶ See United States v. Garcia, 474 F.3d 994, 998 (7th Cir. 2007).

³⁰⁷ United States v. White, 401 U.S. 745, 753 (1971) ("Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable. An electronic recording will many times produce a more reliable rendition of what a defendant has said than will the unaided memory of a police agent. It may also be that with the recording in existence it is less likely that the informant will change his mind, less chance that threat or injury will suppress unfavorable evidence and less chance that cross-examination will confound the testimony. Considerations like these obviously do not favor the defendant, but we are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question.").

³⁰⁸ See United States v. Karo, 468 U.S. 705 (1984); Kyllo v. United States, 533 U.S. 27 (2001).

³⁰⁹ *Kyllo*, 533 U.S. at 35-36.

³¹⁰ Id. at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)).

³¹¹ Silverman, 365 U.S. at 512.

Herbert (442-503) Fall 2011

BERKELEY JOURNAL OF CRIMINAL LAW

[Vol. 16:2

the warrant requirement for the officer who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor. In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes."³¹²

This principle was extended to location tracking long before *Kyllo* in *Karo*, but it is even more relevant as tracking technology becomes more accurate. LandAirSea's TrackingKey boasts accuracy of 2.5 meters,³¹³ and the accuracy of tracking devices will almost certainly improve over the next decade. For example, the availability of other satellite-based networks such as the Russian GLONASS or the European Galileo will allow manufacturers to check information from multiple sets of satellites against each other.³¹⁴ Additionally, cell-site tracking has the ability to, in some cases, track users to specific floors of their buildings.³¹⁵ As devices become more accurate, the possibility that they will be used to reveal details about the home increases dramatically. Therefore, these devices pose the potential Fourth Amendment issues discussed in *Kyllo*.

This is particularly true when considered in conjunction with the increased miniaturization of location-tracking devices. GPSit's FS1, including the battery, is the size of a business card and less than a quarter-inch thick.³¹⁶ By contrast, the device used in *Knotts* needed enough batteries to fill the bottom two inches of a five-gallon drum.³¹⁷ And tracking devices continue to decrease in size. In fact, in 2001, the New York Times reported that scientists had developed a chip that could be inserted under the skin.³¹⁸ Even though it is unlikely that law enforcement would ever attempt to insert a device under a person's skin

_

³¹² Kyllo, 533 U.S. at 37.

³¹³ GPS Tracking Key Specifications, supra note 218; GPS Tracking Key Pro Specifications, supra note 220.

³¹⁴ See Wilson, supra note 183 (mentioning improvements in accuracy that will come from the use of GLONASS).

³¹⁵ Blaze testimony, supra note 195, at 30 ("New and emerging cell location techniques can work indoors and in places not typically accessible to GPS receivers. Cell-phone location information is quietly and automatically calculated by the network, without unusual or overt intervention that might be detected by the subject.").

³¹⁶ FS1 Battery Powered Covert GPS Tracker, supra note 244.

³¹⁷ Interview with Stephen Hagenah, supra note 134.

³¹⁸ Simon Romero, *Location Devices' Use Rises Prompting Privacy Concerns*, N.Y. TIMES (Mar. 4, 2001), http://www.nytimes.com/2001/03/04/business/location-devices-use-rises-prompting-privacy-concerns.html.

499

2011 WHERE WE ARE WITH LOCATION TRACKING

without a warrant,³¹⁹ it is easy to imagine law enforcement officers attaching a device to a watch, a pair of sneakers, or a wallet. To the extent that these items are worn or carried by people at all times, the risk of revealing details about the home will increase dramatically.

Some experts have said the move toward increased protection of the home is a mistake,³²⁰ but it is a position the Supreme Court has steadfastly supported. Just two years after holding in *Knotts* that the monitoring of a beeper on public streets was not a constitutionally protected search, the Court determined that the "monitoring of a beeper in a private residence, a location not open to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of the residence."³²¹

C. Power Supply

For as long as location-tracking devices have used batteries, the size of the battery has far surpassed the size of the device. Moreover, Hagenah said that the cold Minnesota winters often required him to replace the batteries on the cars he was tracking every few days. 323

³¹⁹ Such conduct would almost certainly violate the Fourth Amendment. *See* Winston v. Lee, 470 U.S. 753 (1985) (holding that surgery to remove a bullet from a suspect's body, even with a state order, was unreasonable and violated the Fourth Amendment). ³²⁰ *See, e.g.*, United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (2010) (Kozinski, J., dissenting) ("The very rich will still be able to protect their privacy with the aid of electric gates, tall fences, security booths, remote cameras, motion sensors and roving patrols, but the vast majority of the 60 million people living in the Ninth Circuit will see their privacy materially diminished by the panel's ruling.").

³²¹ United States v. Karo, 468 U.S. 705, 714 (1984). *See also supra* notes 304-08 and accompanying text (discussing the Court's holdings that any intrusion into the home violates the Fourth Amendment).

³²² The RF-enabled beeper used by Investigator Hagenah and his partners in *Knotts* was only about the size of a pack of cigarettes, but it required so many nine-volt batteries that the investigators filled the bottom two inches of the five-gallon drum of chloroform. Interview with Stephen Hagenah, *supra* note 134.

³²³ *Id.* By contrast, in Cape Cod in April 1975, officers investigating individuals suspected of manufacturing and distributing a controlled substance were able to use the signal from a beeper for more than two weeks before it died. United States v. Moore, 562 F.2d 106, 108-09 (1st Cir. 1977) (quoting an affidavit from one of the investigators which stated that on April 29, the "electronic surveillance signal placed in the chemicals . . . indicated the chemicals acquired on the 14th of April and observed and deposited at that house on the 14th of April remained in that house").

[Vol. 16:2

500

Today, the miniaturization of lithium ion batteries has played an important role in the scalability of tracking devices.³²⁴ Yet the battery is still by far the biggest part of tracking device. For instance, when Wired magazine and iFixIt.com dismantled and analyzed the satellite-based tracking device used by the FBI to track the animal activist, they found that the battery pack, which included four lithium-thionyl chloride D cell batteries, was significantly bigger than the rest of the device.³²⁵ iFixIt.com said each of the four batteries had about double the lifespan of an iPad 2.³²⁶

The tracking device that Afifi found on his car was also battery-powered, but according to a former FBI agent interviewed by Wired.com, that is unusual because the FBI typically designs its tracking devices so that they can be attached to a car's battery supply. Attaching the device to the car's battery supply, rather than powering it with a separate battery, was a technique used by some GPS manufacturers—at least those promoting navigation (if not those promoting tracking)—as early as 1995. It is particularly popular design option for active devices because those devices tend to require more power. 329

The question of how long a device can last without government intervention would seem to cut in both directions. On the one hand, a longer battery life allows the police to obtain a larger amount of information on a civilian without any extra work. If the "mosaic" argument put forth by the D.C. Circuit is a viable Fourth Amendment

-

³²⁴ Interview with Steve Moehling, *supra* note 221.

³²⁵ Tracking Device Teardown, supra note 86. For more on the animal activist incident, see supra notes 86-87 and accompanying text.

³²⁶ Tracking Device Teardown, supra note 86.

³²⁷ Zetter, *supra* note 95. For a more in-depth discussion of the Afifi incident, see *supra* notes 84-85 and accompanying text.

³²⁸ See Ditlea, supra note 164, at 121 ("Project Northstar's receiver as well as other GPS in-dash devices draw power from the car battery.").

³²⁹ Testimony of Peter Minahan, *supra* note 59, at 403 ("The live tracker would have to be—generally it's hooked to the electrical system of the car. They can be battery operated. However . . . the battery systems that are out there for that particular live system. They usually don't last too long. So generally speaking they are attached to the electrical system, hooked up to the electrical system."). *But see* Testimony of David Kirschner, *supra* note 234 (noting that the battery in the active GPS tracker used lasted from September 27 to October 14 before dying and that it then took the investigators five days to replace the batteries).

501

2011 WHERE WE ARE WITH LOCATION TRACKING

doctrine, then a longer battery life may paint a more detailed mosaic, which would favor calling it a search.³³⁰

On the other hand, a longer battery life also means fewer trips to the car to replace the device. As early as Knotts, some members of the court were skeptical about the constitutionality of the installation of the device.331 In Karo, the Court held that the installation of the device into the can did not violate the Fourth Amendment, 332 but the court has not ruled since on the installation of a tracking device on a defendant's private car. Dissenting from the D.C. Circuit's decision not to rehear Maynard en banc, Judge Kavanaugh noted that, even with a rehearing, the government might not prevail, in part, because the installation of the device may have violated the defendant's expectation of privacy.³³³ Judge Kavanaugh cited to the unanimous 1961 decision Silverman v. United States (also cited by Brennan in his concurrence in *Knotts*), which found a Fourth Amendment violation in the installation of a listening device on the defendant's property.³³⁴ Judge Kozinski's passionate dissent in the Ninth Circuit's denial of rehearing en banc of United States v. Pineda-*Moreno* also focused on the improper installation, though Judge Kozinski

³³⁰ United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010) ("Prolonged surveillance reveals types of information not revealed by short-term surveillance, such as what a person does repeatedly, what he does not do, and what he does ensemble. These types of information can each reveal more about a person than does any individual trip viewed in isolation. Repeated visits to a church, a gym, a bar, or a bookie tell a story not told by any single visit, as does one's not visiting any of these places over the course of a month. The sequence of a person's movements can reveal still more; a single trip to a gynecologist's office tells little about a woman, but that trip followed a few weeks later by a visit to a baby supply store tells a different story.") *cert. granted sub nom.* United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011) (No. 10-1259).

³³¹ United States v. Knotts, 460 U.S. 276, 286 (Brennan, J., concurring) ("I think this would have been a much more difficult case if respondent had challenged, not merely certain aspects of the monitoring of the beeper installed in the chloroform container purchased by respondent's compatriot, but also its original installation.").

³³² United States v. Karo, 468 U.S. 705, 711 ("The 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 respondents then had any legitimate expectation of privacy in it.").

³³³ United States v. Jones, 625 F.3d 766, 770 (2010) (Kavanaugh, J., dissenting) ("As the defendant here rightly points out, the police not only engaged in surveillance by GPS but also intruded (albeit briefly and slightly) on the defendant's personal property, namely his car, to install the GPS device on the vehicle.").

³³⁴ Silverman v. United States, 365 U.S. 505 (1961).

argued that trespass onto the driveway, which he considered to be in the curtilage of the home, was a violation of the Fourth Amendment. 335

A device that does not use batteries but instead taps into the battery supply of the car would raise different but equally complex Fourth Amendment issues. In McIver, Judge Kleinfeld thought that "the law requires us to treat the installation as a seizure for Fourth Amendment purposes" because the installation interfered with the car owner's protected interest in excluding individuals from performing mechanical work or altering his vehicle without consent.³³⁶ In that case, the device was battery-powered, meaning Judge Kleinfeld was concerned about the alterations that occurred when the device was simply attached to the undercarriage of the car.³³⁷ A device that requires the investigators to open up the hood or dashboard to attach the device to the car battery would raise these issues more clearly. The Supreme Court had these issues in mind when it granted certiorari in Jones. 338 Though the government requested certiorari on the question of whether the use of a tracking device violated the Fourth Amendment, the Supreme Court, in granting the petition, requested that the parties also brief the question of whether the installation of the device violated the Constitution.³³⁹

Additionally, the use of a suspect's car battery might constitute a seizure, which could also violate the Fourth Amendment if done unreasonably.³⁴⁰ As the Supreme Court has noted, "the concept of a 'seizure' of property is not much discussed in our cases."341 However, it is well-established that "[a] 'seizure' of property occurs when there is some

³³⁵ United States v. Pineda-Moreno, 617 F.3d 1120, 1123 (9th Cir. 2010) (Kozinski, J., dissenting).

³³⁶ United States v. McIver, 186 F.3d 1119, 1133 (9th Cir. 1999) (Kleinfeld, J., concurring).

³³⁷ *Id*.

³³⁸ See United States v. Jones, 131 S. Ct. 3064 (U.S. June 27, 2011). For a discussion of why the case is called *Jones* in the Supreme Court after being called *Maynard* in the D.C. Circuit, see supra note 2.

³³⁹ Jones, 131 S. Ct. 3064.

³⁴⁰ Cf. United States v. Williams, 592 F.3d 511, 514 (4th Cir. 2010) (describing the taking by the police of a suspect's computers, CDs, DVDs and gun as a seizure but noting that the seizure was reasonable).

³⁴¹ United States v. Jacobson, 466 U.S. 109, 113 n.5 (1984) (finding that agents who took control of a package from Federal Express exerted control over the package and was clearly a seizure, but later holding that it was not an unreasonable seizure).

503

2011 WHERE WE ARE WITH LOCATION TRACKING

meaningful interference with an individual's possessory interests in that property." A tracking device that draws from the car's battery supply would seem to interfere with the possessory interest the car owner has in that battery power. And to the extent that the battery power is replenished, the device would seem to interfere with the owner's possessory interest in the gasoline that it took to power the car. In *United States v. Jacobson*, the Supreme Court found that the destruction of a small amount of cocaine used to conduct a "field test" of the substance was a seizure because "by destroying a quantity of the powder [the government] converted what had been only a temporary deprivation of possessory interests into a permanent one." Analogously, the destruction of even a small amount of gasoline would result in the permanent deprivation of the suspect's possessory interest in the gasoline. The court would then have to decide whether the seizure is reasonable.

Courts considering location tracking have traditionally dismissed the claim of a seizure rather quickly, but they have not yet been confronted with a device that draws its power from a car battery.

-

³⁴² *Id.* at 113 (noting that the definition comes primarily from cases involving seizure of people); *see also*, Soldal v. Cook County, 506 U.S. 56, 61-62 (1992) (holding that the test for whether action constitutes a seizure is whether there is meaningful interference with an individual's possessory interests in the property but noting that "[w]hether the Amendment was in fact violated is, of course, a different question that requires determining if the seizure was reasonable"). The Court in *Soldal* made it clear that almost all property, not just property with a particular privacy interest, is protected against unlawful seizures. *Id.* at 65 ("We thus are unconvinced that any of the Court's prior cases supports the view that the Fourth Amendment protects against unreasonable seizures of property only where privacy or liberty is also implicated."); *see also* Altman v. City of High Point, 330 F.3d 194, 205 (4th Cir. 2003) (holding that "when the officers destroyed the dogs, they 'seized' the plaintiffs' 'effects'" but finding also that the officers did not act in an objectively unreasonable manner).

³⁴³ *Jacobson*, 466 U.S. at 124-25 (finding that police action that resulted in the loss of even a small amount of the defendant's drugs was a seizure because the defendant had a possessory interest in the property). *But see* Cardwell v. Lewis, 417 U.S. 583, 591 (1974) ("With the 'search' limited to the examination of the tire on the wheel and the taking of paint scrapings from the exterior of the vehicle left in the public parking lot, we fail to comprehend what expectation of privacy was infringed.").

³⁴⁴ United States v. Place, 462 U.S. 696, 703-04 (1983) (conducting a balancing test of the government interest and the level of intrusion, similar to the test in *Terry v. Ohio*, 392 U.S. 1 (1968)). In *Jacobson*, the Supreme Court held that the destruction of a de minimis amount of drugs was reasonable given that the police had probable cause to believe it was drugs. *Jacobson*, 466 U.S. at 125.

[Vol. 16:2

504

Notably, Judge Posner in *Garcia* wrote, "The defendant's contention that by attaching the memory tracking device the police seized his car is untenable. The device did not affect the car's driving qualities, *did not draw power from the car's engine or battery*, did not take up room that might otherwise have been occupied by passengers or packages, did not even alter the car's appearance, and in short did not 'seize' the car in any intelligible sense of the word." This statement seems to imply that Judge Posner believes the seizure analysis might be different if the device drew power from the car's engine or battery.

Even though a significant percentage of devices today appear to be powered through the car's battery, the Supreme Court may not reach this question in *Jones* because the device in that case was battery-powered,³⁴⁶ leaving open the possibility of more litigation.

V. CONCLUSION

In 1983, the Supreme Court allowed police to use a tracking device to help them follow a suspect without first securing a warrant. In the three decades since *Knotts*, the courts that have considered the constitutionality of location tracking have generally been content to rely on *Knotts* for the proposition that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."³⁴⁷

Even though tracking has been written about ad nauseum, missing from the literature (and the court opinions) is a discussion of the devices in use by law enforcement and a pointed analysis of their capabilities. But this analysis—how the device is installed, how long the battery lasts, how accurate it is, and what information it provides police—is critically important to any Fourth Amendment discussion. Devices that can determine the precise location of a suspect through triangulation and send that information to the police wherever they may be located could reveal information that is not actually exposed to the public.³⁴⁸ Devices that are accurate enough to determine the location of

³⁴⁵ United States v. Garcia, 474 F.3d 994, 996 (7th Cir. 2007) (emphasis added).

³⁴⁶ Testimony of Solomon Bitsie, *supra* note 124, at 16 ("That particular device has a satellite antenna on it, plus it has two cell phone antennas. And, actually this particular one, we used the battery pack to operate it.").

³⁴⁷ United States v. Knotts, 460 U.S. 276, 281 (1983).

³⁴⁸ See supra notes 266-301 and accompanying text.

505

2011 WHERE WE ARE WITH LOCATION TRACKING

Amendment's prohibition against unreasonable seizures.³⁵⁰

the suspect inside of the home may violate the Supreme Court's long-standing principle that the home is sacred territory incapable of even minor penetration without a warrant and absent exigent circumstances.³⁴⁹ And if investigators are required to open the hood of the car in order to attach the device to the battery supply, the intrusion may violate the suspect's interest in his car—or may even be enough to trigger the Fourth

The Supreme Court is poised to answer some of these questions in *Jones*. However, the device used in that case did not tap into the car's battery supply and was not accurate enough to violate the sanctity of the home. For three decades, courts have interpreted *Knotts* to mean that all location tracking is constitutional, even without a warrant. Even after the Court's ruling in *Jones*, it is important that courts faced with questions about location tracking consider the capabilities of the device at issue and all of the constitutional issues that the device may raise. It is important that courts do not once again fall into the trap of thinking that the entire

field of location tracking is settled based on the use of one subset of the

See supra notes 302-17 and accom

technology.

³⁴⁹ See supra notes 302-17 and accompanying text.

³⁵⁰ See supra notes 318-43 and accompanying text.