TILT LAW & TECHNOLOGY
WORKING PAPER SERIES

Criminal investigation and privacy in US law

Bryce C. Newell

Tilburg University, TILT
b.c.newell@tilburguniversity.edu

Version 1.0, February 2017

Citation: B.C. Newell, Criminal investigation and privacy in US law, TILT Law & Technology Working Paper Series, version 1.0, February 2017.

Abstract

The law regulating criminal investigation both legitimates the government's use of power and limits it by setting conditions for intrusions on fundamental rights and liberties. Privacy is one of the most prominent issues in establishing and limiting investigation powers. This paper analyses criminal investigation in relation to privacy in US law, with particular focus on privacy-related limitations and safeguards to criminal investigation powers. As part of a large-scale project on privacy protection in the 21st century, together with similar country studies, it will facilitate comparative legal analysis of criminal investigation (a relatively under-researched field), and also help to better understand privacy, as the forms and scope of privacy protection in criminal investigation law tell us something about how legislators conceptualize privacy, and how and to what extent the law protects different types of privacy.

Privacy-related crimes in US law

Version 1.0 (working paper), 28 February 2017

CONTENTS

1. Introduction

This report provides an overview of how privacy is protected through the law of criminal procedure in the United States. This working paper, which is part of a larger and on-going project, provides an overview of (selected) privacy-related aspects of US criminal procedure. We structure our analysis along four types of objects of the right to privacy, as identified in our earlier work: the protection of persons, places, things, and data.[1] Because the overall goal of this project is to generate a better understanding of the concept of privacy and its importance in our contemporary society filled with myriad new forms of surveillance and other privacy intrusions (and to do so from a comparative perspective), we conceptualize privacy broadly and include provisions that relate to the broad theme of protecting aspects of persons and their personal lives (encompassing the various types and dimensions of privacy we present in Koops, et al. (2017)). This conceptualization undoubtedly encompasses a large part of criminal procedure law. The current working version of this draft includes more substantive analysis of particular provisions (those prioritized by our on-going research to date), and additional analysis and analysis of additional provisions will continue to be added as the research progresses.

[1] *See* Koops, et al., *A Typology of Privacy*, 38 U. PA. J. INT'L L. __ (2017) (forthcoming).

Section 2 contains a short summary of the basic elements of US criminal procedure. Sections 3-4 outline criminal provisions related to protecting places (section 3) and persons (section 4).

2. Background: US criminal procedure

In the United States, criminal procedure rules are primarily dictated by judicial interpretations of the Fourth, Fifth, and Sixth Amendments to the US Constitution (part of the "Bill of Rights" adopted shortly after the Constitution was ratified).[2] However, the police are also regulated by state law through state courts and state legislatures,[3] as some states provide additional (stricter) rules that regulate police conduct.[4] As a result, federal (and state) courts tasked with interpreting the constitutional provisions and legislative enactments, generally serve as the first line of response for individuals raising privacy claims stemming from government use of new forms of privacy-invading techniques or technologies.[5] The Supreme Court of the United States frequently accepts and decides appeals related to criminal procedure, and it has developed a substantial body of case law on issues of privacy connected to government search and seizure (Fourth Amendment), compelled testimony and due process (Fifth Amendment), and assistance of counsel (Sixth Amendment), among others.

The most frequently cited form of constitutional privacy protection within criminal procedure is the Fourth Amendment's prohibition on unreasonable search and seizure. The text of the amendment contains two clauses: the first protects individuals and their "houses, papers, and effects, against unreasonable searches and seizures"; while the second describes the particularities and requirements of a judicially-issued warrant.[6] Supreme Court interpretations of the Fourth Amendment have required police to obtain warrants to overcome to overcome the general presumption of unreasonableness—though reasonable searches, or searches conducted pursuant to a judicially-created exception, fall outside the amendment's prohibition.[7] Warrants must be supported by affidavits that demonstrate probable cause, and must describe "the place to be searched, and the persons or things to be seized" with particularity.[8]

The Fifth Amendment, on the other hand, protects—among other things—the privilege against compelled self-incrimination. Prior to the Supreme Court decision in Miranda v. Arizona in

---

[2] CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: REGULATION OF POLICE INVESTIGATION 42, 50 (4th ed., Newark, NJ: Matthew Bender/LexisNexis, 2007).
[3] *Id.*.
[4] *See e.g.*, Wash. State Const. art I § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law," a stricter standard than that of the Fourth Amendment, which only requires warrants for "unreasonable" searches); State v. Snapp, 174 Wash.2d 177, 187-188 (Wash. 2012) ("The protections guaranteed by article I, section 7 are qualitatively different from those under the Fourth Amendment. Warrantless searches are per se unreasonable under our state constitution, subject to a limited set of carefully drawn exceptions" (citations omitted)); Rev. Code Wash. § 10.79.040 (prohibiting *all* searches of "any private dwelling house or place of residence without the authority of a search warrant"). State rules must be equivalent to or stricter then (and not more lenient) than federal Fourth Amendment requirements, as police are regulated by both state and federal rules.
[5] *See* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 802 (2004).
[6] U.S. CONST. amend IV.
[7] *See also* Daniel E. Chefitz, Note: *Fourth Amendment—The Presumption of Reasonableness of a Subpoena Duces Tecum Issued by a Grand Jury*, 82 J. CRIM. L. & CRIMINOLOGY 829 (1992).
[8] U.S. CONST. amend IV.

1966, most authority suggested that the privilege as only implicated in circumstances where a person was legally compelled to incriminate themselves at the risk of legal sanction—for example, contempt of court penalties for not responding to questions while under oath in a court of law—and not during police interrogation.[9]

3. The protection of places

3.1. Vehicles

For Fourth Amendment purposes, vehicles are considered "effects"—essentially items of personal property—that attract constitutional protection against unreasonable search and seizure.[10] However, the Supreme Court has repeatedly held that, for Fourth Amendment purposes, citizens have less substantial privacy interests in automobiles and other vehicles (e.g. boats) than they do with regard to their homes, dwellings, and other non-mobile structures.[11] That is, there is a "constitutional difference between houses and cars."[12] The Supreme Court has justified this lowered privacy interest in vehicles on multiple (complementary) theories, namely, that 1) vehicles are *mobile* and function primarily as a means of transport (or could be driven away before a warrant could be obtained), or because 2) vehicles attract a lesser expectation of privacy as they are not typically the "repository of personal effects," don't serve as a person's residence, are subject to significant licensing and registration requirements (because of the "compelling government need for regulation"[13]), and their contents are often in plain view on public streets. As put by the Supreme Court in 1974:

> One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where its occupants and its contents are in plain view.[14]

In Cardwell v. Lewis, the Court held that "where probable cause exists, a warrantless examination of the exterior of a car is not unreasonable under the Fourth and Fourteenth Amendments."[15] Upholding the reasonableness of examining tires and taking paint samples from the exterior of suspect's car, the Court stated:

> 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. Stated simply, the invasion of privacy, 'if it can be said to exist, is abstract and theoretical.'[16]

Searches of vehicles can be justified, under current law, in the following circumstances:

- Searches conducted under the "automobile exception" to the Fourth Amendment's warrant requirement (does not require any right to arrest occupants)
- Searches conducted incident to the arrest of the driver or a passenger

---

[9] Frank W. Miller,
[10] *See e.g.,* U.S. v. Jones, 132 S.Ct. 945, 949 (2012), *citing* United States v. Chadwick, 433 U.S. 1, 12 (1977) .
[11] *See* Cardwell v. Lewis, 417 U.S. 583, 590 (1974); Miller, et al., Criminal Justice Administration, p. 302.
[12] Chambers v Maloney, 399 U.S. 42 (1970).
[13] Carney at 392.
[14] *Cardwell* at 590.
[15] *Cardwell* at 591-92.
[16] At 591-92, *citing* Air Pollution Variance Board v. Western Alfalfa Corp., 416 U.S. 861, 865 (1974).

- Searches for weapons (for officer safety) during non-arrest stops or detentions
- When a search warrant has been obtained

Under the search incident to arrest exception, containers in the vehicle may also be subject to warrantless searches.

3.1.1. The "automobile exception"

One of six major exceptions to the Fourth Amendment's warrant requirement is the "automobile exception," first announced by the Supreme Court in the 1925 case of *Carroll v. United States*,[17] and later affirmed in subsequent cases, including the second leading case on this question, *Brinegar v. United States*, in 1949.[18] In *Carroll*, the court held that:

> the guaranty of freedom from unreasonable searches and seizures by the Fourth Amendment has been construed, practically since the beginning of the government, as recognizing a necessary difference between a search of a store, dwelling house, or other structure in respect of which a proper official warrant readily may be obtained and a search of a ship, motor boat, wagon, or automobile for contraband goods, where it is not practicable to secure a warrant, because *the vehicle can be quickly moved out of the locality or jurisdiction in which the warrant must be sought*.[19]

The Court held that officers can stop and search vehicles, without any corresponding cause to arrest the driver or any of its occupants, as long as the officer has "probable cause for believing that [the] vehicles are carrying contraband or illegal merchandise."[20]

In California v. Carney, the Court explained that,

> although ready mobility alone was perhaps the original justification for the vehicle exception, our later cases have made clear that ready mobility is not the only basis for the exception. The reasons for the vehicle exception, we have said, are twofold. 428 U.S., at 367, 96 S.Ct., at 3096."Besides the element of mobility, less rigorous warrant requirements govern because the expectation of privacy with respect to one's automobile is significantly less than that relating to one's home or office." *Ibid.*

In Carney, the vehicle at issue was a motor home, which had been searched by officers looking for drug without a warrant. The California Supreme Court had held that, because the vehicle was a motor home, the automobile exception did not apply, "the expectations of privacy in a motor home are more like those in a dwelling than in an automobile because the primary function of motor homes is not to provide transportation but to 'provide the occupant with living quarters.'"[21] However, the US Supreme Court reversed, holding that:

> When a vehicle is being used on the highways, or if it is readily capable of such use and is found stationary in a place not regularly used for residential purposes-temporary or otherwise-the two justifications for the vehicle exception come into play. First, the vehicle is obviously readily mobile by the turn of an ignition key, if not actually moving. Second, there is a reduced expectation of privacy stemming from its use as a licensed motor vehicle subject to a range of police regulation inapplicable to a fixed dwelling. At

[17] Carroll v. United States, 267 US. 132 (1925).
[18] Brinegar v. United States, 338 U.S. 160 (1949).
[19] *Carroll* at 153 (emphasis added).
[20] *Carroll*, at 154.
[21] 389

least in these circumstances, the overriding societal interests in effective law enforcement justify an immediate search before the vehicle and its occupants become unavailable.[22]

In these circumstances, a warrantless search of the vehicle was justifiable as long as probable cause existed at the time of the search. Carney also distinguished the facts of the case from those in which a motor home might not be subject to the exception:

> We need not pass on the application of the vehicle exception to a motor home that is situated in a way or place that objectively indicates that it is being used as a residence. Among the factors that might be relevant in determining whether a warrant would be required in such a circumstance is its location, whether the vehicle is readily mobile or instead, for instance, elevated on blocks, whether the vehicle is licensed, whether it is connected to utilities, and whether it has convenient access to a public road.[23]

However, some state constitutions provide more privacy protections in these cases, such as in Montana, where no automobile exception exists.[24]

3.1.2. Search of container in vehicle under the automobile exception

Per California v. Acevedo, searches of containers found in automobiles are subject to the automobile exception, BUT searches of containers may only be conducted without a warrant when there is probable cause to believe the container might hold evidence. That is, police may search the container (but not for the rest of the vehicle) when the object of the probable cause is the container itself, OR when the probable cause is to search the vehicle, they may also search inside the containers found in the vehicle as long as the probable cause would extend (i.e. when it is likely or possible that the evidence sought might be contained in the container.

> The police may search an automobile and the containers within it where they have probable cause to believe contraband or evidence is contained.[25]

And, quoting and upholding the rule in Ross (an earlier case), the court found that:

> "The scope of a warrantless search of an automobile ... is not defined by the nature of the container in which the contraband is secreted. Rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found."[26]

This right to search extends to all containers within a vehicle, regardless of whether they are owned by the person driving (or suspected of criminal conduct) or another passenger whom the police have no specific probable cause to believe has participated in any crime.[27]

Another, possible supplementary exception here is the Sanders footnote 13 "single-purpose container" rule, which holds that containers that disclose their contents by plain view, plain sight, or plain smell, also do not attract any reasonable expectation of privacy.[28]

---

[22] Carney at 392-93.
[23] Carney at 394, fn 3.
[24] State v. Elison, 302 Mont. 228, 249 (2000).
[25] Acevedo at 580.
[26] Acevedo at 579-580, quoting Ross, 456 U.S., at 824.
[27] Wyoming v. Houghton, 526 U.S. 295, (1999).
[28] The following is fn. 7 from U.S. v. Gust, 405 F.3d 797 (9th Cir. 2005):

> Courts have extended the *Sanders* footnote 13 exception beyond the classic "plain view once removed" scenario to cover "plain touch" cases, *see, e.g.*, *United States v. Portillo*, 633 F.2d 1313, 1320 (9th Cir.1980) (upholding warrantless search where officer lawfully came into contact with paper bag containing gun as he put his hand down to support his weight, because "[u]nder ... *Sanders* ... appellants did not possess a reasonable expectation of privacy in the

3.1.3. Inventory searches

As long as they impound (seizure) or the vehicle is justified, a regular inventory search of contents is permissible,[29] but only when such a search is conducted using "standardized procedures" and was not a case of rummaging around looking for evidence.[30]

3.1.4. Searches of vehicles for weapons

Police may search for or seize weapons during automobile stops in order to maintain their safety, including conducting Terry-style frisks for weapons on drivers or passengers when the officer has a reasonable belief that the person may be armed,[31] or "frisks" of vehicles for weapons – based on articulable facts that the peson may be dangerous and that a vehicle might hold weapons, and limited to searching areas where "a weapon might be placed or hidden."[32]

4. The protection of persons

4.1. Protections for behavioural privacy

4.1.1. Location tracking

In the United States, judicial interpretations of the Fourth Amendment to the United States' Constitution governs location tracking by the police. Procedurally, the Federal Rules of Criminal Procedure (primarily Rule 41) also regulate how and when warrants for various types of investigative location tracking activities can take place. Certain state-level laws may also regulate police conduct in those particular states more rigorously than the Fourth Amendment does, but any such state laws are outside the scope of this report.

The Fourth Amendment reads,

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[33]

Generally, the Fourth Amendment will apply to location-tracking activities that amount to a "search."[34] When investigative conduct would amount to a search, the Fourth Amendment requires the police to obtain a warrant prior to engaging in such conduct. Whether a search is, or is not, reasonable depends on whether the search would 1) constitute a trespass to or interference with a "constitutionally protected area" (e.g., the subject's house, personal property, communications, or body) or 2) whether it would violate the subject's legitimate

---

paper bag[ ]" as its contents "were apparent from the outward feel of the container"), and "plain smell" cases, *see, e.g., United States v. Haley*, 669 F.2d 201, 203-04 (4th Cir.1982) (upholding warrantless search of boxes and bags smelling of marijuana because for the purposes of the *Sanders/Robbins* exception, "[a]nother characteristic which brings the contents [of a container] into plain view is the odor given off by those contents"). These extensions of the *Sanders*exception are not implicated in this appeal.

[29] South Dakota v. Opperman, 428 U.S. 364 (1976).
[30] Colorado v. Bertine, 479 U.S. 367, 376 (1987), quoted and affirmed in Florida v. Wells, 495 U.S. 1 (1990).
[31] Adams v. Williams, 407 U.S. 143 (1972); Pennsylvania v. Mimms, 434 U.S. 106 (1977).
[32] Michigan v. Long, 463 U.S. 1032, 1049-50 (1983).
[33] U.S. Const. Amend. IV.
[34] CHARLES H. WHITEBREAD & CHRISTOPHER SLOBOGIN, CRIMINAL PROCEDURE: AN ANALYSIS OF CASES AND CONCEPTS 98 (6th ed., St. Paul, MN: West, 2015).

expectation of privacy.[35] These questions have been raised in a number of Supreme Court and lower federal court decisions (see below).

Federal law defines "tracking device" broadly, as "an electronic or mechanical device which permits the tracking of the movement of a person or object."[36] If law enforcement seek to obtain a tracking warrant, Rule 41 of the Federal Rules of Criminal Procedure outlines certain requirements. Tracking warrants may authorize tracking activities that occur within the territorial jurisdiction of the court issuing the warrant or order, or elsewhere as long as the installation of the device occurred within the court's jurisdiction.[37] Under Rule 41 (and Fourth Amendment case law), a tracking warrant may only be issued if the law enforcement's evidence demonstrates probable cause to believe that the tracking will result in the acquisition of evidence of criminal wrongdoing.[38]

Rule 41 also outlines certain requirements specific to tracking warrants. For example, 18 U.S.C. section 3117(e)(2)(C) states:

> **Warrant for a Tracking Device.** A tracking-device warrant must identify the person or property to be tracked, designate the magistrate judge to whom it must be returned, and specify a reasonable length of time that the device may be used. The time must not exceed 45 days from the date the warrant was issued. The court may, for good cause, grant one or more extensions for a reasonable period not to exceed 45 days each. The warrant must command the officer to:
>
> (i) complete any installation authorized by the warrant within a specified time no longer than 10 days;
>
> (ii) perform any installation authorized by the warrant during the daytime, unless the judge for good cause expressly authorizes installation at another time; and
>
> (iii) return the warrant to the judge designated in the warrant.

After executing a tracking warrant, an officer must note on the warrant "the exact date and time the device was installed and the period during which it was used."[39] Additionally, within 10 days after the tracking has ended, the officer must return the warrant to the judge and serve the subject of the surveillance with a copy of the warrant, unless an extension has been granted under 18 U.S.C. section 3117(f)(3).[40]

The legal goods (interests) protected.

The Fourth Amendment limits unreasonable intrusions by the state into the privacy of US citizens and certain non-citizens "who have… developed sufficient connection with this country to be considered part of [the national] community."[41] The dual tests to determine whether a search has occurred protect against state interference with privacy and certain property-based interests. If state investigative conduct interferes with a person's body, personal property, or communications, or intrudes into the person's home (including the curtilage around the home), it is presumptively unreasonable.

---

[35] *Id.* at 98-99.
[36] 18 U.S.C. § 3117(b).
[37] 18 U.S.C. § 3117(a).
[38] *See, e.g.*, 18 U.S.C. § 3117(d)(1).
[39] 18 U.S.C. § 3117(f)(2)(A).
[40] 18 U.S.C. §§ 3117(f)(2)(B)-(C).
[41] U.S. v. Verdugo-Urquidez, 494 U.S. 259, 265 (1990).

Types of location tracking

The following subsections examine how case law from federal appellate courts regulates certain forms of police investigatory conduct to track the locations and movements of suspects in criminal investigations. Quite a few relevant cases have emerged in recent years. Generally, most of these cases involve tracking via GPS devices or obtaining historical and/or real-time location records from cellular service providers. The analysis of these cases below does not include trial (district) court decisions or state court decisions (at any level).

Visual observation

Generally, unaided human observation or video surveillance of a subject's location will not amount to a search under the Fourth Amendment, especially when the officer observes the subject in a publicly accessible place[42] or when the officer observes the subject from a place where the officer has the legal right to be.[43] As the Tenth Circuit has stated very clearly, "The use of video equipment and cameras to record activity visible to the naked eye does not ordinarily violate the Fourth Amendment."[44] In another Tenth Circuit decision, *United States v. Houston*, the court held that a person cannot maintain a legitimate expectation of privacy in activities that occur outside their home and that are visible to any passersby (for example, from a public road or sidewalk).[45] However, under the Supreme Court's decision in *Kyllo v. United States*, observation conducted by the use of a device that is "not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion"[46] could be considered a search for Fourth Amendment purposes.[47]

GPS (or GPS-like) tracking

Cases involving GPS-based tracking or earlier forms of GPS-like technologies have arisen in federal appellate courts since the late 1970s, with the Supreme Court weighing in for the first time in *United States v. Knotts*[48] in 1983. Many of these early cases involved challenges to the

---

[42] *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281-82 (1983) ("A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").
[43] *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible."); *see also* Dow Chemical Co. v. United States, 476 U.S. 227 (1986); Kyllo v. United States, 533 U.S. 27 (2001) (use of thermal imaging device was a search, in part because it extended beyond mere visual observation from a public vantage point).
[44] United States v. Jackson, 213 F.3d 1269, 1280 (10th Cir. 2000), *vacated on other grounds*, 531 U.S. 1033 (2000).
[45] United States v. Houston, 813 F.3d 282, 287-88 (6th Cir. 2016) ("There is no Fourth Amendment violation, because Houston had no reasonable expectation of privacy in video footage recorded by a camera that was located on top of a public utility pole and that captured the same views enjoyed by passersby on public roads."). However, in at least one district court, a trial judge has found that extended and warrantless video surveillance of a home can violate a reasonable expectation of privacy. United States v. Vargas, Order Granting Defendant's Motion to Suppress, Case no. CR-13-6025-EFS (E.D. WA., Dec. 15, 2014) ("society expects that law enforcement's continuous and covert video observation and recording of an individual's front yard must be judicially approved").
[46] Kyllo v. United States, 533 U.S. 27 (2001).
[47] This might include, for example, the use of through-the-wall radar or WiFi signal analysis software, each of which could track movements through walls of a home or other constitutionally protected areas.
[48] 460 U.S. 276 (1983).

use of "beepers" to track various items, including vehicles,[49] airplanes,[50] and containers or packages of contraband given or sold to suspects.[51] As defined by the Court in *Knotts*, "A beeper is a radio transmitter, usually battery operated, which emits periodic signals that can be picked up by a radio receiver" and that can be used to track the movement of an object to which it is attached.[52] Prior to *Knotts*, courts were divided on the question of whether the Fourth Amendment applied to the use of beepers, although many held that tracking automobiles or airplanes on public roads or airspace, respectively, did not constitute a Fourth Amendment search. As the Ninth Circuit summarized its case law in 1976,

> (u)nder the law of this circuit, . . . attachment of an electronic location device to a vehicle moving about on public thoroughfares (or through the public airspace) does not infringe upon any reasonable expectation of privacy and therefore does not constitute a search. . . . Consequently, no warrant is needed . . . unless fourth amendment rights necessarily would have to be violated in order to initially install the device.[53]

Some of these decisions were predicated on the courts' conclusions that airplanes, automobiles, and contraband were heavily regulated and, as such, they attracted diminished expectations of privacy. Tracking airplane locations was necessary to keep the airspace safe, thus a suspect could not claim a reasonable expectation of privacy in the location of an aircraft.[54] Automobiles moving about on public roads are exposed to public view and scrutiny, thus diminishing the expectation of privacy a driver or passenger may have in the vehicle's location.[55] Contraband, by its very nature as something that a suspect has no legal right to possess in the first place, cannot attract a legitimate expectation of privacy, thus tracking it cannot violate a Fourth Amendment interest.[56] Some courts also analogized beeper use to visual surveillance, finding no importance (for constitutional purposes) in the augmentation to visual surveillance provided by a transponder.[57] Under these early cases, the strongest case for a Fourth Amendment violation had to do with whether the *installation* of the beeper constituted a search (e.g., it was

---

[49] United States v. Knotts, 460 U.S. 276, 281-82 (1983).
[50] United States v. Bruneau, 594 F.2d 1190, 1194 (8th Cir. 1979), *cert. denied*, 444 U.S. 847 (1979) ("the use of a transponder to track aircraft in public airspace [does not] constitute[] a search within the fourth amendment").
[51] *See* United States v. Bruneau, 594 F.2d 1190, 1194 fn. 6 (In the context of contraband, "courts have consistently held that use of a beeper in such circumstances is not a search on the ground that no one has a 'legitimate expectation of privacy in substances which they have no right to possess at all.' United States v. Moore, 562 F.2d 106, 111 (1st Cir. 1976); See, e. g., United States v. Botero, 589 F.2d 430 (9th Cir. 1978); United States v. Pringle, 576 F.2d 1114, 1119 (5th Cir. 1978) (beeper placed in package of heroin); United States v. Emery, 541 F.2d 887, 890 (1st Cir. 1976) (beeper placed in packages of cocaine); United States v. Perez, 526 F.2d 859, 863 (5th Cir.), Cert. denied, 429 U.S. 846, 97 S.Ct. 129, 50 L.Ed.2d 118 (1976) (beeper placed in television which was bartered in a heroin trade); United States v. French, 414 F.Supp. 800, 803, 804 (W.D.Okl.1976) (beeper placed in marijuana); United States v. Carpenter, 403 F.Supp. 361, 365 (D.Mass.1975) (beeper placed in packages of cocaine)").
[52] United States v. Knotts, 460 U.S. 276, 277 (1983).
[53] United States v. Pretzinger, 542 F.2d 517, 520 (9th Cir. 1976).
[54] *See, e.g.*, United States v. Miroyan, 577 F.2d 489 (1978) ("use of the transponder merely to monitor the location of the aircraft as it passed through public airspace was not a search").
[55] *See e.g.*, United States v. Hufford, 539 F.2d 32 (9th Cir. 1976) ("One has a lesser expectation of privacy in a motor vehicle because its function is transportation and it seldom serves as one's residence or as the repository of personal effects. A car has little capacity for escaping public scrutiny. It travels public thoroughfares where both its occupants and its contents are in plain view."); Cardwell v. Lewis, 417 U.S. 583, 590 (1974) (plurality); Rakas v. Illinois, 439 U.S. 128, 153-154, and n. 2 (1978) (POWELL, J., concurring); South Dakota v. Opperman, 428 U.S. 364, 368 (1976).
[56] United States v. Moore, 562 F.2d 106, 111 (1st Cir. 1976).
[57] *See, e.g.*, Hufford, 539 F.2d at 34; Knotts, 460 U.S. at .

installed while agents were trespassing or interfering with property in which the suspect had a reasonable expectation of privacy). However, a number of cases did not find Fourth Amendment violations on that basis either.[58]

In 1983, the Supreme Court took up the issue when it granted certiorari and decided *Knotts*. In that case, police had attached a beeper to the inside of "a five gallon container of chloroform" with the consent of the company that owned the container, because they suspected one of the defendants of stealing and buying chemicals that could be used to make illegal drugs.[59] At the police's request, the company agreed to fill that particular container and deliver it to the defendant when he made his next purchase of chloroform.[60] The police then tracked the defendant's vehicle by using both the beeper and by maintaining visual contact until the container was transferred to the second defendant's vehicle.[61] The police eventually cut off visual contact with the second vehicle when the driver began to make evasive maneuvers.[62] At that point, the police also lost the beeper signal.[63] The police then reacquired the signal about an hour later by searching the area with a helicopter equipped with a receiver, and located the vehicle at the defendant's cabin.[64] Importantly, there was no evidence that the beeper was used to track the location of the container inside the cabin, but only to position the container as located somewhere in that vicinity.[65]

The *Knotts* Court held that the use of the beeper did not violate the defendants' Fourth Amendment rights.[66] The court stated,

> A person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another. When [the defendant] travelled over the public streets he voluntarily conveyed to anyone who wanted to look the fact that he was travelling over particular roads in a particular direction, the fact of whatever stops he made, and the fact of his final destination when he exited from public roads onto private property.[67]

The Court drew an analogy between their holding in this case and the third party doctrine promulgated in *Smith v. Maryland*,[68] which involved the use of a "pen register" to collect information about telephone calls made by a suspect. In the Court's view, the use of the beeper merely augmented the visual surveillance capabilities that the police could generally use, and did not alter their conclusion that surveillance on public roads and in "open fields" did not

---

[58] *See, e.g.*, U.S. v. Clayborne, 584 F.2d 346 (10th Cir. 1978) (warrantless placement of electronic tracking device in a container of ether was not a per se violation of the Fourth Amendment); United States v. Frazier, 538 F.2d 1322 (8th Cir. 1976) (holding that the attachment of tracking device to suspect's car was an "actual trespass," but that suppression of evidence was not appropriate because the search was justified by probable cause); United States v. Bentley, 706 F.2d 1498 (8th Cir. 1983) (probable cause existed for attaching an electronic tracking device to a machine bought by the defendant).
[59] *Knotts*, 460 U.S. at 278.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.* at 278-79.
[66] The respondent in the case did not challenge the installation of the beeper in the chloroform container, so the court did not address that issue directly, although Justices Brennan and Stevens both discussed this issue briefly in their concurrences. *Id.* at 285-87.
[67] *Id.* at 281-82.
[68] 442 U.S. 735 (1979).

attract Fourth Amendment protections because the suspects voluntarily exposed their movements in such places to third parties. As stated by the Court:

> Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case.[69]

Although the defendant argued that such a holding would legitimize "twenty-four hour surveillance of any citizen of this country… without judicial knowledge or supervision," the Court stated that "the 'reality hardly suggests abuse.'"[70] Additionally, the court stated 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."[71]

A year later, the Court held, in *United States v. Karo*, that DEA agents did not violate the defendants' Fourth Amendment rights when they installed a beeper inside a can of ether prior to its sale to one of the defendants,[72] but that a violation occurred when the agents tracked the can after it entered a private residence.[73] The installation of a tracking device was permissible, the court stated, regardless of whether the agents replaced one of the original cans with one of their own or installed their device into one of the original cans with consent of the owner of the cans at the time the installation took place, because the defendants did not have any legitimate expectation of privacy in the can at the moment of installation (before purchasing it).[74] The court explained its reasoning as follows:

> The mere transfer to [the defendant] of a can containing an unmonitored beeper infringed no privacy interest. It conveyed no information that [the defendant] wished to keep private, for it conveyed no information at all. To be sure, it created a potential for an invasion of privacy, but we have never held that potential, as opposed to actual, invasions of privacy constitute searches for purposes of the Fourth Amendment. A holding to that effect would mean that a policeman walking down the street carrying a parabolic microphone capable of picking up conversations in nearby homes would be engaging in a search even if the microphone were not turned on. It is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence.[75]

After the sale, however, agents used the beeper to track the can after it entered a private residence.[76] Because of the Fourth Amendment's broad prohibition on unwarranted intrusions into homes, the court held that when the "Government surreptitiously employs an electronic device to obtain information that it could not have obtained by observation from outside the curtilage of the house," and does so without a warrant, it violates the Fourth Amendment.[77] In this situation, the court continued, the device does more than merely augment an officer's visual abilities.

---

[69] *Id.* at 282.
[70] *Id.* at 284, *quoting* Zurcher v. Stanford Daily, 436 U.S. 547, 566 (1978).
[71] *Id.* at 284.
[72] United States v. Karo, 468 U.S. 705, 711 (1984).
[73] *Id.* at 714.
[74] *Id.* at 711.
[75] *Id.* at 712.
[76] *Id.* at 714.
[77] *Id.* at 714-15.

> Even if visual surveillance has revealed that the article to which the beeper is attached has entered the house, the later monitoring not only verifies the officers' observations but also establishes that the article remains on the premises.[78]

Where, in *Knotts*, "the information obtained… was 'voluntarily conveyed to anyone who wanted to look,'" the information obtained in *Karo* included facts about the inside of the house (e.g., the continued presence of the can) "that could not have been visually verified" without intruding into the curtilage.[79]

Between 1984 and 2012, when the Supreme Court decided *United States v. Jones*,[80] circuit courts around the country continued to decide cases involving different forms of beeper or GPS tracking. Some of these cases extended the reasoning of *Knotts* in the context of GPS tracking, holding that a warrant was not required before inserting a tracking device into an intercepted package of heroin[81] or and that the installation of tracking devices on vehicles did not violate the Fourth Amendment because GPS tracking merely

> utilizes technology to substitute "for an activity, namely following a car on a public street, that is unequivocally not a search within the meaning of the [Fourth Amendment].'[82]

In *United States v. Garcia*, the Seventh Circuit reasoned that

> GPS tracking is on the same side of the divide with ... surveillance cameras and ... satellite imaging, and if what they do is not searching in Fourth Amendment terms, neither is GPS tracking.[83]

However, one circuit court came to the opposite conclusion, in *United States v. Maynard*.[84] In *Maynard*, which later became *Jones* on appeal to the Supreme Court, the judge stressed that the facts of the case, which involved continuous GPS monitoring of the defendant's vehicle over a 28 day period, directly pressed on the question left open by *Knotts*—that is, whether "dragnet-type law enforcement practices" such as "'wholesale' or 'mass' electronic surveillance… requires a warrant."[85] The judge held that prolonged GPS monitoring of a vehicle for 28 days amounted to an unreasonable search, because the GPS monitoring had obtained information that was "not exposed to the public."[86] The judge reasoned that,

> unlike one's movements during a single journey, the 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. Second, the whole of one's movements is not exposed *constructively* even though each individual movement is exposed, because that whole reveals more—sometimes a great deal more—than does the sum of its parts.[87]

---

[78] *Id.* at 715.
[79] *Id.* at 715, *quoting* Knotts, 460 U.S. at 281.
[80] United States v. Jones, 565 U.S. 400 (2012).
[81] United States v. Gbemisola, 225 F.3d 753 (DC Cir. 2000).
[82] United States v. Cuevas–Perez, 640 F.3d 272, 273-74 (7th Cir. 2011), *quoting*, United States v. Garcia, 474 F.3d 994, 997 (7th Cir. 2007). *See also* United States v. Pineda-Moreno, 591 F.3d 1212 (9th Cir. 2010), *rehearing after remand at* U.S. v. Pineda-Moreno, 688 F.3d 1087 (9th Cir. 2012) (exclusionary rule not applicable because police relied on existing law (pre-Jones) when they tracked vehicle without a warrant), *overruled and vacated by* United States v. Jones, 132 S.Ct. 1533); United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir.2010).
[83] Garcia, 474 F.3d at 997.
[84] United States v. Maynard, 615 F.3d 544 (D.C.Cir. 2010).
[85] *Id.* at 556, 558.
[86] *Id.* at 558.
[87] *Id.* at 558.

This reasoning was informed by the "mosaic theory," which the judge borrowed from case law related to exemptions to disclosure under the federal Freedom of Information Act for national security purposes.[88] And, according to the judge, prolonged GPS tracking violated the defendant's reasonable expectation of privacy, in part because,

> 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. 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.[89]

This reasoning was later endorsed at the Supreme Court by both concurring opinions in *Jones*,[90] despite the fact that Justice Scalia's majority opinion avoided the reasonable expectation of privacy test altogether in finding that the installation of the GPS tracking device inside the vehicle's rear bumper violated the defendant's Fourth Amendment rights because it amounted to an unwarranted trespass and interference to the defendant's property.[91] According to the primary opinion, the installation was a search for Fourth Amendment purposes because, "[t]he Government physically occupied private property for the purpose of obtaining information"[92] when the agent installed the tracking unit. This holding is consistent with *Karo* because, in *Jones*, the defendant already possessed the vehicle at the time the device was installed by the police.[93]

In a number of later cases, defendants contested GPS tracking that occurred prior to the *Jones* decision. In many of these cases, courts have applied the "good faith exception" to the exclusionary rule, allowing evidence to be admitted in those cases on the basis that the officers had reasonably relied on existing legal precedent at the time they installed the tracking devices.[94] In at least one case, a court refused to exclude evidence obtained from the

---

[88] *Id. at 562, quoting* CIA v. Sims, 471 U.S. 159, 178 (1985) ("[w]hat 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") (internal citations omitted).

[89] *Id.* at 562.

[90] *Jones*, 565 U.S. at 417-18 (Sotomayor, concurrence), 428-31 (Alito, concurrence).

[91] *Jones*, 565 U.S. at 404-05.

[92] *Id.* at 404.

[93] *Id.* at 409-10 ("Jones, who possessed the Jeep at the time the Government trespassorily inserted the information-gathering device, is on much different footing").

[94] *See, e.g.*, United States v. Cabrera, 651 Fed.Appx. 118 (3rd Cir. 2016) (pre-Jones GPS tracking of vehicle fell within exclusionary rule's good faith exception); United States v. Martin, 807 F.3d 842 (7th Cir. 2015) (warrantless GPS tracking of defendant's car for 45 days, prior to Jones decision, did not justify exclusion of evidence); United States v. Robinson, 781 F.3d 453 (8th Cir. 2015) (placement of GPS device on car fell within good faith exception to exclusionary rule); United States v. Taylor, 776 F.3d 513 (7th Cir. 2015) (warrantless GPS tracking of vehicle was reasonable pre-Jones); United States v. Smith, 609 Fed.Appx. 180 (5th Cir. 2015) (unpublished) (warrant for GPS tracking a vehicle was justified by good faith reliance on existing precedent); United States v. Ransfer, 749 F.3d 914 (11th Cir. 2014) (police attaching global positioning system (GPS) tracking device to vehicle without obtaining a warrant reasonably relied on long-standing, clear circuit precedent); United States v. Katzin, 769 F.3d 163 (3d Cir. 2014) (exclusionary rule did not apply to evidence obtained as a result of GPS tracking, as a reasonable agent would have believed in good faith that the use of a

warrantless use of a GPS tracking unit because the police had also obtained the same information by tracking the suspect's phone, which was covered by a valid warrant.[95]

In one recent Supreme Court decision, the question was whether a state program that mandated satellite-based monitoring of certain recidivist sex offenders after they had completed their sentences was a Fourth Amendment search. In *Grady v. United States*, the court held that "a State … conducts a search when it attaches a device to a person's body, without consent, for the purpose of tracking that individual's movements."[96]

Cell-site location information

In a number of recent cases, defendants have challenged police access to and use of location information obtained (primarily) from cellular service providers. So-called "cell-site location information" can be potentially accessed after the fact (historical location tracking) or in real time (real-time location tracking). In cases involving police accessing historical location information from cellular service providers under the Stored Communications Act,[97] courts have generally held that no search has occurred, citing the third party doctrine and equating location information with non-content information (such as that captured by pen registers) that attracts lesser constitutional protection.[98] Under the Stored Communications Act, the government may access such records so long as it demonstrates "reasonable grounds" to believe that the records are "relevant and material to an ongoing investigation,"[99] a lesser standard than the probable cause required for a warrant. In the context of real-time location tracking of suspects' cellular phones, courts have also applied the reasoning from *Knotts* to determine that defendants did not have legitimate expectations of privacy in their location while they moved about in publicly accessible places, like public highways.[100] In other cases, phone tracking has been justified under the authority of warrants or other court orders, and as such have not been unreasonable.[101]

GPS device without a warrant was lawful prior to the Jones decision); United States v. Brown, 744 F.3d 474 (7th Cir. 2014) ("Knotts and Karo jointly show that tracking a car's location by GPS is not a search no matter how long tracking lasts"), *cert. denied*, 135 S.Ct. 378 (2014); United States v. Aguiar, 737 F.3d 251 (2nd Cir. 2013) (warrantless placement of global positioning system device (GPS) on defendant's vehicle fell within the good-faith exception to exclusionary rule).

[95] U.S. v. Luna-Santillanes, 554 Fed.Appx. 402 (6th Cir. 2014) (unpublished).

[96] Grady v. North Carolina, 135 S.Ct. 1368, 1370 (2015).

[97] 18 U.S.C. §§ 2701, *et seq*.

[98] United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (government did not conduct a "search" for Fourth Amendment purposes when it obtained cell tower locational data from defendants' wireless carrier – based on non-content/metadata distinction and the third party doctrine); United States v. Graham, 824 F.3d 421 (4th Cir. 2016) (cell-site tracking without a warrant did not violate the Fourth Amendment due to the third party doctrine), *overruling* United States v. Graham, 796 F.3d 332 (4th Cir. 2015); United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (obtaining CSLI under the SCA not a "search" for Fourth Amendment purposes), *overruled* 754 F.3d 1205 (2014).

[99] 18 U.S.C. § 2703(d).

[100] *See, e.g.*, United States v. Forest, 355 F.3d 942 (6th Cir. 2004) (interception of cellular phone data revealed defendant's general location while traveling on public highways. Court applied *Knotts*, finding "no legitimate expectation of privacy in the cell-site data because the DEA agents could have obtained the same information by following Garner's car").

[101] *See, e.g.*, United States v. Luna-Santillanes, 554 Fed.Appx. 402 (6th Cir. 2014); *see also* United States v. Turner, 781 F.3d 374 (8th Cir. 2015) (exclusion of evidence was not proper remedy for government's failure to comply with procedural requirements for preparing, executing, and returning a warrant for a tracking device, namely precise location information from defendant's cell phone).

Use of a cell-site simulator (stingray)

Police use of cell-site simulators (also sometimes called IMSI catchers, or "stingrays") to capture and redirect cellular communications is becoming a significant issue, and cases challenging the use of these devices are only just beginning to appear. For example, in *United States v. Patrick,*[102] the Seventh Circuit held that the warrantless use of a cell-site simulator to locate a suspect with an outstanding warrant did not require exclusion of evidence when it was used to locate the suspect in a public space. However, the court explicitly avoided a full analysis of whether the use of the simulator was itself a search for Fourth Amendment purposes, leaving that analysis for future cases.[103]

Using software (e.g., MoocherHunter) to locate a computer

In a growing number of (primarily) district court decisions, defendants have challenged the investigatory use of directional WiFi tracking antennas and associated software. Generally, police have used these technologies to identify locations where child pornography or other illicit material is being downloaded.[104] Besides using directional antennas to physically locate the source of WiFi transmissions, police have also often relied on locating computers based on IP addresses.[105]

[102] United States v. Patrick, 842 F.3d 540 (7th Cir. 2016).
[103] *Id.* at 545.
[104] *See, e.g.,* U.S. v. Stanley, 753 F.3d 114 (3rd Cir. 2014) (warrantless use of MoocherHunter software to locate the probable residence where a wireless signal was emitted from was reasonable)
[105] *See, e.g.,* U.S. v. Reynolds, 626 Fed.Appx. 610 (6th Cir. 2015).