2015

Where Are You Going, Where Have You Been? Seriously, Let Me See Your GPS.

Rajendra Persaud
Hostra University

Follow this and additional works at: https://academicworks.cuny.edu/clr

Part of the Law Commons

Recommended Citation
Available at: https://academicworks.cuny.edu/clr/vol18/iss2/8

The CUNY Law Review is published by the Office of Library Services at the City University of New York. For more information please contact cunylr@law.cuny.edu.
Where Are You Going, Where Have You Been? Seriously, Let Me See Your GPS.

Acknowledgements
He would like to thank Alafair Burke, criminal law professor, for guidance throughout writing this piece and also Toni Aiello, reference librarian, for her input and assistance. Both were instrumental in commenting on earlier drafts.

This article is available in City University of New York Law Review: https://academicworks.cuny.edu/clr/vol18/iss2/8
WHERE ARE YOU GOING, WHERE HAVE YOU BEEN?
SERIOUSLY, LET ME SEE YOUR GPS.

CASE COMMENT: UNITED STATES V. ALVAREZ (2014)

Rajendra Persaud*

Technological advances continue to confound already dense fourth amendment jurisprudence. As modern devices become more powerful, the information stored and accessed within raises new issues that did not exist only a few decades ago. As such, new technological devices have the potential to create cases of first impression upon the courts. Recently, in U.S. v. Alvarez, Judge McAvoy ruled warrantless searches of cell phones unconstitutional in the absence of exigent circumstances or a need to protect officer safety.¹ The opinion compared cell phones to modern computers² that house a wealth of private information within³ (akin to personal

* Rajendra Persaud is a 3L at Hofstra School of Law. He would like to thank Alafair Burke, criminal law professor, for guidance throughout writing this piece and also Toni Aiello, reference librarian, for her input and assistance. Both were instrumental in commenting on earlier drafts. He can be reached at rpersa13@pride.hofstra.edu.


³ See, e.g., United States v. Mitchell, 565 F.3d 1347, 1351 (11th Cir. 2009) (explaining that computers are heavily relied upon for both personal and business use because of capabilities in storing personal letters, e-mails, financial information, passwords, family
residences\(^4\)). Thus, the smart phones were granted protection similar to computer hard drives\(^5\) and all information obtained from the seized phones was suppressed.\(^6\)

The court declined to extend this reasoning to the seized GPS device, instead comparing it to a paper map\(^7\) despite the latter’s primitive nature. The court distinguished the GPS device by reasoning that the device’s function was designed to guide a person on a trip, the information contained was easily available to the public, and the seizure was connected to the officer’s reasonable suspicion about the defendants’ presence in the area.\(^8\)

This comment addresses the oversight regarding the technological capability of the GPS device and considers implications in light of future litigation.

I. BACKGROUND OF Alvarez

Border Patrol agents observed a suspicious person standing near a convenience store entrance in Ellenburg, New York (near the Canadian border).\(^9\) Upon questioning, the individual revealed that he was a citizen of Cuba and not lawfully in the United States.\(^10\) He stated that he ventured across the border on foot.\(^11\) At the Border Patrol Station, the individual indicated that his girlfriend was scheduled to escort him to Florida in a red Honda.\(^12\) Later, the Border Patrol agents searched the area for the Honda and found it driven by two Hispanic females in the parking lot of the same convenience store.\(^13\) After briefly speaking with the women, the agents requested their presence at the Border Patrol station for further questioning.\(^14\) The initial suspect, already in custody at the station, indicated that he knew the two women and that one was, in fact, his girlfriend.\(^15\) Without consent or warrant, an agent searched a seized cell phone to

---

\(^4\) See Payton v. New York, 445 U.S. 573, 590 (1980) (“In terms that apply equally to seizures of property and to seizures of persons, the Fourth Amendment has drawn a **firm line** at the entrance to the house. Absent exigent circumstances, that threshold may not reasonably be crossed without a warrant.”) (emphasis added).

\(^5\) Id. at 18-19.

\(^6\) Id. at 10.

\(^7\) Id. at 2.

\(^8\) Id.

\(^9\) Id. at 1-2.

\(^10\) Id.

\(^11\) Id.

\(^12\) Id.

\(^13\) Id.

\(^14\) Id. at 3.

\(^15\) Id. at 4.
allegedly obtain information on the charge of alien smuggling, before examining the vehicle’s GPS device to determine what addresses were recently entered into the device (a Miami, Florida address was listed as “Home”). Both women were placed under arrest after interrogation.17

II. WARRANTLESS SEARCH JURISPRUDENTIAL OVERVIEW18

The Fourth Amendment prohibits unreasonable searches and seizures, requiring a warrant based upon probable cause.19 Courts consistently hold that determining what qualifies as a search entails a “twofold requirement, first that a person ha[s] exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as ‘reasonable.’”20

Searches conducted without warrant or consent are unreasonable per se under the Fourth Amendment with the exceptions of a few specific doctrines.21 A search incident to arrest is permissible without a warrant or consent if an officer shows that the purpose of the search is to prevent the destruction of evidence or safeguard an officer from harm.22 Brief, in-person detentions are permissible under certain circumstances. “Stop and Frisk” includes a stop to detect and prevent crime, and frisk (external pat down) to guard against concealed weapons or other potential harms that

16 Id.
17 Id. at 6.
19 U.S. CONST. AMEND. IV (“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.”); see U.S. v. Ortiz, 422 U.S. 891, 895 (1975) (“the central concern of the Fourth Amendment is to protect liberty and privacy from arbitrary and oppressive interference by government officials”); see also Illinois v. Andreas, 463 U.S. 765, 771 (1983) (“The threshold question, then, is whether an individual has a legitimate expectation of privacy in the contents of a previously lawfully searched container”); see generally United States v. Chadwick, 433 U.S. 1, 12 (1977) (discussing that a vehicle is considered an “effect” for fourth amendment considerations and is subject to the constitutional standard of reasonableness).
21 Id. at 357.
place an officer’s safety at risk.\textsuperscript{23} Evidence in “plain view” may be seized by officers who are already lawfully located on a particular premises, even if the newly discovered evidence is absent from the search warrant.\textsuperscript{24} Certain containers, as small as cigarette packages, can be examined during a search incident to arrest even if the officer is not specifically suspicious that the contents contained within are illegal, as long as the search is not conducted in an abusive or extreme manner.\textsuperscript{25} An officer may search a vehicle’s passenger compartment even if no contact is made with the arrestee until after the suspect has left vehicle, so long as the arrestee was a “recent occupant” of that vehicle.\textsuperscript{26}

To illustrate the expansion of the fourth amendment line of cases, consider a recent Supreme Court ruling. In Riley, the defendant was stopped by a police officer for driving with expired registration tags.\textsuperscript{27} After learning that Riley’s license was suspended, the officer impounded Riley’s car.\textsuperscript{28} An officer retrieved a cell phone from Riley’s pants pocket during a search incident to arrest.\textsuperscript{29} At the police station about two hours after the arrest, a detective specializing in gangs searched the phone for evidence of gang activity.\textsuperscript{30} The Court took a reasonableness approach to examine the warrantless search.\textsuperscript{31} The Court considered prior justifications for warrantless searches, finding that they were inapplicable. “Digital data stored on a cellphone cannot itself be used to harm an arresting officer or effectuate an arrestee’s escape.”\textsuperscript{32} While police officers can examine the physical exterior of the phone for harmful weapons, like a hidden razor blade, an officer may not cite physical danger as an excuse for the warrantless search of a cell phone once the phone has been secured and any potential physical threats has been eliminated.\textsuperscript{33} Likewise, preventing the destruction of evidence was inapplicable because remote wiping and data encryption were not among the officers’ suspicions.\textsuperscript{34} Remote wiping occurs when a phone receives a signal that erases stored data and data encryption occurs when a password is enabled on the device.\textsuperscript{35}
held that officers must generally secure a warrant before conducting a cell phone search.\textsuperscript{36}

\textbf{III. EXPECTATION OF PRIVACY IN THE GPS DEVICE}

The owner of a GPS device has an objective reasonable expectation of privacy because one expects others will not use the device unless authorized,\textsuperscript{37} which represents the hallmark of the right to be let alone.\textsuperscript{38} The owner’s authorization typically requires either express consent by the owner or an implied understanding that the passenger is assuming a navigational role in charting a new course for the vehicle. By its nature, the GPS device is not used for purposes other than navigation.\textsuperscript{39}

Similarly, the owner has a subjective expectation of privacy in assuming an officer will not remove the device from its location in the vehicle, turn it on, and rummage through its contents without consent or a warrant.\textsuperscript{40} In \textit{Alvarez}, Judge McAvoy ruled against the defendants’ attempt to suppress

\textsuperscript{36}Id. at 2485.

\textsuperscript{37}See State v. Rupnick, 125 P.3d 541, 559 (2005) (justifying the Fourth Amendment requirement of a warrant to search a computer’s contents premised on a computer owner’s reasonable expectation of privacy in the information stored within the hard drive); \textit{cf.} People v. Moorer, 959 N.Y.S.2d 868, 881 (N.Y. Cnty. Ct. 2013) (“People are not so oblivious that they are not aware that cell phones purchased today come with GPS technology which can pinpoint the location of the phone at any given time so long as it is turned on and the GPS technology has not been deactivated or disabled. That technology also enables a person to be mobile and have constant access to and use of his cell phone. By a person’s voluntary utilization, through GPS technology, of a cell phone, a person necessarily has no reasonable expectation of privacy with respect to the phone’s location—vis a vis the pinging—even though he maintains what may be a reasonable expectation of privacy in the content of his phone conversations.”); \textit{but see} United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012) (holding that a suspect had no reasonable expectation of privacy in the data given off by his voluntarily procured prepaid cell phone by positing that if a tool used to transport contraband emits a traceable signal, then police may track it).

\textsuperscript{38}Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) (“The right to be let alone—the most comprehensive of rights and the right most valued by civilized men”).


\textsuperscript{40}See State v. Granville, PD-1095-12, 2014 WL 714730, at *3 n.16-17 (Tex. Crim. App. Feb. 26, 2014) (“Courts have held that (1) a person has a subjective expectation of privacy in the contents of his cell phone, and (2) this expectation of privacy is one that society recognizes as reasonable and legitimate”), \textit{available at} https://www.eff.org/files/2014/02/27/granville_majority.pdf.
WHERE ARE YOU GOING, WHERE HAVE YOU BEEN?

information located within a GPS device. In so ruling, the Judge compared the information available within the GPS device to information available in a paper map in the front seat of a car. In stark contrast to this reasoning, a GPS device is actually the functional equivalent to a limited subject matter hard drive, conveying specific geographical information via satellite.

GPS devices provide technological support far beyond that which any paper map can provide. The words behind the acronym GPS are “Global Positioning System,” which reflects the device’s capability to triangulate positions using satellites. GPS devices are far more intricate than paper maps because a GPS device user need only push a button to determine his or her place in the world or create a complex route to a new destination. GPS devices employ real-time technology to track the vehicle’s location in relation to its destination. This technology enables the device to reroute a driver who has gone awry and provide proximal destinations according to the driver’s actual location and intended destination. These features illustrate the wide array of uses available through most GPS devices, but not paper maps.

Unlike traditional maps, GPS devices are capable of geographical triangulation and storing previous locations for future access. This storage capacity creates a log of the driver’s whereabouts otherwise unavailable if one were consulting a paper map. The paper map comparison is tenuous because modern GPS devices harness satellite technology in a manner maps are not designed to and cannot be capable of utilizing.

The owner of a GPS device possesses a privacy interest in the device and its contents. Cell phones contain sensitive information, ranging from stored financial data to revealing photographs. The Court should consider

---

41 Stashenko, supra note 2.
42 Alvarez, supra note 2, at 10.
45 Xu, supra note 44, at 1.
47 Daniels, supra note 47, at 3; Bogens, supra note 47, at 5.3-5.8.
48 Adam Levin, The 10 Dumbest Risks People Take with their Smartphones,
that similarly sensitive information is included in a GPS device, although limited to geographical data, including home addresses, addresses of friends, businesses, acquaintances, and family members, and other private destinations. A person that does not consent to a search should be protected from an unreasonable invasion of privacy in his or her GPS device. Like a hard drive, the GPS device stores a wealth of information regarding where the individual has previously traveled to, where the individual now is, and even maintains the potential for conveying where the individual plans to travel. The significant difference between a cell phone and GPS device is simply that GPS devices are limited to geographical information. Both devices possess sensitive and personal information that should be afforded privacy protection. The scope of information available in a computer or cell phone hard drive is wide-ranging, while the GPS device is limited to geographic information either entered by the user or suggested by the device itself. While the implications appear lesser in the GPS context because the information available is limited to geographical substance, the evidence obtained could be proof of criminal culpability and should be treated with this concern in mind.

IV. Plain View

The plain view doctrine permits a law enforcement officer to seize evidence beyond the scope of the warrant when criminality is immediately apparent and where the search and seizure does not invade privacy. The ability to store locations within the GPS device is a common feature amongst many GPS devices on the market today. See, e.g., SONY, Nav-U Instruction Manual 15 (2008), available at https://docs.sony.com/release/NVU73T_83T_EN.pdf.

See United States v. Galpin, 720 F.3d 436, 447 (2d Cir. 2013) (“The potential for privacy violations occasioned by an unbridled, exploratory search of a hard drive is enormous. This threat is compounded by the nature of digital storage.”).

“A search is a search, even if it happens to disclose nothing but the bottom of a turntable.” Hicks, 480 U.S. at 325 (1987) (Scalia, J.) (emphasis added); see also U.S. v. Ortiz, 422 U.S. 891, 896 (1975) (“A search, even of an automobile, is a substantial invasion of privacy.”).

United States v. George, 975 F.2d 72, 78 (2d Cir. 1992); Horton v. California, 496 U.S. 128, 133 (1990) (“The “plain-view” doctrine is often considered an exception to the general rule that warrantless searches are presumptively unreasonable, but this characterization overlooks the important difference between searches and seizures. If an article is already in plain view, neither its observation nor its seizure would involve any invasion of privacy”); United States v. Corral, 970 F.2d 719, 723 (9th Cir. 1992) (“A plain view seizure of incriminating evidence is sustainable if (i) the police officer is lawfully located in a place from which the item can plainly be seen; (ii) the officer has a lawful right of access to the item itself; and (iii) it is “immediately apparent” that the seized item is
plain view doctrine should not apply to GPS devices.

A GPS device, like any hard drive, conveys no detail of criminality in plain view. Unlike a cell phone, which may convey basic information from the home screen or the phone case, accessing a GPS log requires manipulation of the device. When powered on, the device has the potential to display where the user is traveling to and where the user actually is located. When powered off, the device is clearly not helpful.

Rather, discovering anything useful to establish culpability requires something more. In the hard drive context, discovery requires performing searches, accessing previously inaccessible files, opening documents, and conducting other computer-related inquiries. While an officer generally has authority to seize incriminating evidence in plain view if he or she has prior justification for the intrusion, the evidence embedded in the GPS device is unknown until the device is powered on and one searches through its stored locations (with the singular exception of information displayed by the device if it is routing a driver to a specified location). Thus, the listings of previously traveled destinations amounting to geographic evidence obtained from a GPS device can almost never be discovered inadvertently. Searching a computer or GPS device requires a virtually indistinguishable process: scouring digital media to obtain incriminating virtual evidence.

---

53 United States v. Wurie, 728 F.3d 1, 2 (1st Cir. 2013) aff’d Riley, 134 S.Ct. 2473 (2014) (officers saw the cell phone’s caller ID screen and the “my house” label, in plain view, but had to open the phone to view Wurie’s call log).

54 For examples of what constitutes “something more,” see Ariz. v. Hicks, 480 U.S. 321, 324-25 (1987) (holding that the manipulation of equipment is unquestionably a separate search apart from the lawful and reasonable search for the shooter, victims, or weapons that were the lawful objective of the officer’s entry into the apartment); see also Bond v. United States, 529 U.S. 334, 336 (2000) (holding that an officer’s physical manipulation of a bus passenger’s bag violated his reasonable expectation of privacy because the inspection was more intrusive than purely visual inspection).

55 The court in Galpin discussed whether the plain view doctrine applied in a case where a computer forensics analyst inadvertently observed images of child pornography after learning that the defendant accessed certain websites, knew there might be photos indicating same, and also knew that storage media might contain names and images of victims. The Court remanded for a determination on whether a search limited to evidence of a registration violation necessitates opening image and video files. Galpin, supra note 51, at 444.

56 Coolidge, supra note 25, at 466; Horton, supra note 53, at 135.

57 Cf. United States v. Otero, 563 F.3d 1127, 1132 (10th Cir. 2009) (“The modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the (warrant) particularity requirement that much more important.”).
V. The Search Incident to Arrest Context

Absent a warrant, police officers must have some other justification to conduct a reasonable search; one such exception is the search incident to arrest doctrine.\(^5\) This doctrine normally implicates officer safety or evidence preservation rationales;\(^6\) however neither safety nor evidence apply in *Alvarez* because these defendants were not in the vehicle when the border patrol agents approached and did not pose a threat.\(^7\)

The United States Court of Appeals for the First Circuit in *Wurie*\(^8\) decided the warrantless search of a suspect’s flip cell phone in the search incident to arrest context.\(^9\) That court held that although searching the suspect’s call log was less invasive than searching text messages, emails, or photographs, the search incident to arrest exception does not authorize the warrantless search of data on a cell phone seized from an arrestee’s person.\(^10\) Notwithstanding the need to preserve information from the call log that may be overridden by new calls or intentionally deleted, the court noted that the phone could be shut off, placed in a Faraday enclosure,\(^11\) the battery removed, or the contents mirrored to prevent technical wiping.\(^12\)

While the warrantless search of cell phones is unconstitutional without a

---

\(^5\) Arizona v. Gant, 556 U.S. 332, 338 (2009) (concluding that circumstances involving automobiles justify a search incident to arrest when it is reasonable to believe evidence may be contained within the vehicle); *Chimel*, 395 U.S. at 762-63, 767-68 (holding that when an object that comes into view during a search incident to arrest and is appropriately limited in scope, it may be seized without a warrant).

\(^6\) See *Robinson*, 414 U.S. at 234 (“The justification or reason for the authority to search incident to a lawful arrest rests quite as much on the need to disarm the suspect in order to take him into custody as it does on the need to preserve evidence on his person for later use at trial.”)


\(^8\) Affirmed by a unanimous Supreme Court, *see Riley v. California*, 573 U.S. 2473, 2479 (2014).

\(^9\) *Wurie*, 728 F.3d at 15 (Howard, J., dissenting).

\(^10\) *Id.* at 13.

\(^11\) See *Physical Evidence Bulletin*, BUREAU FORENSIC SERVS., http://oag.ca.gov/sites/all/files/pdfs/cci/reference/peb_18.pdf (last visited Nov. 25, 2014) (directing officers to preserve digital evidence when a device is powered on by switching the device to “Airplane Mode” and placing it in a Faraday bag, which blocks wireless signals to the device thereby preventing the reception of calls and text messages while preserving the contents of the device without further manipulation); A faraday cage is a hollow enclosure of conducting material that is capable of blocking wave signals into and out of the enclosure. Calling a cell phone within the bag will result in immediately hearing a voicemail message. It is like an impenetrable prison for whatever the cage withholds. An example of a faraday cage is an anti-static bag, which can be purchased online for less than a dollar per unit online. Matthew French, *Mobile Phone Faraday Cage* (Nov. 25, 2014), http://arxiv.org/pdf/1112.5495.pdf.

\(^12\) *Wurie*, 728 F.3d at 11.
specific showing of exigent circumstances to search the phone immediately, like the imminent destruction of evidence located within, this reasoning must now also be extended to GPS devices.

Under the circumstances of *Alvarez*, there are no time, safety, or preservation arguments that justify the officer’s search of the GPS device without a warrant. A GPS device can be placed in a Faraday enclosure the same way that a cell phone can. Furthermore, the comparison to paper maps fails to properly characterize the GPS device in a manner that reflects its technological capabilities. GPS devices do not implicate the same privacy concerns that other courts discussed because the device’s subject matter content is reserved exclusively to geography. However, this limited subject matter should not preclude protection for the information contained within these devices because the user still maintains an expectation of privacy; the exceptions to the warrant requirement must justify the officer’s actions in accordance with the device.

VI. FUTURE CONSIDERATIONS

Today, most people with smart phones have access to GPS devices. Thus, the Supreme Court will inevitably confront the constitutionality issue of searching and seizing GPS devices, whether in the GPS device itself or as a collateral matter related GPS technology and cell phone searches.

There is a distinction between attaching a GPS device to a vehicle to track its future whereabouts and obtaining a GPS device from a vehicle and searching its contents for previously traveled to destinations. The Supreme Court held in *Jones* that attaching a GPS device to a vehicle, then monitoring its movements on public streets constitutes a search under the fourth amendment. The Supreme Court did not address whether an officer is permitted to freely search a GPS device located within a suspect’s vehicle.

Future GPS technology will expand to newer devices. The distinction between a GPS device and a paper map lies in the ability to manipulate the GPS device to seek previously traveled to destinations, stored addresses, or even a current route programmed to a future destination. The GPS device certainly contains more information than an ordinary paper map, but the GPS device is limited in ways that a modern smart phone is not. While the illustrated complexity of the GPS device should defeat the paper map analogy, what remains unclear is whether a GPS device should be given the same treatment as a computer. Courts afford more protection to computers

---

68 Smith, supra note 14, at “Summary.”
because of the quantity and variety of information stored. The Supreme Court in Riley acknowledged that modern smart phones are themselves minicomputers that harness the abilities of a multitude of devices including, but not limited to cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, newspapers, and, of course, a telephone. Viewing GPS data on a cell phone has the potential to implicate other data within the phone, considering cell phone users operate their smart phones like personal computers. GPS software is already available within applications on smart phones, embedded within watches, and pre-installed within many technologically savvy automobiles.

---

69 See, e.g., United States v. Carey, 172 F.3d 1268, 1275 (10th Cir. 1999) (hesitating to oversimplify fourth amendment doctrines in light of the realities of massive modern computer storage); see also Raphael Winick, Searches and Seizures of Computers and Computer Data, 8 HARV. J.L. & TECH. 75, 104 (1994) (“Since electronic storage is likely to contain a greater quantity and variety of information than any previous storage method, computers make tempting targets in searches for incriminating information.”).

70 Riley, supra note 28, at 2489.

71 Pew Research Center, Cell Phone Activities 2012: Photo Taking, Texting, and Accessing the Internet are the Most Popular Activities People Pursue with their Mobile Phones, 4-10 (2012) (charting the variety of uses that cell phone users engage in beyond just making calls), available at pewinternet.org/files/old-media/Files/Reports/2012/PIP_CellActivities_11.25.pdf.


73 See, e.g., TOMTOM, NIKER SPORTWATCH GPS, INSTRUCTIONAL MANUAL 20, available at http://www.tomtom.com/lib/doc/Nike-SportWatch-QuickStartGuide-EN.pdf (explaining how the watch’s history stores up to fifty of the user’s most recent runs and orders the events chronologically).

While similar cases involve searching a user’s cell phone, the Court must not limit its holding, but consider devices with similar capabilities including, but not limited to GPS devices, tablets, cell phones, and even mobile gaming consoles with internet access and storage functions. Rather, GPS data and smart phone technologies should be treated as corollary issues to resolve future disputes. Failing to delineate between GPS software and the devices themselves will give rise to inevitable litigation regarding the type of information accessed and whether the user possesses a reasonable expectation of privacy in the searched information.

* * *