# *U.S. v. Jones*: Inadequate to Promote Privacy for Citizens and Efficiency for Law Enforcement

Vikram Iyengar*



## I. INTRODUCTION

Five members of the Supreme Court held that when the government installed a Global Positioning System (GPS) device on Antoine Jones's car and used that GPS to monitor the vehicle's movements, it conducted a Fourth Amendment search.[1] Justice Antonin Scalia delivered the majority opinion, which declared that by installing the GPS, the government trespassed on Jones's property for the purpose of obtaining information.[2] Although the Court unanimously agreed on the judgment, Justice Samuel Alito argued that the government conducted a Fourth Amendment search by long-term GPS monitoring only because it

* The author thanks Professor Elizabeth Magill, Richard E. Lang Professor of Law and Dean of Stanford Law School, and Professor David Ball, Assistant Professor at the Santa Clara University School of Law, for introducing me to Constitutional and Criminal Law. The author also thanks Professor George Fisher, Judge John Crown Professor of Law at Stanford Law School, for his helpful comments on a previous version of this Note. Finally, the author is grateful to the board and editors of the *California Law Review* for their help in selecting and providing the research sources used in this Note.

[1] United States v. Jones, 132 S. Ct. 945, 947, 949 (2012).

[2] *Id.*

violated Jones's reasonable expectation of privacy (REOP).[3] Justice Sonya Sotomayor agreed with Justice Alito's argument regarding Jones's REOP, foreseeing the dangers of technology's encroachment upon privacy;[4] however, she joined the majority holding on the issue of trespass.[5]

This Note considers the trespass and REOP doctrines—part of Fourth Amendment jurisprudence—and argues that because the Scalia majority focused on physical trespass and did not insist on addressing whether the government violated Jones's REOP, the opinion is unduly narrow, unclear, and inadequate to protect citizens from unconstitutional government intrusions upon their persons and effects, arising from future technologies.

## II. REVIEWING *U.S. V. JONES*

In 2004, law enforcement began investigating Jones for narcotics violations.[6] The government installed a GPS on Jones's car without a valid warrant and tracked his movements twenty-four hours a day for four weeks.[7] In 2008, based on the GPS evidence, Jones was sentenced to life in prison for conspiracy to distribute cocaine.[8] In 2010, the D.C. Circuit overturned Jones's conviction, holding that the police unreasonably searched Jones because the search—conducted without a warrant—violated his REOP.[9] In 2011, the Supreme Court granted certiorari to resolve, in part, whether warrantless use of the GPS on public streets violated the Fourth Amendment.[10]

Because the Fourth Amendment proclaims "[t]he right of the people to be secure in their . . . effects,"[11] and the intrusion of the GPS would have been considered a search of an "effect" at the time of the amendment's adoption,[12] the majority held that it was a search.[13] In support, Justice Scalia cited a line of cases dating back to 1765, in which Fourth Amendment protections were based on physical intrusion on private property.[14]

---

[3] *Id.* at 958, 964 (Alito, J., concurring).

[4] *Id.* at 955–56 (Sotomayor, J., concurring) (citing Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that the use of a thermal imaging device was a search even in the absence of a trespass)).

[5] *Id.* at 954–55.

[6] *Id.* at 948 (majority opinion).

[7] *Id.*

[8] *Id.* at 948–49.

[9] United States v. Maynard, 615 F.3d 544, 563–67 (D.C. Cir. 2010), *aff'd in part sub nom.* United States v. Jones, 132 S. Ct. 945 (2012).

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

[11] U.S. CONST. amend IV.

[12] *Jones*, 132 S. Ct. at 949 (citing United States v. Chadwick, 433 U.S. 1, 12 (1977)).

[13] *Id.*

[14] *See id.* at 949–51 (citing various cases, including Entick v. Carrington, (1765) 95 Eng. Rep. 807 (K.B.) (discussing the relevance of property rights when analyzing search and seizure); Soldal v.

The majority conceded that in the 1967 case *Katz v. United States*,[15] the Supreme Court stated that the "'Fourth Amendment protects people, not places.'"[16] The majority further noted that the REOP test—providing that a violation occurs when a search intrudes upon a person's reasonable expectation of privacy—was first articulated by Justice Harlan in his concurrence in *Katz*.[17] However, the majority explained that *Katz* did not abandon the trespass theory, and that the Fourth Amendment continues to protect the enumerated areas ("persons, houses, papers, and effects") from trespass by the government.[18] In his concurrence, Justice Alito criticized the majority for relying on two post-*Katz* cases to demonstrate that "a technical trespass is sufficient to establish the existence of a search."[19] Responding to the concurrence, Justice Scalia declared that courts must guarantee a minimum level of Fourth Amendment protection from physical trespass, while considering expectations of privacy only in the absence of trespass.[20]

In concurring, Justice Alito stated that he would have decided the issue by applying the REOP test and "by asking whether [Jones'] reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[21] Justice Alito argued that a physical trespass was "neither necessary nor sufficient to establish a constitutional violation" under the REOP test.[22] Attaching the GPS could not be a search because "if the device had not functioned or if the officers had not used it, no information would have been obtained."[23] The warrantless use of the GPS was a violation of *Katz*'s REOP test (and was therefore considered a search) only because a twenty-eight day surveillance without a GPS would be exceptionally demanding and society would not expect such a search to be conducted.[24] However, Justice Alito also cited *United States v. Knotts*[25] and stated that short-term monitoring on public streets likely accords with society's REOP and is not a search.[26]

While Justice Sotomayor concurred that *Katz* "augmented, but did

---

Cook Cnty., 506 U.S. 56, 65–67 (1992) (holding that physically taking a trailer was a seizure even without an invasion of privacy)).

[15] 389 U.S. 347 (1967) (holding that electronic eavesdropping in a public telephone booth, where the electronic device did not penetrate the wall, is a search).

[16] *Jones*, 132 S. Ct. at 950 (quoting *Katz*, 389 U.S. at 351).

[17] *Id.* (citing *Katz*, 389 U.S. at 360 (Harlan, J., concurring)).

[18] *Id.* at 950–51 (citing Alderman v. United States, 394 U.S. 165, 176, 180 (1969)).

[19] *Id.* at 960–61 (Alito, J., concurring) (referring to the majority's reliance on *Soldal*, 506 U.S. 56 and *Alderman*, 394 U.S. 165).

[20] *Id.* at 953 (majority opinion).

[21] *Id.* at 958 (Alito, J., concurring).

[22] *Id.* at 960 (quoting United States v. Karo, 468 U.S. 705, 713 (1984) (emphasis and internal quotation marks omitted)).

[23] *Id.* at 958.

[24] *Id.* at 964.

[25] 460 U.S. 276 (1983) (holding that tracking a beeper in a car on a day-trip on public roads is not a search).

[26] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

not displace" the trespass test, she disagreed with Justice Alito's approach, which she considered to "discount[] altogether the constitutional relevance of the Government's physical intrusion on Jones' [vehicle]."[27] However, she echoed Justice Alito's concern that the trespass doctrine is complicated by the fact that many forms of surveillance using modern technology can be carried out without physical intrusion.[28] Furthermore, she questioned the constitutionality of even short-term GPS surveillance that is capable of constructing a record of an individual's "familial, political, professional, religious, and sexual associations."[29] She explained that such GPS surveillance "evades the ordinary checks that constrain abusive law enforcement practices"; the surveillance is relatively inexpensive, covert, and can record and store data that the government can review far into the future in search of information about trips to private destinations, such as "the abortion clinic, the AIDs treatment center, the strip club, the criminal defense attorney," and so on.[30]

While the majority did affirm *Kyllo v. United States*[31] (which held that sense-enhancing technology used to gather information otherwise unobtainable though ordinary senses is a search even in the absence of a trespass),[32] *Jones* is unduly narrow because it based its ruling only on the government's minor trespass.[33] And though at least five justices would find that a search had occurred in a situation involving the same intrusion on the REOP but without involving trespass,[34] future litigation will be necessary to determine the permissibility of warrantless tracking of factory-installed GPS and smartphones in the absence of trespass.[35] Moreover, the *Jones* analysis is insufficient to protect citizens from intermittent, short-term government monitoring that could be used to put together a profile of a citizen's everyday life.[36] Consumers who voluntarily but unwittingly use social tools, such as "phone-location-tracking services," that allow persons "to find (or to avoid) others who

---

[27] *Id.* at 955 (Sotomayor, J., concurring).
[28] *Id.*
[29] *Id.*
[30] *Id.* at 955–56 (quoting People v. Weaver, 12 N.Y.3d 433, 441–42 (2009)).
[31] 533 U.S. 27 (2001).
[32] *Id.* at 40.
[33] *See Jones*, 132 S. Ct. at 961 (Alito, J., concurring) (stating that the majority "attaches great significance" to the trespass at issue—attaching a small object to the bottom of a car without interfering with the car's operations—"that most would view as relatively minor").
[34] The five concurring justices were Justices Sotomayor, Alito, Ginsburg, Breyer, and Kagan. *Id.* at 954, 957. Justices Ginsburg, Breyer, and Kagan joined Justice Alito's concurring opinion. *Id.* at 957.
[35] *See Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (noting that "[w]ith increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones"); *see also* Renee M. Hutchins, *Tied up in Knotts? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 432–33 (2007) (discussing the difference between types of monitoring under new technologies).
[36] *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (noting that "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable"); *see also* United States v. Knotts, 460 U.S. 276, 281–82 (1983) (holding that tracking a beeper in a car on a day-trip on public roads is not a search).

enroll in these services"[37] and wearable cameras such as Google Glass,[38] may be especially at risk.[39]

## III. FOURTH AMENDMENT JURISPRUDENCE BEFORE *JONES*

The Supreme Court has analyzed law enforcement's use of sense-enhancing aids under the Fourth Amendment thirty times[40] since *Olmstead v. United States*,[41] in which wires were inserted along the telephone lines from the suspect's house without trespass.[42] The Court held that the wiretap was not a search because evidence was secured only by "hearing" and there was no trespass.[43] However, in *Katz*, the Court announced a radical departure from *Olmstead* by considering immaterial intrusion using technology sufficient to constitute a search.[44] In *Katz*, the FBI placed a bug on top of a telephone booth and recorded Katz's conversations.[45] The Court held that the fact that the bug did not penetrate the booth had "no constitutional significance," and that the Fourth Amendment extends not only the seizure of property, but also to "oral statements overheard without any technical trespass."[46] Justice Harlan's concurrence created a two-part test that defined the requirements for protection: (1) an exhibition of a subjective "expectation of privacy," and (2) the expectation being objectively "reasonable."[47] Under this test, intercepting Katz's conversations without a warrant was "presumptively unreasonable" because Katz expected his conversations to be conducted in private and because society would consider his expectation of privacy reasonable.[48]

In 1979, the *Katz* test made a reappearance in *Smith v. Maryland*,[49] where it was applied to determine whether a telephone company's use of

---

[37] *Jones*, 132 S. Ct. at 963 (Alito, J., concurring).

[38] *See generally Google Glass*, GOOGLE, http://www.google.com/glass/start, <http://perma.cc/D8QK-JRVX>. Google Glass, made by Google, is a wearable, optical head-mounted display that includes features such as giving directions, taking photographs, and supplying facts about the wearer's surroundings and location. *Id.*; *see also* Amir Efrati, *Google Glass Privacy Worries Lawmakers*, WALL ST. J., May 16, 2013, http://online.wsj.com/news/articles/SB10001424127887324767004578487661143483672, <http://perma.cc/RU2F-SRHN> (describing the product).

[39] *See* Hutchins, *supra* note 35, at 410–11 (stating that technological advancements create electronic trails that may reduce privacy).

[40] *Id.* at 423. For a discussion of sense-enhancing aids such as spike mikes, thermal imagers, and drug-sniffing dogs, *see id.* at 423 n.76.

[41] 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967)

[42] *Id.* at 456–57.

[43] *Id.* at 464.

[44] *Katz*, 389 U.S. at 359.

[45] *Id.* at 348.

[46] *Id.* at 353 (internal quotation marks omitted).

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

[48] *Id.*

[49] 442 U.S. 735 (1979).

a pen register[50] to record numbers dialed by the suspect constituted a search.[51] The Court held that a search did not take place because the suspect "voluntarily conveyed . . . information to the telephone company" and because similar devices were routinely used for billing.[52] Moreover, the majority asserted that the suspect had "assumed the risk" of disclosure and therefore had no REOP.[53] Such a troubling notion could be problematic as applied to future technologies where assumptions of risk may be unwitting and involuntary.[54]

Both the majority and Justice Alito's concurrence in *Jones* cited the application of the *Katz* test in *Knotts*, albeit for different reasons.[55] In *Knotts*, the police placed a transmitting beeper within a drum of chloroform purchased by the suspect and used the beeper signal to follow his car during a single trip.[56] The Court ruled that the suspect had no REOP traveling in an automobile on public roadways and had "voluntarily conveyed" his location because the public could observe him and gather information about his route, destination, and any stops.[57] In *Jones*, Justice Scalia cited *Knotts* in support of the assertion that "mere visual observation does not constitute a search."[58] In contrast, Justice Alito's concurrence cited it as proof that *Jones* should have been decided under *Katz*, since *Knotts* turned on whether the suspect's REOP had been violated, regardless of trespass.[59] *Knotts* may well be the reason why the *Jones* analysis will prove inadequate in the future because the assumption underlying the *Knotts* decision—that visual information can be voluntarily conveyed—may hand the government a free license to use social media tools for intrusion on citizens.

More recently, in *Kyllo*, the Court re-affirmed *Katz* and strengthened protections for private homes by creating a "firm" line at a home's entrance.[60] In *Kyllo*, the government used a thermal imager (which did not penetrate the suspect's house) to measure heat from the roof and walls, which generated evidence that the suspect was growing marijuana indoors.[61] The majority described the core of the Fourth Amendment being "the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion."[62] Therefore,

---

[50] A pen register is a device that collects the telephone numbers of outbound phone calls made on a monitored phone line. 18 U.S.C. § 3127(3) (2012).

[51] *Smith*, 442 U.S. at 736.

[52] *Id.* at 744.

[53] *Id.* (internal quotation marks omitted).

[54] *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (discussing individuals' expectation of privacy with respect to the information they share through digital media).

[55] *Id.* at 953 (majority opinion); *id.* at 958, 964 (Alito, J., concurring) (stating that short-term GPS monitoring accords with REOP).

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

[57] *Id.* at 281, 284–85.

[58] *Jones*, 132 S. Ct. at 953.

[59] *Id.* at 958, 964 (Alito, J., concurring).

[60] Kyllo v. United States, 533 U.S. 27, 40 (2001).

[61] *Id.* at 29–30.

[62] *Id.* at 31 (quoting Silverman v. United States, 365 U.S. 505, 511 (1961)) (internal quotation marks

when a device that is "not in general public use" is employed to "explore details of [a] home that would previously have been unknowable without physical intrusion, the surveillance is a search."[63] The dissent criticized the majority's "unknowable without physical intrusion" requirement, arguing that it incorrectly equated "the mental process of analyzing data" with "a physical intrusion."[64] However, that argument is unpersuasive; information from inferences and mental processes may be readily available without physical intrusion, and remain free to be used under *Kyllo*. However, the majority's opinion is prone to uncertainty under future technologies such as social media that *are* in general public use.

To support the trespass theory in *Jones*, instead of using the prevailing Fourth Amendment jurisprudence, Justice Scalia first relied upon *Olmstead*, which held that no search occurred where wiretaps were attached to wires on public streets but did not enter the suspects' houses or offices.[65] However, that rule has been criticized, notably by Justice Brandeis's dissent in *Olmstead*, which claimed that the location of the "physical connection with the telephone wires" was immaterial, and that the Fourth Amendment instead prohibited "unjustifiable intrusion by the government upon the privacy of the individual."[66] In diluting the protections of *Katz* by relying on *Olmstead*, *Jones* therefore lays bare the privacy of citizens under new technologies that do not require trespass.[67]

Secondly, the *Jones* majority used *Alderman v. United States*[68] to claim that the Fourth Amendment turns on trespass, because *Alderman* held that conversations between two persons obtained by "warrantless placement of electronic surveillance devices in their homes" cannot be used as evidence even against a *third* person.[69] However, *Alderman* has been routinely cited to support the proposition that property rights only reflect society's recognition of REOP, which is what determines the parameters of a search.[70] Therefore, *Alderman* provides little support for the majority's theory.

Finally, Justice Scalia based his trespass argument on *Soldal v. Cook County*,[71] in which the Court held that a seizure of a mobile home implicated the Fourth Amendment even without an invasion of privacy.[72]

---

omitted).

[63] *Id.* at 40 (internal quotation marks omitted).

[64] *Id.* at 49 (Stevens, J., dissenting).

[65] United States v. Jones, 132 S. Ct. 945, 950 (2012) (citing Olmstead v. United States, 277 U.S. 438, 464 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967)).

[66] *Olmstead*, 277 U.S. at 478, 479 (Brandeis, J., dissenting).

[67] *See Jones*, 132 S. Ct. at 959 (Alito, J., concurring) (discussing the lack of protection provided by *Olmstead*'s focus on physical trespass rather than on the extent of the intimate details uncovered by the intrusion).

[68] 394 U.S. 165 (1969).

[69] *Jones*, 132 S. Ct. at 950 (citing Alderman v. United States, 394 U.S. 165, 176 (1969)).

[70] United States v. Karo, 468 U.S. 705, 732 n.7 (1984) (Stevens, J., concurring in part and dissenting in part).

[71] 506 U.S. 56 (1992).

[72] *Jones*, 132 S. Ct. at 951 (citing Soldal v. Cook Cnty., 506 U.S. 56, 60–62 (1992)).

However, as Justice Alito pointed out, *Jones* did not involve a seizure, but a search—a relevant distinction;[73] therefore, *Soldal*, like *Olmstead* and *Alderman*, is an inadequate basis for the holding in *Jones*. Justice Alito further explained that because Fourth Amendment jurisprudence at the time *Jones* was decided was firmly centered on the *Katz* REOP test,[74] *Jones* is not in harmony "with a substantial body of existing case law."[75]

## IV. *JONES* MUDDIES FOURTH AMENDMENT PROTECTIONS FOR THE FUTURE

In this Part, this Note examines the *Jones* ruling, its potential impact on future legislation, and most importantly, its soundness in terms of public policy from the viewpoint of three emerging technologies that are poised to become the basis for future government intrusion into citizens' privacy: (1) non-trespassory location monitoring; (2) ubiquitous-presence technologies; and (3) intermittent-monitoring technologies.

### A. Non-Trespassory Location Monitoring

Tracking using factory- and owner-installed automotive GPS and smartphones involves no trespass. In fact, "[a] large industry exists around automotive 'telematics:'" "'voice and data communication between vehicles and information service providers'" (ISPs) that can record vehicles' locations.[76] The use of GPS devices has become increasingly common: several companies today market GPS tracking devices to parents of teenage drivers, the FTC requires all cell phones post-2002 to enable GPS tracking, and transponders for automated toll systems have associated tracking data.[77] With the ease presented by database connectivity, the government could *potentially* ask an ISP to track individuals or groups of individuals based on certain characteristics.[78] Therefore, the *Jones* majority's "reliance on the law of

---

[73] *Id.* at 960 (Alito, J., concurring).

[74] *Id.* at 959–60.

[75] *Id.* at 961.

[76] John S. Ganz, Note, *It's Already Public: Why Federal Officers Should Not Need Warrants to Use GPS Vehicle Tracking Devices*, 95 J. CRIM. L. & CRIMINOLOGY 1326, 1343 (2004).

[77] *Id.* at 1344, 1345–47 (describing new technologies used for tracking).

[78] For example, consider the implications of the government requesting data associated with all registered democrats or consumers by ethnicity (using last names).

Under the current law, the government can only request particularized information about specific individuals, unless it is sweeping up information on foreign communications. *See generally* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended in scattered sections of 18 & 50 U.S.C.). *See also* Cyber Intelligence Sharing and Protection Act, H.R. 624, 113th Cong. (1st Sess. 2013) (providing for the "sharing of certain cyber threat intelligence and

trespass will present particularly vexing problems" in the future by leaving the rules unclear for technologies that do not involve "physical touching."[79]

Moreover, by relying on and affirming the *Knotts* holding that there is no REOP when location information has been voluntarily conveyed to the public,[80] Justice Scalia left the question open of whether GPS data conveyed to car manufacturers, ISPs, and tow-trucks is protected. While four of the concurring justices in *Jones* did narrow *Knotts*' rule that there is no REOP on public streets,[81] and would likely rule against the government in a case identical to *Jones* but without trespass, future cases will require only one additional vote to hold that warrantless monitoring by factory-installed GPS and smartphones is constitutional.

However, as Justice Alito noted, simply relying on *Katz* may also be insufficient to draw clear constitutional boundaries for the government.[82] A person's expectation of privacy, what society considers reasonable, and what judges think privacy should be can change with technology.[83] Consider a location service system like OnStar, which General Motors (GM) has sought to make standard on its cars and

---

cyber threat information between the intelligence community and cybersecurity entities," among other purposes, CISPA was passed in the House of Representatives but stalled in the Senate Select Committee on Intelligence); Gerry Smith, *Senate Won't Vote on CISPA, Deals Blow to Controversial Cyber Bill*, HUFFINGTON POST, Apr. 25, 2013, http://www.huffingtonpost.com/2013/04/25/cispa-cyber-bill_n_3158221.html, <http://perma.cc/QZ88-HRH6> (stating that the Senate is unlikely to vote on CISPA and discussing the bill's controversial nature due to the broad data that it seeks to make available to government agencies).

However, intercepting foreign communications only requires that one party to the communication is foreign, and therefore large amounts of data about U.S. persons are subject to collection by the government. *See* Spencer Ackerman & James Ball, *NSA Performed Warrantless Searches on Americans' Calls and Emails—Clapper*, GUARDIAN, Apr. 1, 2014, http://www.theguardian.com/world/2014/apr/01/nsa-surveillance-loophole-americans-data, <http://perma.cc/A3VT-2622>; Transcript of Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Mar. 19, 2014), *available at* http://www.pclob.gov/Library/Meetings-Events/2014-March-19-Public-Hearing/19-March-2014_Public_Hearing_Transcript.pdf, <http://perma.cc/74BM-466W> (recording the investigation of the Privacy and Civil Liberties Board into the government's use of Section 702).

Under the authority of PATRIOT Act § 215, the NSA has been collecting "nearly all call detail records generated by certain telephone companies" of Americans—metadata which includes some location information. PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014), *available at* http://www.fas.org/irp/offdocs/pclob-215.pdf, <http://perma.cc/W84J-XLYN> (noting that, although cell phone companies remove cell site location information from records before transmitting to the NSA, the metadata can contain some "indication of a caller's geographic location," including the identifier that pinpoints the segment of the communication line connecting two callers). *But see* Mark Hosenball & Alina Selyukh, *Obama's NSA Overhaul May Require Phone Carriers to Store More Data*, REUTERS, Apr. 3, 2014, http://uk.reuters.com/article/2014/04/03/us-usa-security-obama-idUKBREA3228O20140403, <http://perma.cc/EW9M-4DML> (noting President Obama's proposal to reform the NSA phone records collection program).

[79] *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

[80] *Id.* at 951–52 (majority opinion) (citing United States v. Knotts, 460 U.S. 276, 281–82 (1983)).

[81] *See id.* at 964 (Alito, J., concurring) ("[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy"). The four Justices joining the opinion were Justices Ginsburg, Breyer, and Kagan. *Id.*at 957.

[82] *Id.* at 962.

[83] *Id.*

trucks;[84] consumers may expect GM to track them, but whether they expect GM to share that data with law enforcement is unclear.

Two potential solutions to the problem lie in the *Jones* concurrences. First, Justice Alito distinguished the permissible short-term monitoring in *Knotts* from that which occurred in *Jones*.[85] Because society would not expect law enforcement to "secretly monitor and catalogue every single movement of an individual's car" for twenty-eight days, using a GPS to do so was a search.[86] Similarly, since it would not be practicable for the government to track and reconstruct months of individual activity without factory-installed or smartphone GPS systems, using the technology to do so would be a clear violation of REOP, thus requiring a warrant. Had the *Jones* majority decided the case on the extent and length of monitoring rather than on the issue of trespass, it would have promoted clarity for such non-trespassory technologies in the future.

Second, Justice Sotomayor criticized Justice Alito's "'tradeoff' of privacy for convenience" theory because consumers should not lose constitutional rights simply by disclosing information "to some member of the public for a limited purpose."[87] She asserted that information that should be protected, such as a list of web sites visited, could only receive constitutional protection "if . . . Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy."[88] Such an expansion of Fourth Amendment protections, if made by either Congress or the Court, would prevent unreasonable searches in the social media sphere as well.

### B. Ubiquitous-Presence Technologies

Recent technological developments allow the linking, search, and storage of data between multiple surveillance cameras.[89] These surveillance cameras include everything from relatively traditional cameras, such as cameras on storefronts, to cameras on new technologies, like cell phone cameras and cameras on drones.[90] The

---

[84] Ganz, *supra* note 76, at 1345.

[85] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

[86] *Id.*

[87] *Id.* at 957 (Sotomayor, J., concurring).

[88] *Id.*

[89] Marc J. Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEXAS L. REV. 1349, 1465 (2004).

[90] Presenting serious ramifications for the future of privacy, in 2005 Congress authorized U.S. Customs and Border Protection to use unarmed Predator unmanned aerial vehicles, or drones, to assist police in searching for undocumented immigrants and smugglers. Brian Bennett, *Police Employ Predator Drone Spy Planes on Home Front*, L.A. TIMES, Dec. 10, 2011, http://articles.latimes.com/print/2011/dec/10/nation/la-na-drone-arrest-20111211, <http://perma.cc/76HR-P52G>.

Virginia, the first state to pass anti-drone legislation, has now announced amendments that will allow police to use drones in cases involving imminent danger to citizens. Jason Koebler, *Virginia*

linking can create a ubiquitous surveillance camera, able to capture most of American life.[91] These technologies have special privacy concerns in conjunction with new and developing biometric technologies.[92] Together, the technologies will allow governments to "reconstruct people's activities and retrace their movements through a given day" and "scrutinize or identify people whose identity and detailed behavior is otherwise likely to remain unknown."[93] Due to its emphasis on the doctrine of trespass, the *Jones* majority did not even attempt to address how such use of ubiquitous-presence technologies in law enforcement could implicate Fourth Amendment rights.

The Supreme Court's first attempt at resolving the use of airborne surveillance, in *California v. Ciraolo*,[94] does not provide sufficient clarification on the issue. The Court held that a plane flying at 1,000 feet above a fenced-in backyard to look for marijuana plants was not a search; the suspect had no REOP because the plane was in navigable airspace and the plants could be viewed with "the naked eye."[95] However, in his dissent, Justice Powell criticized the Court's assertion that backyards are visible to the public because members of the public fly in commercial aircraft and can view activities in backyards.[96] Justice Powell noted that while a commercial aircraft could fly over the suspect's property, the "risk that a passenger on such a plane might observe private activities, and might connect those activities with particular people" was "too trivial to protect against."[97] Accordingly, individuals do not "knowingly expose" their backyards by refraining to shelter them from aerial surveillance.[98] Further complications arise from the fact that drones can fly at lower altitudes and for more extended periods of time than most commercial aircraft.[99] As a result, the holdings in *Ciraolo* and *Jones* leave REOP rules unclear in the context of drones peering into backyards.

In his *Jones* concurrence, Justice Alito alluded to the best solution to the problem of drawing constitutional boundaries for

---

*Governor on Drone Ban: Police Use OK*, U.S. NEWS & WORLD REP., Mar. 26, 2013, http://www.usnews.com/news/articles/2013/03/26/virginia-gov-on-drone-ban-police-use-ok, <http://perma.cc/XJY8-RCSR>; H.B. 2012, 2013 Leg. (Va. 2013). Tellingly, drone industry officials declared that if drones were banned, as in the original bill, the state's industry would suffer. *Id.*

[91] Blitz, *supra* note 89, at 1409–10.

[92] *Id.* at 1383–84.

[93] *Id.* at 1465; *see also* Charlie Savage, *Facial Scanning Is Making Gains in Surveillance*, N.Y. TIMES, Aug. 21, 2013, http://www.nytimes.com/2013/08/21/us/facial-scanning-is-making-gains-in-surveillance.html?pagewanted=all&_r=0, <http://perma.cc/8REM-UGJB> (describing the government's research into Biometric Optical Surveillance System, "a system that would pair computers with video cameras to scan crowds and automatically identify people by their faces").

[94] 476 U.S. 207 (1986).

[95] *Id.* at 209, 215.

[96] *Id.* at 223–24 (Powell, J., dissenting).

[97] *Id.*

[98] *Id.* at 224 (citing *id.* at 213 (majority opinion)) (internal quotation marks omitted).

[99] *See* Paul McBride, *Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, 74 J. AIR L. & COM. 627, 635–36 (2009) (discussing the distinct capabilities of certain drones and how these can be instrumental in gathering information).

ubiquitous-presence technologies: action by Congress.[100] For example, after *Katz*, Congress enacted a comprehensive statute to regulate wiretapping instead of leaving it to the courts.[101] In *Jones*'s wake, the Geolocational Privacy and Surveillance Act was introduced in the House of Representatives[102] and in the Senate[103] to compel the police to obtain a warrant before attaching a GPS device to a car, locating persons through their smartphones, or obtaining geolocation data from ISPs.[104] In the absence of decisive action in *Jones*, such legislation will be vital to close loopholes opened by drone surveillance.

### C. Intermittent-Monitoring technologies

Justice Sotomayor expressed concern in *Jones* about short-term monitoring that can evade checks on the police, ultimately allowing law enforcement to construct profiles of citizens' lives from intermittent monitoring, pieced together through it information provided by third parties.[105] While various types of information are subject to this use—Justice Sotomayor references phone numbers, URLs, emails, and online shopping lists[106]—social media may have the most sweeping implications.

Justice Sotomayor stated that the "[g]overnment's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[107] Furthermore, in *Alderman*, the Court declared that *Katz* did not narrow any protections extended to the home, noting that the home is different for purposes of the Fourth Amendment.[108] However, is there protection for personal information voluntarily disclosed to ISPs and the public via social media from within the home?

A possible framework for addressing this issue can be constructed

---

[100] *See* United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring) (expressing approval for Congress' enactment of legislation to govern the use of wiretapping and discussing Congress' failure to enact legislation governing the use of GPS technology in law enforcement).

[101] *Id.* at 963 (citing 18 U.S.C §§ 2510–2522 (2006 & Supp. IV 2006)).

[102] Geolocational Privacy and Surveillance Act, H.R. 2168, 112th Cong. (1st Sess. 2011).

[103] Geolocational Privacy and Surveillance Act, S. 1212, 112th Cong. (1st Sess. 2011).

[104] Kim Zetter, *Bills Would Mandate Warrants for GPS Tracking, Cellphone Location Data*, WIRED MAG., Mar. 22, 2013, http://www.wired.com/threatlevel/2013/03/warrantless-gps-tracking, <http://perma.cc/322F-P79Q>.

It is worth noting the stark contrast between the process associated with these proposed bills and that of the hasty pro law enforcement legislation passed in the days after 9/11, as well as after the 1993 World Trade Center and 1995 Oklahoma City attacks. *See* Peter P. Swire, *Katz is Dead. Long Live Katz*, 102 MICH. L. REV. 904, 915 (2003) (discussing the post-disaster legislation).

[105] *See Jones*, 132 S. Ct. at 956–57 (Sotomayor, J., concurring) (stating that "[a]wareness that the Government may be watching chills associational and expressive freedoms.").

[106] *Id.* at 957.

[107] *Id.* at 956.

[108] Alderman v. United States, 394 U.S. 165, 178–80 (1969); *see also* Kyllo v. United States, 533 U.S. 27, 40 (2001) (noting that "the Fourth Amendment draws a firm line at the entrance to the house") (internal quotation marks omitted).

based on Justice Marshall's dissent in *Smith*, in which he proposed that the *Katz* REOP test be replaced with a test that focuses "not on the risks an individual can be presumed to accept" when sharing information, "but on the risks he should be forced to assume in a free and open society."[109] However, considering Justice Marshall's description of the "basic values underlying the Fourth Amendment" and the fact that government intrusions "significantly jeopardize [people's] sense of security,"[110] citizens should not be required to assume the risk that information they share will be turned over to the police. Unfortunately, *Jones* did not clarify the expectations related to intermittent, reconstructive social media monitoring.[111] Fortunately, however, Congress is showing its concern over privacy concerns raised by Google Glass cameras that would enable the public and police to view a continuous feed of everything a consumer is viewing wherever he is.[112] A solution to the problem may be to protect private speech and thought contained in digital media content, while allowing the monitoring of address and network information (e.g., contacts that a suspect is communicating with).[113]

Finally, proponents of lax warrant requirement for GPS monitoring assert that "[t]echnology-based information is less likely to be distorted than is evidence based on human perception," because "GPS evidence does not take sides," thus providing a neutral and credible method of gathering evidence.[114] Furthermore, they argue that GPS enhances officer safety and efficiency because officers need not actually follow suspects and risk being "made."[115] While these are strong arguments, the very nature of our criminal justice system's reliance on juries—composed of ordinary citizens handing down verdicts—suggests that our constitutional principles rely on the idea that human perception and emotions are vital in deciding the fate of fellow citizens. Because *Jones* failed to examine these issues, the Court and legislature will have to address them in the near future.

## V. CONCLUSION

Jones's reliance on trespass and its failure to insist on examining the REOP related to GPS monitoring muddies Fourth Amendment

---

[109] Smith v. Maryland, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting).

[110] *Id.* at 751 (internal quotation marks omitted).

[111] *See generally Jones*, 132 S. Ct. 945.

[112] Efrati, *supra* note 38.

[113] *See* Orrin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1017–20 (2009) (arguing that in the online setting, privacy protections should be based on a distinction between content and non-content information).

[114] Ganz, *supra* note 76, at 1355–56 (internal quotation marks omitted).

[115] *Id.* at 1356. "Made" refers to an officer being "discovered by a suspect." *Id.*

protections in the context of advanced technology. Determining constitutional boundaries for new technologies, such as social media, that enable the government to intrude on vast amounts of sensitive information voluntarily disclosed by citizens poses a "particularly vexing" challenge.[116] Moreover, the rules for domestic drone surveillance, where citizens cannot be held to have voluntarily broadcast data, is left unclear. Ultimately, Congress and the Court will need to define the parameters of voluntary disclosure, the extent of the REOP, where the boundary of a home ends, and the distinction between private content and public network administration information in order to establish constitutional limits to surveillance that both protect citizens and enable police efficiency and safety.

[116] *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (stating that new electronic information, made available through ever-advancing technology, will pose problems if the courts continue to focus on physical trespass when determining whether a search has occurred).