ARTICLES

THE FOURTH AMENDMENT BEYOND *KATZ*, *KYLLO* AND *JONES*: REINSTATING JUSTIFIABLE RELIANCE AS A MORE SECURE CONSTITUTIONAL STANDARD FOR PRIVACY

RICHARD SOBEL, BARRY HORWITZ, AND GERALD JENKINS*

* Richard Sobel, Visiting Scholar, Buffett Center, Northwestern University and Associate, Du Bois Institute, Harvard University; Barry Horwitz, Associate, Greenberg Traurig LLP; and Gerald Jenkins, Principal, Goldberg Kohn. We would like to thank Mile Knabe and Heidi Kuehl for able research assistance, and Lesley Arca, Jake Laperruque, the Cyber Privacy Project, David Abrams, Latanya Sweeney, and the Topics in Privacy seminar at Harvard Law School for comments on earlier versions of this paper. We also appreciate the comments and suggestions of editors at the *Public Interest Law Journal*.

ABSTRACT

In reaffirming the broad scope of the Fourth Amendment, the Supreme Court's judgment in United States v. Jones *forms the basis for more reliable privacy protections. The majority opinion upheld the traditional view of the Amendment based on property rights, whereby the government's physical intrusion upon private property (by attaching a technological device to Jones' car to track his location) is considered a search within the meaning of the Fourth Amendment. Justice Alito's concurring opinion held that attaching a GPS monitor to enable long-term surveillance is a search based on Jones' "reasonable expectation of privacy," a test first articulated in 1967 in Justice Harlan's concurrence in* Katz v. United States.

Justice Sotomayor's concurring opinion in Jones *bridges the gap by supporting the majority's trespass test as "an irreducible constitutional minimum," but acknowledging that rapidly advancing technology enables the government to ascertain more personal information than ever before. Further, Justice Sotomayor articulated the need to reconsider the third-party doctrine (that individuals retain no reasonable expectation of privacy in information voluntarily disclosed to third parties). Thus, the Jones opinions collectively reflect the Court's determination, prefigured in Justice Scalia's majority opinion in* Kyllo v. United States *in 2001, not to let advances in technology nullify Fourth Amendment protections.*

However, the lesser-known seven-person majority opinion in Katz *used a "justifiable reliance" standard, which provides a stronger and more secure basis for Fourth Amendment protections than the fluctuating "reasonable expectations of privacy" proposed in Justice Harlan's solo concurrence. The majority opinion in* Katz *recognized that the Fourth Amendment protects "people, not places," and held that the Fourth Amendment protects people in public when they "justifiably relied" on their privacy. Such privacy interests are grounded in the text of the Fourth Amendment: "the right of the people to be secure in their persons, houses, papers and effects."*

The Jones *opinions reflect the need for maintaining traditional Fourth Amendment rights in the face of constantly advancing technology. This article advocates reinstating the* Katz *majority holding—a justifiable reliance standard reinforcing that the Fourth Amendment protects "people not places"—as the better mechanism to secure Fourth Amendment rights, particularly in virtual "effects." The justifiable reliance test encompasses the trespass and reasonable-expectation-of-privacy tests within a single framework that secures Fourth Amendment protections in the digital age.*

I. INTRODUCTION

In reaffirming the broad scope of the Fourth Amendment, the Supreme Court's unanimous conclusion in *United States v. Jones*[1] created the basis for more reliable Fourth Amendment protections. In *Jones*, the government attached an electronic Global Positioning System (GPS) tracking device to a car registered to Jones' wife.[2] Although the government obtained a warrant, the warrant only authorized installing the tracking device within ten days and only within the District of Columbia.[3] Instead, the government installed the device on the eleventh day in Maryland.[4] For four weeks, the government tracked the car's location and movement, and the tracking device relayed over 2,000 pages of data.[5] Based on the information received, the government indicted and convicted Jones of conspiracy to distribute cocaine.[6]

The *Jones* majority opinion, authored by Justice Scalia, upheld the traditional view of the Fourth Amendment based on property rights: that the government's "physical intrusion" upon "private property for the purpose of obtaining information . . . would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[7] Justice Alito's concurring opinion agreed that physically applying a technological device to a vehicle for the purpose of GPS monitoring was such an intrusion and would be a search based on a "reasonable expectation of privacy," first articulated in Justice Harlan's solo concurrence in *Katz v. United States*.[8] In addition, Justice Sotomayor's concurring opinion accepted the majority's use of the trespass test as "an irreducible constitutional minimum,"[9] but recognized that ever-advancing technology has "enable[d] the Government to ascertain, more or less at will, [people's] political and religious beliefs, sexual habits, and so on."[10]

The evolution of Fourth Amendment jurisprudence has often followed technological developments, with the courts at times supporting and at other times undermining safeguards to Fourth Amendment rights. Though the majority opinion in *Jones* was arguably premised on narrow property-based grounds, the implications of *Jones* are broader because a majority of Justices recognized that technology has now enabled the government to record, store and analyze an unprecedented amount of information.[11] The Justices' opinions collectively re-

---

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

[2] *Id.* at 948.

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] *Id.*

[7] *Id.* at 949.

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

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

[10] *Id.* at 956 (Sotomayor, J., concurring).

[11] *Id.* (Sotomayor, J., concurring) (noting that people's "movements [can] be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will,

flect the Court's determination, prefigured in Justice Scalia's 2001 majority opinion in *Kyllo v. United States*, not to let advances in technology nullify Fourth Amendment protections based on the language used in precedents that addressed older technologies, like landline telephones.[12]

The seven-person majority opinion by Justice Stewart in *Katz v. United States* in 1967 provides a stronger, more secure basis for privacy protection in the justifiable reliance standard, which is broader than either the property-based trespass test or the reasonable-expectation-of-privacy test. The weaker reasonable-expectation test was, in fact, first proposed by Justice Harlan in his concurring opinion in *Katz*, in which no other Justice joined.[13] The majority opinion in *Katz* recognized that the Fourth Amendment protects "people, not places."[14] Further, the Court held that the Fourth Amendment's reach extends to privacy rights in public, stating:

> The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth, and thus constituted a "search and seizure" within the meaning of the Fourth Amendment.[15]

The people's right to justifiably rely on their privacy interests is firmly grounded in the Fourth Amendment "right of the people to be secure in their persons, houses, papers and effects."[16] These enumerated elements clearly demonstrate protections for both property interests (*e.g.*, houses and papers) and privacy interests (*e.g.*, people and effects).[17]

While *Jones* has renewed reliance on the traditional trespass test for determining Fourth Amendment violations in the digital age, the concurring opinions reflect an understanding of the need for upholding Fourth Amendment privacy interests in the face of constantly advancing technology. As set forth below, reinforcing the current pertinence of the *Katz* majority holding by reinstating a "justifiable reliance" standard would advance the goal of protecting people against Fourth Amendment violations, wherever they may be. The jus-

---

their political and religious beliefs, sexual habits, and so on"); *id.* at 963 (Alito, J., concurring) (noting that "[r]ecent years have seen the emergence of many new devices that permit the monitoring of a person's movements. . . . cell phones and other wireless devices now permit wireless carriers"—and by extension, the government—"to track and record the location of users").

[12] Kyllo v. United States, 533 U.S. 27, 33-34 (2001) ("It would be foolish to contend that the degree of privacy secured to citizens by the Fourth Amendment has been entirely unaffected by the advance of technology. . . . To withdraw protection of this minimum expectation would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment.").

[13] Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

[14] *Id.* at 351.

[15] *Id.* at 351-53.

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

[17] *See infra* notes 24-30 and accompanying text.

tifiable reliance standard can be broken down into a two-part test: (1) a person relies on his Fourth Amendment rights and (2) such reliance is justifiable under the circumstances. Justifiable reliance encompasses both the trespass test (reliance is most justifiable within one's home, office, car or, temporarily, an enclosed telephone booth) and the reasonable-expectation test (an expectation of privacy is most reasonable when a court determines that a person relied on maintaining privacy, and that the person's reliance was justified), but it is not limited to those two standards.

The justifiable reliance test parallels the reasonable-expectations-of-privacy test used by most courts today. But the different implications of the terms "justifiable" (as opposed to "reasonable") and "reliance" (as opposed to "expectations") necessarily convey a broader and more secure standard. The *Katz* Court intended such a broader test for Fourth Amendment privacy protections—one that does not require trespass against home or property, and one that does not require disbelief in the potency of continuing technological advances. Reasonable expectations protect us when we reasonably think our privacy is protected, but such conceptions are constantly changing and may depend on the latest news report of the most recent technology affecting privacy. Justifiable reliance protects us when we rely on defensible situations against unwarranted governmental intrusion, that is, when the history, text and context of the Fourth Amendment tell us our privacy is protected.

The *Katz* majority's justifiable reliance standard is an umbrella test that combines and reframes the existing trespass and reasonable-expectation-of-privacy tests. This more inclusive and reliable standard ensures that the government cannot abuse advancing technology in the digital age to erode privacy protections, particularly with unreasonable searches of virtual "effects" as guaranteed by the Fourth Amendment.[18] Moreover, as set forth below, the broader justifiable reliance test upholds privacy interests where the trespass and reasonable-expectation tests fail to do so.

Thus, courts can use justifiable reliance to strengthen and advance traditional Fourth Amendment protections (*e.g.*, letters and private papers) to their digital analogues (*e.g.*, emails and text messages). The justifiable reliance test is not limited by place, ownership or other property interests, nor is it limited by changing expectations. Public opinion and technology shape expectations, which may vary, often without any basis in fact. Justifiable reliance takes us out of the fickle realm of what the public expects today (and may no longer expect next month), and back to the actual words and intent of the Fourth Amendment.

---

[18] *Kyllo*, 533 U.S. at 34 (recognizing that technology should not be permitted to "erode the privacy guaranteed by the Fourth Amendment").

II. FOURTH AMENDMENT JURISPRUDENCE

A. *The Text of the Fourth Amendment Outlines Property and Privacy Interests*

An analysis of Fourth Amendment jurisprudence begins with the text itself, which broadly outlines people's rights in both property and privacy:

> 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.[19]

That the Fourth Amendment protects property rights is clear: the text enumerates the right of people "to be secure in their persons, houses, papers and effects." At the time the Fourth Amendment was adopted, it was well-established under English common law that "the house of every one is to him as his castle and fortress, as well for his defence against injury and violence as for his repose."[20] A well-known case at that time, which the majority cited in *Jones*, is *Entick v. Carrington*, in which the plaintiff sued the King's messengers for trespass after they broke into his home to search for "seditious papers."[21] *Entick* also recognized people's property interests in their private papers.[22] Thus, the property aspect of Fourth Amendment rights was widely recognized at its adoption, and has guided its interpretation for years.[23]

At the same time, however, the Fourth Amendment's text both explicitly and implicitly addresses privacy rights. The explicit recognition of privacy rights arises from the enumeration of the people's right "to be secure in their *persons* [and] *papers*."[24] The security in one's "person" is understood to invoke a privacy interest: the "right to be let alone"[25]—to be free of invasive touching upon one's most fundamentally private sphere: one's body.[26] Similarly, the security

---

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

[20] Semayne's Case, (1572) 77 Eng. Rep. 194 (K.B.) 195.

[21] Entick v. Carrington, (1765) 95 Eng. Rep. 807 (C.P.) 817.

[22] Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (C.P.) 1066 ("Papers are the owner's goods and chattels: they are his dearest property . . . .").

[23] *See infra* notes 35-44 and accompanying text.

[24] U.S. CONST. amend. IV (emphasis added).

[25] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890).

[26] *See, e.g.*, Campbell v. Miller, 499 F.3d 711, 718 (7th Cir. 2007) (recognizing that "strip searches involving the visual inspection of the anal area are 'demeaning, dehumanizing, undignified, humiliating, terrifying, unpleasant, embarrassing, repulsive, [and] signify[ ] degradation and submission . . .'" (quoting Mary Beth G. v. City of Chicago, 723 F.2d 1263, 1272 (7th Cir. 1983) (alterations in original)), and noting that "[t]he invasion of privacy rights at issue [in such searches] is at its highest, no matter where the search [is] conducted"). The right to be secure in one's "person" also invokes a privacy interest prohibiting the

of one's "papers" clearly invokes the privacy interest long recognized in democratic societies: the right to freedom of thought, and freedom to express thought to others in private correspondence.[27]

Implicit recognition of the right to privacy, and a basis for its protections in an evolving technological environment, can also be found in the final enumerated term: the security of one's "effects." James Madison's proposed draft of the Fourth Amendment originally attempted to preserve "'[t]he rights of the people to be secured in their persons, their houses, their papers, and their other property, from all unreasonable searches and seizures . . . .'"[28] However, Congress' revisions of Madison's proposal, including changing the wording "and their other property" to "and effects," "broadened the scope of the Amendment in some respects."[29] While the Supreme Court has stated that "the term 'ef-

---

government from fundamentally interfering with one's personhood. For example, if the holding of *Lawrence v. Texas* means anything, it is that the government cannot intrude upon the right of individuals to engage in private consensual conduct not harmful to others:

> The statutes do seek to control a personal relationship that, whether or not entitled to formal recognition in the law, is within the liberty of persons to choose without being punished as criminals. This, as a general rule, should counsel against attempts by the State, or a court, to define the meaning of the relationship or to set its boundaries absent injury to a person or abuse of an institution the law protects. It suffices for us to acknowledge that adults may choose to enter upon this relationship in the confines of their homes and their own private lives and still retain their dignity as free persons. When sexuality finds overt expression in intimate conduct with another person, the conduct can be but one element in a personal bond that is more enduring. The liberty protected by the Constitution allows homosexual persons the right to make this choice.

Lawrence v. Texas, 539 U.S. 558, 567 (2003). The first sentence of *Lawrence* says it all: "Liberty protects the person from unwarranted government intrusions into a dwelling or other private places." *Id.* at 562.

[27] United States *ex rel.* Milwaukee Social Democratic Publishing Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting) ("[T]he use of the mails is almost as much a part of free speech as the right to use our tongues."); *see* Ex Parte *Jackson*, 96 U.S. 727, 733 (1877) ("Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection, except as to their outward form and weight, as if they were retained by the parties forwarding them in their own domiciles. The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be. Whilst in the mail, they can only be opened and examined under like warrant, issued upon similar oath or affirmation, particularly describing the thing to be seized, as is required when papers are subjected to search in one's own household. No law of Congress can place in the hands of officials connected with the postal service any authority to invade the secrecy of letters and such sealed packages in the mail . . ."); *Entick*, 19 How. St. Tr. at 1066 ("[W]here private papers are removed and carried away, the secret nature of those goods will be an aggravation of the trespass, and demand more considerable damages in that respect.").

[28] Oliver v. United States, 466 U.S. 170, 176-77 (1984) (quoting NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 100 n.77 (1937)).

[29] *Id.* at 177. While Madison's original proposal "seemed to be directed against improper

fects' is less inclusive than 'property,'" that statement was based on the belief that "[t]he Framers would have understood the term 'effects' to be limited to personal, rather than real, property."[30] "Effects" has a broader meaning in the digital age.

Still, the Supreme Court has recognized the breadth of the term "effects" by acknowledging privacy interests in, for example, the contents of luggage (a "footlocker")[31] and the contents of a sealed letter or package (whether in the hands of the U.S. postal service or private carriers).[32] The majority in *United States v. Jones* also refers to Jones' car as an "effect."[33] Thus, the inclusion of the term "effects" into the Fourth Amendment was purposeful, and intended to broaden the Amendment to apply to future concepts of personal property and privacy. The inclusive term "effects" is crucial to Fourth Amendment privacy principles in the modern age, where people "effect" online personas, profiles and presences, and in which "papers" have often been replaced in favor of electronic communications, the contents of which are often private or intimate. "Effects" are, in a sense, the precursor to the "virtual" world. That such "effects" are intangible does not mean they lack privacy interests subject to the Fourth Amendment.[34]

---

warrants only," Congress' revisions resulted in the Fourth Amendment having two separate clauses: "The general right of security from unreasonable search and seizure was given a sanction of its own and the amendment thus intentionally given a broader scope. That the prohibition against 'unreasonable searches' was intended, accordingly, to cover something other than the form of the warrant is a question no longer left to implication to be derived from the phraseology of the Amendment." LASSON, *supra* note 28, at 100-03.

[30] *Oliver*, 466 U.S. at 177 n.7 (citations omitted).

[31] United States v. Chadwick, 433 U.S. 1, 15-16 (1977) (holding that respondents were "entitled to the protection of the Warrant Clause with the evaluation of a neutral magistrate, before their privacy interests in the contents of the footlocker were invaded").

[32] See Ex Parte *Jackson*, 96 U.S. at 733; United States v. Jacobsen, 466 U.S. 109, 114 (1984) ("When the wrapped parcel involved in this case was delivered to the private freight carrier, it was unquestionably an 'effect' within the meaning of the Fourth Amendment.").

[33] United States v. Jones, 132 S. Ct. 945, 953 (2012).

[34] *See* United States v. Warshak, 631 F.3d 266, 283-288 (6th Cir. 2010) (holding that email contents are protected under the Fourth Amendment); Wilson v. Moreau, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (holding that an individual "had a reasonable expectation of privacy in his personal Yahoo e-mail account," despite his accessing that account on computers at the public library). For the Fourth Amendment's protections to keep pace with the digital age, it must be recognized that *Katz's* holding that the Fourth Amendment protects "people, not places" extends to virtual manifestations of persons and a person's virtual "effects," such as usernames, passwords, digital signatures, emails, text messages, digital location information, and other forms of recorded and stored communications and data. In essence, the law should recognize that people have a personal property interest in their data and electronic "effects."

B. *Cases Interpreting the Fourth Amendment*

1. Early Cases Preceding Modern Technology: The Trespass Test

Because property rights inherent in the Fourth Amendment have been widely recognized since the nation's founding,[35] it is not surprising that early Supreme Court decisions used a property-based test to determine violations of the Fourth Amendment: a government-sponsored physical trespass on or of tangible property constituted a Fourth Amendment violation.[36] Known as "the trespass test," it was plainly articulated and found to be controlling into the twentieth century by the Supreme Court in *Olmstead v. United States*.[37] There, the test confronted one of the first modern technological advances, the telephone, and its intrusive counterpart, wiretapping.

In 1928, Roy Olmstead was convicted of conspiring to violate the National Prohibition Act.[38] Federal officers gathered the evidence to obtain this conviction by wiretapping telephone lines outside of businesses and offices the defendant used.[39] Federal agents placed their wiretaps on public telephone wires, never directly trespassing upon any property belonging to Olmstead.[40] After scrutinizing earlier Supreme Court Fourth Amendment decisions, the majority determined there was no such violation in this case because "[t]here was no entry of the houses or offices of the defendants."[41] In essence, the *Olmstead* Court articulated that no Fourth Amendment violation exists "unless there has been an official search and seizure of [a] person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage'[42] for the purpose of making a seizure."[43] Since the wires to which federal agents affixed the surveillance tools were not Olmstead's and did not reside within his property, the evidence obtained from such surveillance was deemed to be admissible and the Court affirmed the conviction.[44]

In strong dissent, Justice Louis Brandeis, coauthor of the seminal article "The Right to Privacy,"[45] found that the search violated Olmstead's Fourth

---

[35] The language of Madison's "proposal did not purport to *create* the right to be secure from unreasonable searches and seizures but merely stated it as a right which already existed." LASSON, *supra* note 28, at 100 n.77.

[36] Olmstead v. United States, 277 U.S. 438, 466 (1928); *see also* Gouled v. United States, 255 U.S. 298, 305-06 (1921) (finding a violation of the Fourth Amendment when papers were taken from a private office without the knowledge of the defendant).

[37] *See Olmstead*, 277 U.S. at 456-66 (1928).

[38] *Id.* at 455.

[39] *Id.* at 456-57.

[40] *Id.* at 457.

[41] *Id.* at 464.

[42] A "curtilage" is "the enclosed space of ground and buildings immediately surrounding a dwelling-house." BOUVIER'S LAW DICTIONARY 486 (1897).

[43] *Olmstead*, 277 U.S. at 466.

[44] *Id.*

[45] Warren & Brandeis, *supra* note 25.

Amendment rights.[46] At the outset, Justice Brandeis highlighted that the government "concede[d] that if wire-tapping can be deemed a search and seizure within the Fourth Amendment, such wire-tapping as was practiced in the case at bar was an unreasonable search and seizure, and that the evidence thus obtained was inadmissible."[47] After a discussion of how constitutional language is painted in broad strokes because constitutional principles "must be capable of wider application than the mischief which gave [them] birth,"[48] Justice Brandeis presciently emphasized that expanding technology must not be allowed to vitiate Fourth Amendment principles, stating:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court. . . . Can it be that the Constitution affords no protection against such invasions of individual security?[49]

Justice Brandeis argued that the Framers "undertook to secure conditions favorable to the pursuit of happiness" by, among other things, conferring "against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[50] Thus, he concluded, "[t]o protect that right, every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed, must be deemed a violation of the Fourth Amendment."[51]

Justice Brandeis argued that "[d]ecency, security and liberty alike demand that government officials shall be subjected to the same rules of conduct that

---

[46] *Olmstead*, 277 U.S. at 471-85 (Brandeis, J., dissenting).

[47] *Id.* at 471-72 (Brandeis, J., dissenting).

[48] Specifically, Justice Brandeis quoted *Weems v. United States*, which stated:

> Legislation, both statutory and constitutional, is enacted, it is true, from an experience of evils, but its general language should not, therefore, be necessarily confined to the form that evil had theretofore taken. Time works changes, brings into existence new conditions and purposes. Therefore a principle to be vital must be capable of wider application than the mischief which gave it birth. This is peculiarly true of constitutions. They are not ephemeral enactments, designed to meet passing occasions. They are, to use the words of Chief Justice Marshall "designed to approach immortality as nearly as human institutions can approach it." The future is their care and provision for events of good and bad tendencies of which no prophecy can be made. In the application of a constitution, therefore, our contemplation cannot be only of what has been but of what may be. Under any other rule a constitution would indeed be as easy of application as it would be deficient in efficacy and power. Its general principles would have little value and be converted by precedent into impotent and lifeless formulas. Rights declared in words might be lost in reality.

Id. at 472-73 (Brandeis, J., dissenting) (quoting Weems v. United States, 217 U.S. 349, 373 (1910)).

[49] *Id.* at 474 (Brandeis, J., dissenting).

[50] *Id.* at 478 (Brandeis, J., dissenting).

[51] *Id.* (Brandeis, J., dissenting).

are commands to the citizen."[52] This farsighted dissent, prefiguring *Katz* a generation later, offers words of wisdom that must be heeded now more fully. As set forth below, courts cannot allow the advance of technology solely to benefit the government, while requiring individuals to accept that such technology necessarily vitiates their Fourth Amendment rights.

2. The Modern Era: Development and Acceptance of the Reasonable-Expectation-of-Privacy Test

The trespass test was used to determine Fourth Amendment violations until the 1967 Supreme Court decision in *Katz v. United States*.[53] There, Charles Katz was convicted by the District Court of transmitting betting information by telephone.[54] Paralleling the facts of *Olmstead*, the primary evidence used to obtain the conviction was acquired from an electronic listening device installed upon a public telephone booth used by the defendant.[55] In its analysis, in which seven Justices voted in favor of Katz, the majority found that focusing on whether Katz was located within a "constitutionally protected [area] deflects attention from the problem presented by this case. For the Fourth Amendment protects people, not places."[56] This recognition of Fourth Amendment protection for people *without regard to their location* is a signal contribution of the *Katz* majority.

The *Katz* Court held that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[57] Thus, the Court recognized that the Fourth Amendment protected Katz's conversations in a public telephone booth:

> One who occupies [a telephone booth] shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[58]

More importantly, the Court broadly recognized that the source of its holding was not property rights, but *privacy* rights afforded by the Fourth Amend-

---

[52] *Id.* at 485 (Brandeis, J., dissenting). Justice Brandeis viewed the "Government [as] the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example. Crime is contagious. If the Government becomes a lawbreaker, it breeds contempt for law." *Id.*

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

[54] *Id.* at 348.

[55] *Id.* at 348.

[56] *Id.* at 351 (footnote omitted) (internal quotation marks omitted).

[57] *Id.*

[58] *Id.* at 352.

ment.[59] Quoting *Warden, Maryland Penitentiary v. Hayden*,[60] the Court enunciated that "[t]he premise that property interests control the right of the Government to search and seize has been discredited."[61] Finally, to underscore its importance, the Court reiterated the "people, not places" concept more broadly: that "once it is recognized that the Fourth Amendment protects people—and not simply 'areas'—against unreasonable searches and seizures it becomes clear that the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion into any given enclosure."[62]

Accordingly, the Court noted that the *Olmstead* holding, whereby the test for Fourth Amendment violations depended upon a government-sponsored trespass on private property, "can no longer be regarded as controlling."[63] Rather, the electronic surveillance by the government "violated the privacy upon which [Katz] *justifiably relied* while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[64] Thus, the lower court's decision was reversed, and the evidence obtained by virtue of the unwarranted listening device was deemed inadmissible.[65]

In a separate concurring opinion joined by no other members of the *Katz* Court, Justice Harlan set forth his different interpretation of the majority's justifiable reliance on privacy, stating that the Fourth Amendment protects a person's "reasonable expectation of privacy."[66] He explained that such a protection requires (1) a subjective expectation of privacy, and (2) an objective expectation of privacy, meaning that the expectation "be one that society is prepared to recognize as 'reasonable.'"[67]

Justice Harlan's solo concurrence directly contradicted the majority's agreement that focusing on "constitutionally protected areas" is misguided and "deflects attention from"[68] the real issue presented by the case.[69] Rather, Justice Harlan asserted that the relevant question "is what protection [the Fourth

---

[59] *Id.* at 353.

[60] Warden, Md. Penitentiary v. Hayden, 387 U.S. 294 (1967).

[61] *Katz*, 389 U.S. at 353 (quoting *Warden*, 387 U.S. at 304).

[62] *Id.*

[63] *Id.*

[64] *Id.* (emphasis added).

[65] *Id.* at 359.

[66] *Id.* at 360 (Harlan, J., concurring).

[67] *Id.* at 360-61 (Harlan, J., concurring).

[68] *Id.* at 351.

[69] *Id.* at 361 (Harlan, J., concurring) ("I join the opinion of the Court, which I read to hold only (a) that *an enclosed telephone booth is an area where*, like a home, and unlike a field, *a person has a constitutionally protected reasonable expectation of privacy*; (b) that *electronic as well as physical intrusion into a place that is in this sense private* may constitute a violation of the Fourth Amendment; and (c) that *the invasion of a constitutionally protected area* by federal authorities is, as the Court has long held, presumptively unreasonable in the absence of a search warrant.") (emphases added) (citation omitted).

Amendment] afford[s] to . . . people" and that "the answer . . . *requires reference to a 'place.'*"[70] Thus, contrary to the majority's holding that the Fourth Amendment protects people and not places,[71] Justice Harlan's concurrence stresses that the Fourth Amendment's protections necessarily flow from location-oriented property rights.[72]

Accordingly, Justice Harlan held to the old idea that only physical areas can be worthy of Fourth Amendment protection. His conception is inconsistent with the *Katz* majority—and is also outdated and incomplete—because it incorrectly suggests that Fourth Amendment privacy rights are not separately protected outside of any established property interests.[73] In contrast, the *Katz* majority explicitly held that Fourth Amendment rights can flow independently from property interests and are designed to protect people, wherever they may be.[74] At the time the Fourth Amendment was ratified, courts recognized that the "secret nature" of "private papers" aggravated the trespass and removal of such private papers, resulting in "more considerable damages."[75] In light of the majority's understanding in *Katz*, lower courts that solely rely on the reasonable-expectation test risk being constrained by Justice Harlan's standard. That standard may have been sufficient to support the *Katz* result, but no one else on the *Katz* Court was convinced that the reasonable-expectation test was the only test for privacy protection. In other words, a "reasonable expectation of privacy" may provide a handy standard for protecting a certain subset of Fourth Amendment rights, but it does not protect all such rights intended by the scope of the Amendment. Further, there is no evidence that anyone else on the *Katz* Court considered Justice Harlan's test to be adequate for that purpose, or considered it to be the exclusive standard for protecting privacy.

A year after the *Katz* decision, Justice Harlan advanced his reasonable-expectation test to a majority of the Court in *Mancusi v. DeForte*.[76] There, the Court found a search of the defendant's office to be in violation of the Fourth Amendment.[77] Writing for a majority of six Justices, Justice Harlan stated that the Court's decision in *Katz* "makes it clear that capacity to claim the protection of the [Fourth] Amendment depends not upon a property right in the invaded place, but upon *whether the area was one in which there was a reasonable expectation of freedom from government intrusion*."[78] Rather than citing the

---

[70] *Id.* (Harlan, J., concurring) (emphasis added).

[71] *Id.* at 351.

[72] *Id.* at 360-61 (Harlan, J., concurring).

[73] *See id.* at 353.

[74] Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("Expectations of privacy protected by the Fourth Amendment, of course, need not be based on a common-law interest in real or personal property, or on the invasion of such an interest.").

[75] Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (C.P.) 1066.

[76] Mancusi v. DeForte, 392 U.S. 364 (1968).

[77] *Id.* at 372.

[78] *Id.* at 368 (emphasis added).

majority holding in *Mancusi*, most courts cite to Justice Harlan's solo concurrence in *Katz* about "expectations of privacy" when considering Fourth Amendment issues.[79] Thus, Justice Harlan introduced into Fourth Amendment jurisprudence a useful, but overly narrow test based on expectations, which fails to consider the variety of ways in which the government can unreasonably intrude upon one's privacy.

Although the *Katz* majority's assertion that "the Fourth Amendment protects people, not places"[80] is cited in numerous opinions, it is typically followed by an application of Justice Harlan's concurrence test based on reasonable expectations of privacy.[81] The reasonable-expectation test (sometimes stated as the "legitimate expectation" test) has become the *de facto* standard for Fourth Amendment protection.[82] As a result, the broader majority decision by Justice Stewart in *Katz* about justifiable reliance is generally overlooked or ignored.[83] Yet, its strength as a more secure basis for Fourth Amendment protections deserves broader recognition and application.

Fourth Amendment jurisprudence now uses limiting language to focus on the narrower concept of expectations. Courts discuss trespass and reasonable expectations of privacy, but the broader conception of "freedom from governmental intrusion," which *Katz* era Supreme Court decisions often highlighted,[84] is rarely mentioned anymore.[85] That privacy can be defined more expansively as

---

[79] *See, e.g.*, Oliver v. United States, 466 U.S. 170, 177 (1984); Smith v. Maryland, 442 U.S. 735, 740 (1979); United States v. Titemore, 437 F.3d 251, 256 (2d Cir. 2006).

[80] Katz v. United States, 389 U.S. 347, 351 (1967).

[81] *See, e.g.*, cases cited in note 79.

[82] *See, e.g.*, cases cited in note 79; *see also* Kyllo v. United States, 533 U.S. 27, 32-33 (2001); Bond v. United States, 529 U.S. 334, 337-338 (2000); California v. Ciraolo, 476 U.S. 207, 211 (1986).

[83] *See, e.g.*, cases cited in note 82.

[84] *See, e.g.*, *Katz*, 389 U.S. at 350 (stating that the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion, but its protections go further, and often have nothing to do with privacy at all"); Eisenstadt v. Baird, 405 U.S. 438, 453 (1972) (noting that "[i]f the right of privacy means anything, it is the right of the *individual*, married or single, to be free from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child") (emphasis in original); Mancusi v. DeForte, 392 U.S. 364, 368 (1968) (characterizing the *Katz* decision as making clear that the "capacity to claim the protection of the Amendment depends not upon a property right in the invaded place but upon whether the area was one in which there was a reasonable expectation of freedom from governmental intrusion"); Terry v. Ohio, 392 U.S. 1, 9 (1968) ("We have recently held that 'the Fourth Amendment protects people, not places,' and wherever an individual may harbor a reasonable 'expectation of privacy,' he is entitled to be free from unreasonable governmental intrusion") (citations omitted).

[85] Apart from the opening line in the landmark case, *Lawrence v. Texas*, which states "Liberty protects the person from unwarranted government intrusions into a dwelling or other private places," the phrase "government intrusion" seems to have disappeared from recent Supreme Court cases. 562 U.S. 558, 562 (2003).

freedom from governmental intrusion should continue to inform Fourth Amendment analyses. This is particularly so in the digital age of electronic surveillance because new forms of technological intrusion are beginning to encircle our notions about what we once thought was private. As Justice Douglas noted in his dissent in *United States v. White*:

> Electronic surveillance is the greatest leveler of human privacy ever known. How most forms of it can be held "reasonable" within the meaning of the Fourth Amendment is a mystery. To be sure, the Constitution and Bill of Rights are not to be read as covering only the technology known in the 18th century . . . . [T]he concepts of privacy which the Founders enshrined in the Fourth Amendment vanish completely when we slavishly allow an all-powerful government, proclaiming law and order, efficiency, and other benign purposes, to penetrate all the walls and doors which men need to shield them from the pressures of a turbulent life around them and give them the health and strength to carry on . . . . "Electronic aids add a wholly new dimension to eavesdropping. They make it more penetrating, more indiscriminate, more truly obnoxious to a free society. Electronic surveillance, in fact, makes the police omniscient; and police omniscience is one of the most effective tools of tyranny."[86]

When the Court applied Justice Harlan's reasonable-expectation-of-privacy test in its 1998 decision, *Minnesota v. Carter*, an intriguing discourse between the Justices supported the idea that the majority holding in *Katz* about protections of people and not places remains good law and should be given more weight in current and future decisions.[87] There, Justice Scalia, joined by Justice Thomas, criticized the Court for adopting Justice Harlan's reasonable-expectation-of-privacy test because it is "self-indulgent" and has "no plausible foundation in the text of the Fourth Amendment."[88] At the end of Justice Ginsburg's dissenting opinion, joined by Justices Stevens and Souter, she counters Justice Scalia's criticism by denying "that we have elevated Justice Harlan's concurring opinion in *Katz* to first place" over "the clear opinion of the Court that 'the Fourth Amendment protects people, not places.' "[89]

The *Carter* decision thus suggests that at least five Justices—namely, Justices Scalia, Thomas, Ginsburg, Stevens and Souter—agreed that Justice Harlan's reasonable-expectation-of-privacy rubric is not the only viable test for considering Fourth Amendment privacy protections. Indeed, Justice Ginsburg asserts that this " 'people, not places' . . . core understanding is the *leitmotif* of

---

[86] United States v. White, 401 U.S. 745, 756-60 (1971) (Douglas, J., dissenting) (quoting Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting)).

[87] Minnesota v. Carter, 525 U.S. 83, 91 (1998) (holding that defendants, who were not overnight guests, had no legitimate expectation of privacy in another's apartment where they were present for only a short time).

[88] *Id.* at 97 (Scalia, J., concurring).

[89] *Id.* at 111 n.3 (Ginsburg, J., dissenting) (citations omitted).

Justice Harlan's concurring opinion."[90] The *Carter* colloquy breathed new life into the *Katz* majority's support for constitutional protections for people, not places. By reiterating the importance of upholding the rights of people, regardless of their location, and the need for broader bases for Fourth Amendment protection, it took a step in the direction of *Jones*.

In 2001, the Supreme Court also foreshadowed *Jones* in *Kyllo v. United States*.[91] There, the government used a thermal imaging device to detect radiation emanating from a home, on the suspicion that the owner of the home was growing marijuana using high intensity lamps.[92] Writing for the majority, Justice Scalia held that where "the Government uses a device that is not in general public use"[93] to detect information from inside a home which cannot be seen by the naked eye, "the surveillance is a 'search' and is presumptively unreasonable without a warrant."[94] Rejecting the government's claim that such a search must be upheld, Justice Scalia emphasized that "just as a thermal imager captures only heat emanating from a house, so also a powerful directional microphone picks up only sound emanating from a house," and stated:

> We rejected such a mechanical interpretation of the Fourth Amendment in *Katz*, where the eavesdropping device picked up only sound waves that reached the exterior of the phone booth. Reversing that approach would leave the homeowner at the mercy of advancing technology . . . . While the technology used in the present case was relatively crude, the rule we adopt must take account of more sophisticated systems that are already in

---

[90] *Id.* (Ginsburg, J., dissenting). As shown above, Justice Harlan's concurrence explicitly maintains the concept of "constitutionally-protected areas," and relies upon a "reference to a 'place'" in determining the scope of protection afforded. *See supra* notes 69-72 and accompanying text. Thus, Justice Harlan's *Katz* concurrence *does not* retain a core understanding that the Fourth Amendment protects people as opposed to places or areas.

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

[92] *Id.* at 29-30.

[93] The fact that a device is in "general public use" says nothing of its potential for privacy abuses, and this standard has no basis in Fourth Amendment text or case law. Rather, it relies on the questionable argument that the public's familiarity with a given technology reflects a diminished expectation of privacy relative to that technology, and thus the government may use it to obtain information about civilians without the need for a warrant. But the rate of new technology being introduced and adopted by the public today continues to increase. In fact, GPS tracking devices are reportedly flying off the shelves because "[h]igh-tech tracking tools that would a decade ago have rarely been used outside police and military circles are available today to anyone with a credit card and access to the Internet." Ryan Gallagher, *The Spy Who GPS-Tagged Me*, SLATE.COM (Nov. 9, 2012, 8:33 AM), http://www.slate.com/articles/technology/technology/2012/11/gps_trackers_to_monitor_cheating_spouses_a_legal_gray_area_for_private_investigators.single.html. The broader, more secure "justifiable reliance" test set forth below would not permit the "general public use" standard to vitiate privacy protections. *See infra*, Section III.A.

[94] *Kyllo*, 533 U.S. at 40.

use or in development.[95]

The decision recognized the dangers presented by permitting new technology "to erode the privacy guaranteed by the Fourth Amendment,"[96] leaving individuals "at the mercy of advancing technology."[97] Thus, as the advances and enhancements of technology grow ever quicker, the Court has acknowledged the importance of adopting rules which are practical in application, and which "provide 'a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.'"[98]

3. The More Recent Supreme Court Case: *United States v. Jones*

The Supreme Court's unanimous judgment in *United States v. Jones* in 2012 reaffirmed a broad scope of protection afforded by the Fourth Amendment.[99] Writing for the majority, Justice Scalia held that the government's installation of a GPS tracker on a suspect's vehicle, together with its use of that device to monitor the movements of the target, constitutes a "search" within the meaning of the Fourth Amendment.[100] Thus, the majority upheld the traditional view of the Amendment based on property rights in a technological context—that the government's "physical intrusion" upon "private property for the purpose of obtaining information . . . would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[101]

Justice Alito, joined by Justices Breyer, Ginsburg and Kagan, concurred in the result but for different reasons.[102] They would have used Justice Harlan's test to hold that the installation and use of a GPS device violated Jones' reasonable expectation of privacy.[103] The *Jones* majority indicated that Justice Alito and his colleagues "would apply *exclusively* [the] reasonable-expectation-of-privacy test," yet the decision holds that the "reasonable-expectation-of-privacy test has been *added to*, not *substituted for*," the trespass test.[104] In essence, *Jones* holds that the privacy and property tests coexist. Thus, *Jones* repudiated

---

[95] *Id.* at 35-36.

[96] *Id.* at 34.

[97] *Id.* at 35.

[98] *Id.* at 38 (quoting Oliver v. United States, 466 U.S. 170, 181 (1984)).

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

[100] *Id.* at 949.

[101] *Id.*

[102] *Id.* at 957 (Alito, J., concurring).

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

[104] *Id.* at 952-53. Since the property test relies on a simple standard, it appears to be a threshold test: if a physical trespass has occurred, then a search has also occurred. *See id.* at 955 (Sotomayor, J., concurring) ("[T]he trespassory test applied in the majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs. The reaffirmation of that principle suffices to decide this case."). If no physical trespass has occurred, *Jones* thus appears to counsel that courts should further apply the reasonable-expectation-of-privacy test to deter-

a misconstrued belief permeating judicial opinions and scholarly articles alike—that the *Katz* Court rejected the trespass test and articulated a different analysis for search cases.[105] In fact, *Katz* intended the privacy test to complement the trespass test.[106] Similarly, *Jones* provides two overlapping privacy tests: property and expectations.

Additionally, the concurring opinions in *Jones* collectively suggest that a majority of the Court recognizes the importance of adapting Fourth Amendment principles to the digital age.[107] Justice Alito's concurrence emphasized that "what is really important" in this case is "the *use* of a GPS for the purpose of long-term tracking";[108] furthermore, he suggested that the reasonable-expectation-of-privacy test may be more appropriate in an era when technology enables the government to surreptitiously track the movements of a target.[109] The concurrence concluded that "longer term GPS monitoring in investigations of most offenses impinges upon expectations of privacy"[110]—a statement that Justice Sotomayor supported in a separate concurrence.[111]

Notably, Justice Sotomayor's opinion bridges the gap between Justice Scalia's and Justice Alito's opinions. First, she explained that the "majority's opinion reflects an irreducible constitutional minimum: When the Government physically invades personal property to gather information, a search occurs."[112] But Justice Sotomayor also acknowledged the relative ease of GPS monitoring and its low cost, and "ask[ed] whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Gov-

---

mine whether a search has occurred. *Id.* at 952-953. As set forth below, the broader "justifiable reliance" standard encompasses both of these tests. *See infra*, Section III.A.

[105] *Id.* at 950.

[106] *Id.* at 952.

[107] *Id.* at 961-64 (Alito, J., concurring).

[108] *Id.* at 961 (Alito, J., concurring). Like the "general public use" standard in *Kyllo v. United States*, this "long-term tracking" standard has no basis in the Fourth Amendment text or case law. *See supra* note 93 and accompanying text. The government may only need a few hours' worth of tracking data to uncover one's "political and religious beliefs, sexual habits and so on." *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring). Justice Alito's reliance on the "long-term" nature of the tracking appears to be based on the expenditure that traditional surveillance methods would require to achieve the same result. *Id.* at 963-964 (Alito, J., concurring). But that logic also applies to short-term GPS tracking, where technology enables the government to monitor many more suspects than it could through traditional means, even if only for a short amount of time.

[109] *Jones*, 132 S. Ct. at 961-64 (Alito, J., concurring); *see also* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?* 33 WAKE FOREST L. REV. 307, 323 (1998).

[110] *Jones*, 132 S. Ct. at 964 (Alito, J., concurring). In fact, Justice Alito's concurrence quotes the *Katz* majority about violations of "the privacy upon which [the defendant] justifiably relied." *Id.* at 960 (Alito, J., concurring).

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

[112] *Id.* (Sotomayor, J., concurring).

ernment to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[113] Finally, Justice Sotomayor recognized that courts might need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[114] Such a rule is "ill suited to the digital age," where phone numbers and contents of text messages are disclosed to cellular providers; URLs, email addresses and email contents are revealed to Internet service providers; and purchased books and medications are disclosed to online retailers.[115]

While the opinions in *Jones* collectively articulated a broader understanding of Fourth Amendment rights than that which courts have relied upon for the past half century, there is still a long way to go before Fourth Amendment privacy principles are brought in line with the massive technological changes over that same time period.[116] Indeed, the last two decades alone have given rise to technological advances that enable people to carry the equivalent of mobile personal computers with them at all times.[117] The Internet and the ubiquity of mobile devices have led to fundamental changes in methods of interpersonal communications, including the advent of email and text messaging. Moreover, the government has turned these mobile devices into an alternative method to track people's whereabouts without the need for a physical tres-

---

[113] *Id.* at 956 (Sotomayor, J., concurring).

[114] *Id.* at 957 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979) and United States v. Miller, 425 U.S. 435, 443 (1976)).

[115] *Id.* (Sotomayor, J., concurring).

[116] While attitudes differ across issues, a significant segment of the public still expects its privacy to be retained despite advancing technology. In an August 2012 AP poll, nearly six out of ten respondents (58 percent) expressed concern that "using GPS enabled devices . . . will cause [them] to lose some of [their] privacy." *The Associated Press-National Constitution Center Poll*, Aug. 2012, http://surveys.ap.org/data/GfK/AP-NCC%20Poll%20August%20GfK%202012%20Topline%20FINAL_PRIVACY.pdf. Similarly, in a June 2011 poll, nearly six out of ten respondents (57 percent) expressed disapproval of "the government intercepting [their] emails as part of a broad effort to combat terrorism." *Time Magazine/Abt SRBI Poll: Constitution Withstands Test of Time*, June 2011, http://www.srbi.com/TimePoll5380-Final%20Report-2011-06-22.pdf. Finally, in a July 2005 poll, 93% of respondents opposed "allowing police to enter a person's home at any time without a search warrant." *USA Today/CNN/Gallup Poll*, July 2005, *results available at* http://usatoday30.usatoday.com/news/nation/2005-08-03-security-lines-public-opinion_x.htm.

For a discussion of relative concerns about privacy rights vs. anti-terrorism, see Richard Sobel, *Anti-Terror Campaign Has Wide Support, Even at the Expense of Cherished Rights*, CHI. TRIB., Nov. 4, 2001, at 21.

[117] *See* United States v. Flores-Lopez, 670 F.3d 803, 804 (7th Cir. 2012) ("This appeal requires us to consider the circumstances in which the search of a cell phone is permitted by the Fourth Amendment even if the search is not authorized by a warrant. Lurking behind this issue is the question whether and when a laptop or desktop computer, tablet, or other type of computer (whether called a 'computer' or not) can be searched without a warrant—for a modern cell phone *is* a computer.") (emphasis in original).

pass.[118]

The Framers' understanding that one's "papers" and "effects" give rise to privacy interests suggests that such intangible communication methods likewise present Fourth Amendment concerns. Thus, courts require a comprehensive Fourth Amendment standard that will enable the government to appropriately gather information, while at the same time recognizing that people are afforded practical property and privacy protections promised by the Fourth Amendment in the modern era. The *Katz* majority and *Jones* unanimity provide the foundation for privacy necessary in today's digital age.

III. DEVELOPING A FOURTH AMENDMENT STANDARD FOR THE TWENTY-FIRST CENTURY

The Court's decision in *Jones* expanded privacy protections. By further modernizing the *Olmstead* trespass test beyond *Katz* to a technological era, the *Jones* Court confirmed that the reasonable-expectation-of-privacy test is not the sole method of determining a Fourth Amendment privacy violation. But Justice Alito's concurrence also recognized that, though still a source of privacy protection, the reasonable-expectation-of-privacy test is difficult to apply.[119]

To determine the full scope of the Fourth Amendment, it is necessary to analyze its text through the eyes of the Framers. The Fourth Amendment was adopted in large part as a response to the very general warrants and writs of assistance issued by the British government prior to the Revolutionary War.[120] Because such general warrants and writs of assistance could last indefinitely and did not require probable cause,[121] colonists had almost no *reasonable expectation* of privacy. Thus, if the sole privacy standard under the Fourth Amendment were the reasonable-expectation test, the equivalent of the Fourth Amendment would not have protected the colonists against the general warrants or writs of assistance that gave rise to the Amendment's text.

Reading the Fourth Amendment to condition "the right of the people to be secure in their persons, houses, papers and effects," on *expectations* of privacy, even so-called *objective* expectations, reduces rights to privileges, where the extent of those privileges is determined by official interpretation of popular belief. The reasonable-expectations test enables the government to diminish the scope of the Fourth Amendment by simply intruding and ignoring popular outcry often enough to ensure that the public no longer expects its rights to be

---

[118] *See* United States v. Skinner, No. 09-6497, 2012 WL 3289801 (6th Cir. Aug. 14, 2012) (affirming the warrantless surveillance of an individual through tracking the GPS data emitted by his cell phone).

[119] *See infra* notes 132-134 and accompanying text.

[120] *See* Chimel v. California, 395 U.S. 752, 761 (1969); James Otis, Argument Against Writs of Assistance (Feb. 24, 1761), *available at* http://www.constitution.org/bor/otis_against_writs.htm.

[121] *See* Henry v. United States, 361 U.S. 98, 100-101 (1959).

upheld. The reasonable-expectations test thus holds that, even if one personally believed that his or her rights remained intact, society's belief otherwise (whether correct or not) renders the personal belief "unreasonable." In that case, the Fourth Amendment provides no protection at all.

The *Katz* majority developed a better test that would withstand such assaults on our rights. The cornerstone was its foundational statement that "the Fourth Amendment protects people, not places."[122] The Katz majority then stated, "[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[123] "[T]he right of the people to be secure in their persons . . . and effects"[124] grants broad Fourth Amendment protections to people "[w]herever a man may be."[125] Thus, the Katz majority held that "violat[ing] the privacy upon which [a person] *justifiably relied*" constitutes a search within the meaning of the Fourth Amendment.[126]

The majority holding in *Katz* about justifiable reliance on privacy can be broken down to a two-part test determinative of whether a person's Fourth Amendment rights have been violated: (1) a person must rely on his Fourth Amendment rights, and (2) such reliance must be justifiable under the circumstances. The Court's consistent return to, reiteration and reinforcement of the *Katz* majority's justifiable reliance standard would strengthen privacy foundations and provide a more substantial and secure basis for determining, and for defending against, Fourth Amendment privacy violations.[127]

A. *Reinstating the* Katz *Justifiable Reliance Standard*

The justifiable reliance standard is broad enough to encompass both the property and privacy interests inherent in the Fourth Amendment. In essence, the justifiable reliance standard is already in place with respect to property rights—the trespass test is simply another way of framing it. In the realm of property rights, the trespass test asks whether the government intruded upon or interfered with a person's private property. If so, a search or seizure has occurred, and Fourth Amendment principles apply.

Under the justifiable reliance rubric, the trespass test would be reframed as (1) whether the defendant relied on his property interest, and (2) whether such reliance was justifiable. The answer to both questions is nearly always "yes,"

---

[122] Katz v. United States, 389 U.S. 347, 351 (1967).

[123] *Id.*

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

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

[126] *Id.* at 353 (emphasis added).

[127] Richard Sobel, Letter to the Editor in *Reading Privacy Journal's Mail—Debunking the "Expectations" Standard*, PRIVACY JOURNAL, July 2006, in response to *Do You Still Have an Expectation of Privacy?*, PRIVACY JOURNAL, June 2006; *Statement of the Cyber Privacy Project on the U.S. Supreme Court Decision in* United States v. Jones, CYBERPRIVACYPROJECT.ORG (Feb. 29, 2012).

because relying on a property rights is simply another way of saying that the defendant exercised his right to exclude—the fundamental right guaranteed by property ownership,[128] which is generally justifiable. Thus, the trespass test is merely a property-based subset of the justifiable reliance test.

While property rights are easily managed under the justifiable reliance standard based on a reframed trespass test, privacy rights require further elaboration. Despite becoming the standard Fourth Amendment analysis, the words "reasonable" and "expectation" are not present in Justice Stewart's majority opinion in *Katz*.[129] Comparing the majority's holding to the concurrence emphasizes the differences in reliability: Justice Stewart and the majority emphasize Katz's *justifiable reliance* on his privacy rights, while Justice Harlan's solo concurrence expounds upon Katz's *reasonable expectation of privacy*. Although somewhat similarly phrased, "justifiable reliance" and "reasonable expectations" carry very different connotations. Justifiable reliance presents a broader and more secure standard for courts to apply Fourth Amendment principles, particularly in the digital age, because it allows a court to decide what *should* be protected instead of merely ascertaining what people *expect* to be protected. The reasonable-expectation test may have been sufficient to resolve *Katz* correctly, but it was never intended to be, nor should it be allowed to become, the exclusive test for Fourth Amendment privacy protection.

1. Maintaining Subjective and Objective Standards

At the outset, a Fourth Amendment standard based on justifiable reliance would more effectively combine the use of subjective and objective prongs set forth in the reasonable-expectation-of-privacy test. In Justice Harlan's concurrence, the first prong is whether the defendant had a subjective expectation of privacy in the area invaded, and the second prong is whether society is prepared to accept that the area invaded is subject to a reasonable expectation of privacy.[130]

Under the broader justifiable reliance test, however, courts need to determine (1) whether the individual relied on his privacy by seeking to preserve something as private, and (2) whether the defendant's reliance, "viewed objectively, is 'justifiable' under the circumstances."[131] As set forth below, the first prong would typically be fulfilled, as most individuals can show that they object to unwarranted governmental intrusions when they are in their homes, in their cars, in an enclosed telephone booth, or accessing their private, password-pro-

---

[128] Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) ("One of the main rights attaching to property is the right to exclude others.").

[129] *Katz*, 389 U.S. at 348-59.

[130] *Id.* at 361 (Harlan, J., concurring); *see* Smith v. Maryland, 442 U.S. 735, 741 (1979).

[131] *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 351, 353). *Smith* used the correct formulation, in which the circumstances are relevant to whether the reliance was justifiable. Unfortunately, this important language was lost in subsequent cases.

tected correspondence and data. The second prong may present a closer question, but a determination of whether an individual's reliance is justifiable presents a more consistent standard than relying on a court's ability to pinpoint personal or societal expectations regarding the extent of privacy protections. The former is based on legal norms, and the latter is based on a court's subjective survey of a sometimes fickle and potentially uninformed citizenry. Additionally, a standard based on expectations encourages governmental misbehavior, because if government can usurp rights long enough, society may become skeptical about the extent of those rights, and individuals may lose the ability to prove either individual (subjective) or societal (objective) expectations of those rights.

2. "Reliance" vs. "Expectations"

The words "reliance" and "expectations" mean different things, and the dependence of Fourth Amendment rights on expectations, rather than reliance, has had profound effects over the last half-century, contrary to the *Katz* majority. Reliance means that a person depends upon his or her privacy: that the person objects to the governmental intrusion at the time it occurred (or, if he was unaware of the intrusion at that time, would have objected then or did object upon learning of the intrusion).

In lay terms, the reliance may take the simple form of "The government can't do that! I have my rights!" A lawyer might argue that the government may not conduct the proposed search or seizure without establishing, before a neutral magistrate, the existence of probable cause. But the question for the layman, and eventually the courts, would be simple: Did the defendant rely on his Fourth Amendment privacy rights to restrict, prevent or object to the governmental search or seizure?

By contrast, "expectations of privacy" are significantly more amorphous, in particular, because an "expectation" invokes a time-based belief. Expectations of privacy may differ from person to person and from day to day. As a result, courts interpreting the Fourth Amendment "struggle to apply the 'reasonable expectation of privacy' test and reach contradictory results when they do."[132] Indeed, as noted by Justice Alito in *Jones*, "judges are apt to confuse their own expectations of privacy with those of the hypothetical reasonable person to which the *Katz* test looks."[133] Moreover, such expectations often fluctuate in the face of the rapid pace of technological evolution.[134]

---

[132] Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA JOURNAL (Aug. 1, 2012, 4:20 AM), http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited/.

[133] United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring).

[134] *Id.* (Alito, J., concurring) ("[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and *stable* set of privacy expectations. But technology can change those expectations. *Dramatic technological change may lead to periods*

Today, some people freely share through Facebook and other social media information that only a decade ago was considered to be highly private.[135] Such rapid changes raise vexing questions. Which of those people determine society's view today: the consistent Facebook sharer, or the person who shreds every piece of incoming mail? How does a court make that decision? Is it factual, or a matter for judicial notice? Who has the burden of proof? Asking litigants and courts to define whether a particular expectation of privacy is one that society is willing to accept as reasonable is difficult, and highly likely to yield inconsistent results.[136]

More importantly, *expectations* of privacy are at risk of being molded or controlled over time by unchallenged governmental intrusions on Fourth Amendment rights. In the last decade since the September 11 terror attacks, the governmental security complex has vastly increased.[137] As airport security measures have changed from the use of magnetometers to the introduction of whole body scanners ("WBS") and enhanced pat-downs, people's *expectations* of privacy may have already decreased. Despite the efforts of many to require the government to justify and restrict these intrusions, the enhanced airport searches continue.[138] If the government continues its intransigence long enough, no citizen will be able to prove a societal expectation of privacy, even though society's preference for maintaining privacy never changed. By contrast, despite the dashed expectation, individuals could argue that they rely on security in their private affairs, and that their reliance is justifiable.

As the United States increases surveillance of citizens, whether through intercepting emails and text messages, or through GPS, WBS, and drone monitoring, it can forcibly diminish society's *expectations* about the scope of their privacy rights. With enough time, the government could eliminate virtually any expectation of privacy. But such a situation is exactly when Fourth Amendment privacy principles are most needed.

Tying the extent of Fourth Amendment privacy rights to a court's interpretation of what individuals or society *expect* necessarily limits those rights. This is particularly troublesome in the digital age when, as Justice Sotomayor notes,

---

in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes.") (emphases added).

[135] *See, e.g.*, Rose Golijan, *Consumer Reports: Facebook Privacy Problems Are on the Rise*, NBCNEWS.COM (May 3, 2012), http://www.nbcnews.com/technology/technolog/consumer-reports-facebook-privacy-problems-are-rise-749990.

[136] Nojeim, *supra* note 132. *See also* Richard Sobel & Ramon Torres, *The Right to Travel, a Fundamental Right of Citizenship,* 80 J. TRANSP. L. LOGIST. & POL'Y (forthcoming 2013).

[137] *See, e.g.*, Tom Engelhardt, *Our Nation's National Security Complex*, MOTHERJONES .COM (July 19, 2012, 11:47 AM), http://www.motherjones.com/politics/2012/07/our-nations-national-security-complex.

[138] *See, e.g.*, Glenn Greenwald, *Government Yells "Terrorism" to Justify TSA Procedures*, SALON.COM (Nov. 23, 2010), http://www.salon.com/2010/11/23/tsa_3/.

technology exists "that enables the Government to ascertain, more or less at will, [any person's] political and religious beliefs, sexual habits, and so on."[139] Moreover, Justice Sotomayor's timely warning that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"[140] becomes increasingly pertinent. In today's world, people must disclose phone numbers, email addresses, and Internet addresses, as well as what books, groceries and medications they purchase and use, to third-party service providers.[141] Thus, with the third party doctrine in effect, it is clear that expectations are overly limiting as a source of privacy protections. Revisiting the third party doctrine in light of *Jones* would create more consistent privacy protections for information shared confidentially between private parties.

Fourth Amendment rights should not ebb and flow with judicial interpretations of immeasurable, temporary societal expectations. Rather, as the *Katz* Court held, privacy rights are anchored in an understanding of whether one's reliance on his or her privacy is justifiable.[142] In short, the Fourth Amendment protects people, wherever they are, no matter how strong or weak their expectations of privacy may be. For the reasons set forth above, it is much easier for a court to determine if someone relied upon privacy rather than expected a privacy interest to be maintained. Thus, courts should look to what an individual's privacy interests are and whether the individual relied on her rights, rather than whether she expected her rights to be upheld.

3. "Justifiable" vs. "Reasonable"

The words "justifiable" and "reasonable" likewise do not mean the same

---

[139] *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring).

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

[141] *Id.* (Sotomayor, J., concurring).

[142] By analogy, Justice Black's articulation in the context of contracts in *City of El Paso v. Simmons* demonstrates that the justifiable reliance standard presents firmer foundations for privacy:

> The Contract Clause was included in the same section of the Constitution which forbids States to pass bills of attainder or *ex post facto* laws. All three of these provisions reflect the strong belief of the Framers of the Constitution that men should not have to act at their peril, fearing always that the State might change its mind and alter the legal consequences of their past acts so as to take away their lives, their liberty or their property. James Madison explained that the people were "weary of the fluctuating policy" of state legislatures and wanted it made clear that under the new Government men could safely rely on States to keep faith with those who justifiably relied on their promises.

City of El Paso v. Simmons, 379 U.S. 497, 591 (1965) (Black, J., dissenting) (emphasis added) (quoting THE FEDERALIST, No. 44, at 301 (James Madison) (Cooke ed., 1961)). As with private contracts, people need to be able to rely on the promises of Fourth Amendment protections against altering the social contract between the people and their government—regardless of developing conceptions, technologies or expectations.

thing. An action that is reasonable is typically regarded as one that is rational or logical, while an action that is justifiable need only be defensible, or capable of being shown to be right. Thus, under the reasonable-expectation-of-privacy standard, courts must make a determination as to whether society would regard the privacy expectation as reasonable.[143] As noted above, however, expectations differ and change, so courts interpreting the Fourth Amendment often reach contradictory results.[144] The difficulties arise because courts are forced to decide whether society as a whole would regard a given expectation of privacy as rational or logical. Additionally, Justice Harlan's substitution of "reasonable" for "justifiable" unnecessarily drew the legal history of the hypothetical "reasonable man" standard into Fourth Amendment analyses.

The Supreme Court has previously elaborated on the meaning of "justifiable reliance" based on that term's usage in Sections 537 and 540 of the Restatement of Torts.[145] In the context of a fraud case, the Restatement requires "both actual and 'justifiable' reliance."[146] The Court explained that "[t]he Restatement expounds upon justifiable reliance by explaining that a person is justified in relying on a representation of fact 'although he might have ascertained the falsity of the representation had he made an investigation.'"[147] Even where an investigation would be as simple as "walking across the street [where one] could easily learn" that the representation is false, reliance on the representation can still be justified.[148]

Thus, the Court points to a clear "contrast between a justifiable and [a] reasonable reliance":

> Although the plaintiff's reliance on the misrepresentation must be justifiable . . . , this does not mean that his conduct must conform to the standard of the reasonable man. Justification is a matter of the qualities and characteristics of the particular plaintiff, and the circumstances of the particular case, rather than the application of a community standard of conduct to all cases.[149]

The *Katz* majority's justifiable reliance standard provides a more secure basis for constitutional privacy rights than "reasonableness" as determined by the public. The Fourth Amendment prohibits "unreasonable searches and seizures," meaning that searches and seizures must be "reasonable." However, the text of the Fourth Amendment does not mandate that objections to govern-

---

[143] Smith v. Maryland, 442 U.S. 735, 740 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[144] Nojeim, *supra* note 132.

[145] Field v. Mans, 516 U.S. 59, 70-71 (1995).

[146] *Id.* at 70 (quoting RESTATEMENT (SECOND) OF TORTS § 537 (1977)).

[147] *Id.* (quoting RESTATEMENT (SECOND) OF TORTS § 540).

[148] RESTATEMENT (SECOND) OF TORTS § 540 illus. 1.

[149] *Field*, 516 U.S. at 70-71 (quoting RESTATEMENT (SECOND) OF TORTS § 545A cmt. b) (emphasis added).

mental intrusion or reliance on one's privacy must be "reasonable" or based on "reason." If the *Katz* majority felt that "reasonable" expectations or reliance was a proper standard, they would have said as much. Instead, they avoided the use of "reasonable" relative to *Katz*'s reliance, and instead drew on the firmer conception of whether that reliance was justifiable.

Another fundamental problem with the requirement of "reasonable" expectations is that privacy intrusions and the harm accruing therefrom are not based on logic or rationality. The harm inherent in privacy violations is an intrusion on one's self and one's sense of self, including emotional distress.[150] When state actors search a person's body or effects without constitutional justification, particularly in the context of a pat-down or strip search, the harm experienced by the individual can be both tangible and emotional.[151] When state actors search one's home without probable cause, the owner of the home objectively experiences intrusion and feels emotionally violated because one's home is his or her private sanctuary—or castle.[152] The Framers understood that a search by state actors of one's "papers"—one's private letters and correspondence—would likewise violate bounds of decency. This is because citizens of a free society justifiably believe that their private thoughts, shared in written form, should be read only by their intended recipients. Thus, the government violates the Fourth Amendment when it intercepts and opens mail without a warrant, *even if the mail is in the possession of an arm of the government*, the United States Postal Service.[153] Even more than a search of one's person or house, an unjustified search of one's private correspondence would be akin to the government probing one's mind.[154]

Since part of the harm caused by privacy violations arises in the form of emotional distress, the law of emotional distress can also inform the *methodology* of Fourth Amendment analyses.[155] Because Fourth Amendment privacy vi-

---

[150] Doe v. Chao, 540 U.S. 614, 634 (2004) (Ginsburg, J., dissenting) (finding that Privacy Act violations commonly cause "fear, anxiety, or other emotional distress").

[151] This is especially true in the case of people who have experienced sexual abuse. Kate Daily, *For Survivors of Sexual Assault, New TSA Screenings Represent a Threat*, NEWSWEEK (Nov. 17, 2010 5:45 PM), *available at* http://www.thedailybeast.com/newsweek/2010/11/17/tsa-screenings-worry-sexual-assault-survivors.html.

[152] Minnesota v. Carter, 525 U.S. 83, 84 (1998); *see* Semayne's Case, (1572) 77 Eng. Rep. 194 (K.B.) 195.

[153] United States v. Jacobsen, 466 U.S. 109, 114 (1984).

[154] United States *ex rel.* Milwaukee Soc. Democratic Publ'g Co. v. Burleson, 255 U.S. 407, 437 (1921) (Holmes, J., dissenting) (stating that "the use of the mails is almost as much a part of free speech as the right to use our tongues"); see *Jacobsen*, 466 U.S. at 114 ("Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy; warrantless searches of such effects are presumptively unreasonable."); Ex Parte Jackson, 96 U.S. 727, 733 (1877).

[155] The law of emotional distress should not be used to inform the *standard* for Fourth Amendment violations because such violations are limited to persons enforcing federal and

olations can cause such emotional harm or distress, the Restatement of Torts provides some additional guidance on when one's reliance on his privacy is justifiable. Specifically, comment (d) to Section 46 holds that conduct arousing the resentment of "an average member of the community" is intolerable and would lead to liability.[156] While the term "justifiable" may depend on "the plaintiff and the circumstances of the case," the response of an "average" community member provides a more secure and objective foundation for determining privacy violations than the recourse to a court's estimation of the expectations of a hypothetical reasonable person or of society.

To be clear, "penetrating" and "indiscriminate" technological intrusions are "truly obnoxious to a free society,"[157] and such intrusions may invoke constitutional protections regardless of the average citizen's response or expectations. Intrusions need not meet the standard or even be recognized at the time to violate the Fourth Amendment.[158] But if they do, the resentment or outrage of an "average member of the community"[159] (the Restatement methodology) provides a better approach for determining Fourth Amendment violations than courts' conflicting estimations of the reasonable expectations of a hypothetical individual or society as a whole. Courts would only ask how an average (though not necessarily reasonable) person would respond to the governmental intrusion.

B. *The Justifiable Reliance Standard in Practice*

1. The Justifiable Reliance Standard and *Kyllo*

The Court's holding in *Kyllo v. United States*[160] purports to be based on

---

state law, whereas the law of emotional distress applies to everyone, including private actors. Since private actors are not subject to constitutional constraints, the standard for suing a private actor should be higher than the standard that applies to state actors. In addition, the police have an option not available to private actors: They can get a warrant; and if they do, they can proceed without fear of a lawsuit. The very existence of the warrant alternative means that state actors should be far more circumspect about their intrusions when they choose not to get one.

[156] RESTATEMENT (SECOND) OF TORTS § 46, cmt. d (1965) (emphases added). The section entitled "Outrageous Conduct Causing Severe Emotional Distress" holds that liability attaches where the conduct is so outrageous "as to go beyond all possible bounds of decency, [so] as to be regarded as atrocious, and utterly intolerable in a civilized community. Generally, the case is one in which the recitation of the facts to an average member of the community would arouse his resentment against the actor, and lead him to exclaim, 'Outrageous!'" *Id.*

[157] *See* Lopez v. United States, 373 U.S. 427, 466 (1962) (Brennan, J., dissenting).

[158] Both the objective extent and subjective impression of the intrusion may be somewhat mitigated (and in fact, potentially avoided) by respecting the Fourth Amendment's requirement to get a search warrant from an impartial magistrate.

[159] RESTATEMENT (SECOND) OF TORTS § 46, cmt. d (1965).

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

reasonable expectations of privacy, but the holding would have had firmer foundations if it were based on the broader justifiable reliance standard. Since the police used a thermal imager to detect heat emanating from within the house, there was no physical trespass.[161] Thus, the reasonable-expectation test was the basis for the holding "that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area' constitutes a search—at least where (as here) the technology in question is not in general public use."[162] In reaching that holding, Justice Scalia noted that the Fourth Amendment "protected Katz from the warrantless eavesdropping because he 'justifiably relied' upon the privacy of the telephone booth."[163] Justice Scalia then pointed out that the reasonable-expectation test "has often been criticized as circular and hence subjective and unpredictable."[164] Still, the majority claimed that its opinion is based on the reasonable-expectation test only because, for the interior of a home, "there is a ready criterion, with roots deep in the common law, of the minimal expectation of privacy that *exists*, and that is acknowledged to be *reasonable*."[165] The majority does not explain why homeowners might reasonably expect that the heat emanating beyond the interior of the home would remain private.[166]

Thus, the *Kyllo* majority stretched the reasonable-expectation test to suit its purpose of upholding increased privacy protections for the interior of the home. But the justifiable reliance standard would have been a more apt basis for reaching the same conclusion. There is no question that Kyllo relied on his property and privacy rights by moving to suppress the evidence based on the thermal imaging.[167] Concerning the second prong, the majority believed that Kyllo's reliance on his Fourth Amendment rights was justifiable because the heat lamps were concealed within the privacy of Kyllo's home, which has long been established to be one's private sanctuary (or castle).[168] Thus, the majority felt that the use of extrasensory tools (meaning anything other than one's own senses) to ascertain the contents within a concealed home would alter the relationship between citizen and government by obviating the need for physical intrusion.[169] Accordingly, *Kyllo* presents a situation where the reasonable-ex-

---

[161] *See id.* at 29-30.

[162] *Id.* at 34.

[163] *Id.* at 33.

[164] *Id.* at 34.

[165] *Id.* (emphases in original).

[166] *Id.* at 43-46 (Stevens, J., dissenting). As the dissent points out, such heat can be deduced from outside of the home, even without the need for sense-enhancing technology. *Id.* at 44 (Stevens, J., dissenting).

[167] *Id.* at 30.

[168] Minnesota v. Carter, 525 U.S. 83, 84 (1998); *see* Semayne's Case, (1572) 77 Eng. Rep. 194 (K.B.) 195.

[169] *See Kyllo*, 533 U.S. at 34 ("This assures preservation of that degree of privacy against

pectation test was molded to particular facts, but where the justifiable reliance test would have equally upheld the privacy interests, and on firmer grounds.

2. The Justifiable Reliance Standard and *Jones*

Had the justifiable reliance standard from the *Katz* majority been more prominent when the Supreme Court decided *Jones*, the Court would likely have reached the same result, but without the dispute among the Justices about the proper test. *Jones* clearly relied on both his property and privacy interests in objecting to the government's attachment of a GPS device on his car.[170] The issue then becomes whether such reliance was justifiable under the circumstances. On the basis of property, the answer is clearly yes: Jones had a right to exclude the government from intruding upon his private property for the purpose of obtaining information.[171] Jones' reliance on his privacy interests is also justifiable because the government's surreptitious location tracking goes "beyond all possible bounds of decency" and is "intolerable" in a civilized, democratic society.[172] An average member of the community—upon hearing the government claiming the unfettered right to surreptitiously track the whereabouts of any citizen without having obtained a warrant based upon probable cause—would almost certainly experience resentment against the government.[173]

The majority decision and Justices Alito and Sotomayor's concurrences all lend support for the idea that the Court believed such warrantless surreptitious tracking offends the Constitution and the public's sense of outrage. The majority bases its conclusion on the understanding that "[t]he Government physically occupied private property for the purpose of obtaining information."[174] It relies on the mid-eighteenth century *Entick* case that states:

> "[O]ur law holds the property of every man so *sacred*, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, though he does no damage at all; if he will tread upon his

---

government that existed when the Fourth Amendment was adopted."); United States v. Jones, 132 S. Ct. 945, 954 (2012) (although traditional surveillance for four weeks would require extensive resources and such visual observation may be constitutionally permissible, suggesting that "achieving the same result through electronic means, without an accompanying trespass, [may be] an unconstitutional invasion of privacy"). *See generally* Richard Sobel & John Fennell, *Troubles with Hiibel: How the Court Inverted the Relationship Between Citizens and the State*, 18 S. TEX. L. REV. 613 (2007).

[170] *See Jones*, 132 S. Ct. at 957 (Alito, J., concurring) ("By attaching a small GPS device to the underside of the vehicle that respondent drove, the law enforcement officers in this case engaged in conduct that might have provided grounds in 1791 for a suit for trespass of chattels.").

[171] *Id.* at 949.

[172] RESTATEMENT (SECOND) OF TORTS § 46 cmt. d.

[173] *Id.*

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

neighbour's ground, he must *justify* it by law."[175]

In other words, society would view such a governmental physical intrusion on private property as intolerable because private property is sacred.

Justice Sotomayor concurs, using strong language to condemn the government because it "usurped Jones' property for the purpose of conducting surveillance on him, thereby invading privacy interests long afforded, and undoubtedly entitled to, Fourth Amendment protection."[176] After discussing the potential evils of GPS monitoring by the government—including "chill[ing] associational and expressive freedoms [and] the Government's unrestrained power to assemble data" being "susceptible to abuse"[177]—Justice Sotomayor makes the following conclusion:

> The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society."[178]

In the context of what society would consider a reasonable expectation of privacy, Justice Sotomayor speculates: "I for one doubt that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year."[179] Her conclusion is inescapable: The government's warrantless GPS monitoring of individuals constitutes a Fourth Amendment search because such an unchecked abuse of governmental power is so beyond the bounds of decency and intolerable in our democratic society that it clearly violates citizens' privacy interests.

Finally, Justice Alito's concurrence argued that the trespass—the *property* intrusion—in *Jones* was relatively minor, and that "what is really important" in the case was the *privacy* intrusion—"the use of a GPS for the purpose of long-term tracking."[180] In the context of the reasonable-expectation-of-privacy test, Justice Alito noted that society has believed "that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual's car for a very long period."[181] Indeed, Justice Alito also quoted the majority's justifiable reliance holding of *Katz*, stating that "[w]hat mattered, the Court now held, was whether the conduct at issue 'violated the privacy upon which [the defendant] justifiably relied while using the telephone

---

[175] *Id.* (quoting Entick v. Carrington, (1765) 95 Eng. Rep. 807 (C.P.) 817) (emphases added).

[176] *Id.* at 954 (Sotomayor, J., concurring).

[177] *Id.* at 956 (Sotomayor, J., concurring).

[178] *Id.* (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

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

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

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

booth.'"[182]

Despite his failure to explain why short-term tracking might be acceptable while long-term tracking constitutes a search, Justice Alito's concurrence appears to be grounded in his conviction that the government's secret surveillance and cataloguing of "every single movement of an individual's car" is unacceptable. Thus, a majority of the Court would likely agree that Jones justifiably relied on his privacy to object to the government's attaching a GPS device to his car to continuously monitor his whereabouts.

After *Jones*, courts should recognize that such an official property trespass and privacy intrusion requires warrants under probable cause. Since *Katz* held that "the Fourth Amendment protects people, not places," anything a person seeks to "preserve as private, even in an area accessible to the public, may be constitutionally protected."[183] Indeed, most people seek to preserve as private the wealth of information that could be divined by knowledge of their daily movements. Even short-term monitoring will disclose to the government movements of an "indisputably private nature [such as] trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on."[184]

As such, the *Jones* Court should have gone one key step further: Because the Court found the intrusion to be a search, the police needed a valid warrant under probable cause to probe into a target's daily movements. Additionally, since such private details (and many others) could likewise be divined by government access to text messages, emails and other Internet accounts, particularly those containing online history, the government also needs a warrant to access that information. The ruling in *Jones* clearly defines what constitutes a technological search and extends all of our privacy protections while providing useful guidance to law enforcement. Now the Court should establish that warrants for cause are needed to attach the device, to access the information, and to trace an individual's movements.

3. Privacy in the 21st Century: The Justifiable Reliance Standard Applied to Internet Communications and Data

The best example of the reasonable-expectation test failing where the justifiable reliance standard holds true is in the realm of Internet communications,

---

[182] *Id.* at 960 (Alito, J., concurring) (quoting Katz v. United States, 389 U.S. 347, 353 (1967)). Justice Alito also noted Justice Brandeis' dissent in *Olmstead*, which argued that the "[Fourth] Amendment should be understood as prohibiting 'every unjustifiable intrusion by the government upon the privacy of the individual.'" *Id.* at 959 (Alito, J., concurring) (quoting Olmstead v. United States, 277 U.S. 438, 478 (1928)).

[183] *Katz*, 389 U.S. at 351-53.

[184] *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring) (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

stored data and "cloud"[185] computing. Current Fourth Amendment jurisprudence holds "that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[186] It remains open to question whether the contents of emails and personal data, which are stored on remote servers owned and operated by third party Internet service providers, are subject to Fourth Amendment protection.[187] As in wiretaps, there is no physical intrusion when the government seeks information from a third party server, and the very existence of the emails or data in the hands of third parties suggests that they are not subject to reasonable expectations of privacy.[188] Thus, while many believe that their intimate email conversations and remotely-stored personal data should be constitutionally protected from unwarranted governmental intrusion, the traditional trespass test and reasonable-expectations test provide insufficient legal bases for that result.[189]

However, the broader justifiable reliance test need not be equally constrained by the third party doctrine because the relevant question is whether one's reliance, "viewed objectively, is 'justifiable' under the circumstances."[190] While emails and data are stored by third parties, this does not mean that the emails and data are actually *disclosed* to third parties; rather, access to those emails and data is typically restricted through the use of passwords and data encryption technology.[191] Further, a third party's ability to access stored emails or data does not vitiate justifiable reliance on the security protections of passwords.[192] Passwords may be hacked, locks can be picked, and "a rogue mail

---

[185] Online "cloud" storage as a method for backing up private computer files has become popular in recent years. *See, e.g.*, Bill Snyder, *Dirty Secrets of Dropbox, Google Drive and Other Cloud Storage Services*, CIO.COM (Nov. 16, 2012), http://blogs.cio.com/cloud-computing/17574/dirty-secrets-dropbox-google-drive-and-other-cloud-storage-services.

[186] *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979) and United States v. Miller, 425 U.S. 435, 443, (1976)).

[187] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1210-11 (2004). Though this article was published over eight years ago, the question remains open today—only one court of appeals has held that email contents are protected under the Fourth Amendment. *See* United States v. Warshak, 631 F.3d 266, 283-288 (6th Cir. 2010).

[188] *See* note 186, *supra*, and accompanying text.

[189] Some might refer to that belief as an "expectation," but the third party doctrine holds that such an expectation would not be "reasonable," even though it is likely that a majority of citizens would prefer that their email correspondence remain private.

[190] *Smith*, 442 U.S. at 740 (quoting Katz v. United States, 389 U.S. 347, 351, 353 (1967)).

[191] Even if email and data are disclosed merely through remote storage, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes." *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (quoting *Smith*, 442 U.S. at 749 (Marshall, J., dissenting)).

[192] *See Warshak*, 631 F.3d at 286-287.

handler [can] rip open a letter."[193] While such possibilities may be judged "reasonable," they do not render it unjustifiable for one to rely on the privacy provided by passwords, locks and sealed envelopes. Thus, password-protected, remotely-stored emails and data represent a perfect example of how justifiable reliance is stronger and more secure than the reasonable-expectations test. The justifiable reliance standard relates to what privacy protections one should be able to depend on, whereas the current standard, as modified and diluted by the third party doctrine, has allowed the reasonableness of governmentally-lowered expectations to guide Fourth Amendment decisions.[194]

C. *Troubling Developments After* Jones

1. *United States v. Flores-Lopez*

Unfortunately, *Jones*' bright-line technological search rule for law enforcement has already been muddled by subsequent misunderstandings in courts of appeals. Shortly after the Supreme Court's decision in *Jones*, the Seventh Circuit decided *United States v. Flores-Lopez*.[195] There, the defendant was arrested and his cell phone was searched by the police for the purpose of identifying the cell phone number.[196] The phone's contents were then used to obtain evidence from the phone company that aided in the defendant's conviction.[197] The court held that the search did not violate the Fourth Amendment, and that no warrant was required because the search was "minimally invasive" (a concept created in another 1991 Seventh Circuit opinion).[198] Despite the government's trespass on the defendant's private property (his cell phone), the court decided the issue entirely on privacy grounds.

In the context of holding that the search at issue was reasonable without a warrant, the court recognized several facts, including that: (1) "a modern cell phone is a computer";[199] (2) a modern cell phone (a "smartphone") "is in one aspect a diary writ large . . . [which] is quite likely to contain, or provide ready

---

[193] *Id.* at 287.

[194] While increased governmental surveillance over the last decade may have decreased *expectations* of privacy, justifiable reliance on privacy and preferences for maintaining it may have remained constant or even heightened in reaction to these intrusions. *See* Section III.A.2, *supra*.

[195] United States v. Flores-Lopez, 670 F.3d 803, 804 (7th Cir. 2012).

[196] *Id.* at 804-05.

[197] *Id.*

[198] *Id.* at 807 (citing United States v. Concepcion, 942 F.2d 1170, 1172-73 (7th Cir. 1991)). The claim that an intrusion is "minimally invasive," or that a warrant is not required because the amount of information obtained was minimal, contradicts Justice Scalia's statement in *Kyllo*, which noted that Fourth Amendment principles have "never been tied to measurement of the quality or quantity of information obtained." Kyllo v. United States, 533 U.S. 27, 37 (2001).

[199] *Flores-Lopez*, 670 F.3d at 804.

access to, a vast body of personal data";[200] (3) "[t]he potential invasion of privacy in a search of a [smart]phone is greater than in a search of a 'container' in a conventional sense even when the conventional container is a purse that contains an address book (itself a container) and photos";[201] (4) in the context of Fourth Amendment law, computers and smartphones are unlike other containers or physical objects because they "hold so much personal and sensitive information touching on many private aspects of life [and there] is a far greater potential for the 'inter-mingling' of documents and a consequent invasion of privacy when police execute a search for evidence on a computer";[202] and (5) "[e]ven the dumbest of [smart]phones gives the user access to large stores of information."[203]

In spite of all of these factors, the Seventh Circuit found the search to be reasonable because precedents had established that police officers can look through an arrestee's address book[204] or his diary "to verify his name and address and discover whether the diary contains information relevant to the crime for which he has been arrested,"[205] and because the phone number sought was devoid of privacy interests due to its disclosure to a third party: the phone company.[206] But this entire discourse neglects the simple fact that, like the Court's holding in *Jones*, the government's search of a cell phone's contents would be a *physical* intrusion upon private property for the purpose of obtaining information, and would therefore constitute a search within the meaning of the Fourth Amendment.[207]

More fundamentally, *Flores-Lopez* encapsulates the adage about hard cases and bad law. The police in that case may have sought only to discover the defendant's cell phone number, but police officers are rarely such paragons of restraint. The government emphasized, and the court theorized, other "imag-

---

[200] *Id.* at 805.

[201] *Id.*

[202] *Id.* (quoting United States v. Lucas, 640 F.3d 168, 178 (6th Cir. 2011)).

[203] *Id.* at 806.

[204] *Id.* at 807 (citing United States v. Rodriguez, 995 F.2d 776, 778 (7th Cir. 1993)).

[205] *Id.* The diary precedent is not specifically cited by the opinion, but that precedent gives rise to serious privacy concerns. The decision also recognizes a different, unidentified precedent holding that police officers are "forbidden to peruse love letters recognized as such found wedged between the pages of [an] address book." *Id.* Diaries are equally likely to contain "love letters" or similar personal monologues as they are to contain names or information relevant to crimes. It is highly unlikely that society or the average member of a community would *expect* that police without a warrant are legally authorized to rifle through a person's most private thoughts merely because they were memorialized in a book or computer which happened to be within arm's length at the time the person was arrested.

[206] *Id.* As noted above, Justice Sotomayor believes, and we concur, about the necessity of reconsidering the third-party doctrine, which is "ill suited to the digital age." United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

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

ine[d] justifications for a more extensive search" of the smartphone, such as that an "arrested suspect might have prearranged with co-conspirators to" scatter or remotely wipe the smartphone.[208] Such theoretical statements damage the cause of privacy—when a police officer searches more extensively through an arrestee's smartphone, the government will cite this opinion to support its justification.

Moreover, such rationalizations discount the Supreme Court's admonitions in *Kyllo* about not permitting technology "to erode the privacy guaranteed by the Fourth Amendment"[209] and leaving individuals "at the mercy of advancing technology."[210] Courts must guard against granting technological advantages to police officers while expecting civilians to accept technological benefits with severely diminished Fourth Amendment rights. While the search of the defendant's smartphone was limited to the phone number in the *Flores-Lopez* case, the Seventh Circuit should have instead set a bright-line rule based on *Jones*' trespass holding: Even if a person has been arrested, police officers may not physically intrude upon that person's smartphone, tablet, computer or other device for the purpose of obtaining information without securing a warrant from a neutral magistrate particularly describing the thing to be searched.[211] Paraphrasing the *Katz* majority, "[t]o read the Constitution more narrowly is to ignore the vital role that [such computers and mobile devices have] come to play in private communication."[212]

Under the proposed justifiable reliance test, for both property and privacy interests, the facts of the *Flores-Lopez* case would have upheld the defendant's privacy in the information in his cell phone. First, as stated above, the trespass test dictates that police cannot intrude upon an individual's private property for the purpose of obtaining information. Thus, Flores-Lopez relied on his proper-

---

[208] *Flores-Lopez*, 670 F.3d at 808-10.

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

[210] *Id.* at 35.

[211] In this and other recent cases like *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012), the government appears to argue that it must be entitled to search all such devices to obtain or preserve evidence of crimes, especially the identity of co-conspirators. *See, e.g.*, *Flores-Lopez*, 670 F.3d at 808-10. But given the privacy implications of permitting police officers to rummage through one's personal data solely to find additional incriminating evidence and identities of other potential criminals, courts should lean towards enforcing the warrant requirement. While doing so may result in slower or decreased prosecutions, the benefit to overall privacy and liberty would be substantial. Besides (though this is worthy of another article entirely), the vastly increased incarceration rate in recent decades, together with the unsustainable increase in correctional expenditures—both substantially due to a failed war on drugs—suggest that our nation's priorities should be reconsidered. *See, e.g.*, Fareed Zakaria, *Incarceration Nation*, TIME, Apr. 2, 2012, at 18; Veronique de Rugy, *"Prison Math" and the War on Drugs*, NAT'L REV., June 9, 2011, *available at* http://www.nationalreview.com/corner/269208/prison-math-and-war-drugs-veronique-de-rugy.

[212] Katz v. United States, 389 U.S. 353, 352 (1967).

ty rights in his cell phone, and was justified under the circumstances in attempting to exclude the police from intruding upon his property.

Second, under the privacy rubric, Flores-Lopez objected to the invasion of privacy,[213] so the question becomes whether this reliance on Fourth Amendment rights is justifiable. Since smartphones contain a wealth of intimate information in the form of text messages, e-mails and other personal data, it is highly likely that an average member of the community would be outraged or at least strongly object to the police rifling through one's smartphone merely as an incident to arrest. It is noteworthy that decreased privacy protections in this case were not required to convict the defendant. The evidence against Flores-Lopez included an overheard phone conversation in which he identified a garage where he would deliver the drugs, and an undercover agent was on-site at the garage upon delivery, where Flores-Lopez was arrested with the drugs.[214] Thus, the justifiable reliance standard would provide broader privacy protections for all, even if the result is still a conviction for the defendant.

2. *United States v. Skinner*

Seven months after the Supreme Court's decision in *Jones*, the Sixth Circuit decided *United States v. Skinner*.[215] This case also involved the use of GPS tracking, but unlike in *Jones*, police monitored the defendant through "data emanating from Melvin Skinner's pay-as-you-go cell phone to determine its real-time location."[216] Here, the Sixth Circuit reasoned within the limitations of *Jones*, namely, (1) the majority holding focusing on the trespass test, (2) the Court's failure to articulate that a warrant was required for such a search, and (3) Justice Sotomayor's concurrence that the majority holding "provides little guidance on 'cases of electronic or other novel modes of surveillance that do not depend upon physical invasion on property.'"[217] The Sixth Circuit held that "Skinner did not have a reasonable expectation of privacy in the data given off by his voluntarily procured pay-as-you-go cell phone."[218] The court's analysis concisely demonstrates why using a test based on expectations of privacy is confusing, unreliable and yields contradictory results.

The facts of the case are straightforward: law enforcement agents tracked the data given off by Skinner's phone, though "[a]t no point did agents follow the vehicle or conduct any type of visual surveillance."[219] Rather, the authorities continually "pinged" Skinner's phone and intercepted phone calls, and when

---

[213] *Flores-Lopez*, 670 F.3d at 804-805.

[214] *Id.* at 804.

[215] *Skinner*, 690 F.3d 772.

[216] *Id.*

[217] *Id.* at 780 (quoting United States v. Jones, 132 S. Ct. 945, 955 (2012) (Sotomayor, J., concurring)).

[218] *Id.* at 777.

[219] *Id.* at 776.

the police caught up with Skinner, a K-9 officer's dog alerted officers to the likely presence of narcotics in Skinner's motor home.[220] As Judge Donald noted in his concurring opinion—which disagreed with the majority that Skinner had no reasonable expectation of privacy in his cell phone location data—the officers in this case never actually identified Skinner until they knocked on the motor home's door.[221]

The majority opinion is troubling because it inverts logic and law by holding that Skinner had no reasonable expectation of privacy, in some respects, as a result of his criminal activity: "If a tool used to transport contraband gives off a signal that can be tracked for location, certainly the police can track the signal. The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools."[222] Despite Judge Donald's concurring opinion citing numerous decisions holding that Fourth Amendment "privacy expectations are not diminished by the criminality of a defendant's activities,"[223] the majority's overbroad statement that "certainly the police can track the signal"[224] is worri-

---

[220] *Id.* As of this writing, the Supreme Court has recently heard a case in which it must decide whether police use of a drug-sniffing dog at the front door of an individual's home to identify the presence of narcotics is a Fourth Amendment search. Jardines v. States, 73 So. 3d 34 (Fla. 2011), *cert. granted in part*, 132 S. Ct. 995 (2012). At oral argument, Justice Kagan quoted *Kyllo* regarding the use of sense-enhancing technology to seek information regarding the interior of a home, and the Justices seemed skeptical of the government's argument that the dog's sniff was not a search. *See* Jim Harper, *Drug-Sniffing Dogs Are Sense-Enhancing Technology*, CATO@LIBERTY.ORG (Nov. 1, 2012), http://www.cato-at-liberty.org/drug-sniffing-dogs-are-sense-enhancing-technology/ (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001) ("We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally-protected area' constitutes a search—at least where (as here) the technology in question is not in general public use.")). Justice Scalia also compared a sniffing dog to a pair of binoculars: a tool allowing police to uncover otherwise inaccessible information. *Id.* Thus, whether the intrusion is high-tech (like GPS) or low-tech (like a dog's sniff), it appears that the Court is poised to hold that a search occurs anytime police officers use sense-enhancing tools when intruding upon the curtilage of a home to obtain information.

[221] *Skinner*, 690 F.3d at 786 (Donald, J., concurring in part and concurring in the judgment).

[222] *Id.* at 784 (Donald, J., concurring in part and concurring in the judgment); *see also id.* at 776 (noting the lower court's observation that there was no legitimate expectation of privacy "because the cell phone was utilized on public thoroughfares and was 'bought by a drug supplier and provided to Skinner . . . as part and parcel of his drug trafficking enterprise'").

[223] *Id.* at 785 (Donald, J., concurring in part and concurring in the judgment) (citing United States v. Hicks, 59 F. App'x 703, 706 (6th Cir. 2003); United States v. Pitts, 322 F.3d 449, 458 (7th Cir. 2003); United States v. Fields, 113 F.3d 313, 321 (2d Cir. 1997); United States v. Taborda, 635 F.2d 131, 139 n.10 (2d Cir. 1980)).

[224] *Id.* at 784.

some because it inverts the traditional presumption of innocence into a presumption of guilt merely based on police allegations of criminality. Without the need for a warrant grounded in probable cause, the Sixth Circuit's holding that "certainly the police can track [a] signal" emitted by any person's cell phone could easily undergird a police state where all citizens are subject to electronic surveillance. That only serves to further diminish Fourth Amendment protections, particularly when such protections are based on expectations of privacy.[225]

Moreover, by twisting the meaning of "expectations," the *Skinner* opinion helps to demonstrate why relying on expectations of privacy is confusing and confining:

> The law cannot be that a criminal is entitled to rely on the expected untrackability of his tools. Otherwise, dogs could not be used to track a fugitive if the fugitive did not know that the dog hounds had his scent. A getaway car could not be identified and followed based on the license plate number if the driver reasonably thought he had gotten away unseen. The recent nature of cell phone location technology does not change this. If it did, then technology would help criminals but not the police. It follows that Skinner had no expectation of privacy in the context of this case, just as the driver of a getaway car has no expectation of privacy in the particular combination of colors of the car's paint.[226]

This analysis neglects the objective prong of the reasonable-expectation-of-privacy test—whether society would accept as reasonable the fugitive's and getaway driver's purported beliefs that they had "gotten away unseen."[227]

Additionally, the court asserts that suppressing the cell location data would enable technology to "help criminals but not the police," but the holding suggests the opposite: that technological advances exist to benefit police, but not citizens, who must condition their use of advancing technology on their willingness to give up cherished privacy rights. The opinion includes several such statements that (1) visually trailing a defendant and tracking his location

---

[225] *See* United States v. White, 401 U.S. 745, 756 (1971) (Douglas, J., dissenting) ("Electronic surveillance is the greatest leveler of human privacy ever known. How most forms of it can be held 'reasonable' within the meaning of the Fourth Amendment is a mystery."). GPS monitoring is simply a new form of electronic surveillance creating police omniscience, "and police omniscience is one of the most effective tools of tyranny." Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting). An all-knowing government keeping track of where citizens are at all times would certainly "'alter the relationship between citizen and government in a way that is inimical to democratic society.'" United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

[226] *Skinner*, 690 F.3d at 777 (footnote omitted).

[227] *Id.*

presents "no inherent constitutional difference,"[228] (2) "[l]aw enforcement tactics must be allowed to advance with technological changes,"[229] and (3) "[t]hat the officers were able to use less expensive and more efficient means to track the vehicles is only to their credit."[230]

Contrary to this court's analysis, societal privacy expectations and civilians' ability to justifiably rely on their privacy—in other words, the extent of individuals' Fourth Amendment rights—must also "be allowed to advance with technological changes."[231] Law enforcement agents have to demonstrate probable cause to a neutral magistrate and obtain a warrant before being granted the ability to track the location of civilians because such warrantless police tracking would enable significant abuses of power. The Fourth Amendment does not require that technology "help criminals but not the police." It merely requires that the police convince a neutral magistrate that the proposed intrusion is justified.

A person's decision to take advantage of the latest technology—in this case, to merely purchase and use a cell phone—should not present the Hobson's choice of inevitably reduced Fourth Amendment rights. The appellate court's holding fails to recognize how ubiquitous cell phones are. Again, following the *Katz* majority's logic, "[t]o read the Constitution more narrowly is to ignore the vital role" of cellular telephones "in private communication."[232]

The majority holding also fails its own test, noting that "we determine whether a defendant's reasonable expectation of privacy has been violated by looking at what the defendant is disclosing to the public, and not what information is known to the police."[233] But Skinner's cell phone never disclosed his whereabouts *to the public*; rather, police had to seek information known only to Skinner's cell phone company to track his location. While some cases suggest that such a third party disclosure by Skinner to his cell phone company renders this information non-private, no random member of the public could ask the cell phone company for the right to track Skinner's location.[234]

In support of its holding, the Sixth Circuit relies on *United States v. Knotts*[235]

---

[228] *Id.* at 778.

[229] *Id.*

[230] *Id.* at 780 (emphasis added).

[231] *Id.* at 778.

[232] Katz v. United States, 389 U.S. 347, 352 (1967).

[233] *Skinner*, 690 F.3d at 779 (emphasis added). The reliance on disclosure "to the public" tracks Justice Scalia's reasoning in *Kyllo* about the government's use of technology "that is not in general public use." Kyllo v. United States, 533 U.S. 27, 40 (2001).

[234] This is perhaps why Justice Sotomayor suggests that courts may need to reconsider the third-party doctrine in the digital age. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring). On a certain level, an individual's use of a cell phone implicates the freedom to contract between private parties, which should not necessarily grant police the power to obtain information both parties consider to be private and/or confidential.

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

and *United States v. Forest*.[236] But Judge Donald's concurring opinion in *Skinner* ably demonstrates that those cases are distinguishable because, there, the authorities "had already identified and undertaken visual surveillance of a particular suspect."[237] Instead, here, "police had not and could not establish visual contact with Skinner without utilizing electronic surveillance because they had not yet identified the target of their search."[238] Rather, the first time the authorities laid eyes on Skinner was when they knocked on the door of his motor home.[239] Thus, the officers in this case did not "acquire[ ] only information that they could otherwise have seen with the naked eye,"[240] and "they cannot be said to have merely 'augmented the sensory faculties bestowed upon them at birth.'"[241] The officers should not have been allowed to track Skinner without a warrant or having first identified Skinner through a visual search.

There was no trespass in this case, but under the proposed privacy rubric of the justifiable reliance test, the facts of this case would likely have upheld the defendant's Fourth Amendment rights in his location. Skinner could not have objected to the warrantless tracking of his location at the time it occurred (because he was unaware of it until after he was arrested), but Skinner objected to the intrusion as a Fourth Amendment violation prior to trial.[242] Thus, the question becomes whether Skinner's reliance on his Fourth Amendment rights was justifiable under the circumstances. Unlike in *Jones*, Skinner's location was tracked for only three days,[243] yet it is highly likely that an average member of the community would be outraged by (or at least strongly object to) the police using the data emitted by one's cell phone as a tool to monitor their location continuously, even if only for a short time, particularly because the police had never visually identified the target of their search. While Justice Alito did not set a lower bound of what constitutes "long-term tracking,"[244] the fact remains that a majority of the Supreme Court Justices—including Justice Sotomayor and those who joined Justice Alito's concurring opinion—suggested that the public would justifiably disapprove of being tracked, and that "where uncertainty exists . . . the police may always seek a warrant."[245] Hence, under the

---

[236] United States v. Forest, 355 F.3d 942 (6th Cir. 2004).

[237] *Skinner*, 690 F.3d at 786 (Donald, J., concurring in part and concurring in the judgment).

[238] *Id.* (Donald, J., concurring in part and concurring in the judgment) (emphasis added).

[239] *Id.* (Donald, J., concurring in part and concurring in the judgment).

[240] *Id.* (Donald, J., concurring in part and concurring in the judgment).

[241] *Id.* (Donald, J., concurring in part and concurring in the judgment) (quoting United States v. Knotts, 460 U.S. 276, 282, 285 (1983)).

[242] *Id.* at 776.

[243] *Id.* at 780.

[244] United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J, concurring) ("We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.").

[245] *Id.*

justifiable reliance standard, the *Skinner* search required a warrant and probable cause.

If allowed to stand, this decision could skew the balance of power between citizens and government. As Justice Sotomayor warned in *Jones*, the net result of GPS monitoring is that it makes available, at a low cost, substantial amounts of intimate information "about any person whom the government, in its unfettered discretion, chooses to track." Thus, GPS monitoring "may 'alter the relationship between citizen and government in a way that is inimical to democratic society.'"[246] In a worst-case scenario, monitoring locations of individuals could ultimately lead to governmental control of movement. The Supreme Court, Congress and state legislatures need to articulate that the mere purchase and use of cell phones should not subject individuals to warrantless GPS monitoring.

IV. ADVANCING MORE SECURE PRIVACY STANDARDS

Between the *Katz* concurrence and *Jones*, the Supreme Court has relied on two standards for determining Fourth Amendment violations—traditional trespass and reasonable expectations of privacy. The former relates to Fourth Amendment property rights, while the latter relates to Fourth Amendment privacy rights. These tests represent overlapping bulwarks, both of which can be used to determine the extent of Fourth Amendment privacy rights, as the Court set forth in *Jones*.

But even more capable of advancing Fourth Amendment jurisprudence is the *Katz* majority holding—now more pertinent in view of rapidly advancing technology: that individuals are entitled to justifiably rely on their Fourth Amendment property and privacy rights.[247] The more inclusive justifiable reliance test

---

[246] *Id.* at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)); *see also id.* ("[E]ven short-term monitoring . . . reflects a wealth of detail about [one's] familial, political, professional, religious and sexual associations" and noting that such monitoring will disclose to the government trips of an "'indisputably private nature . . . [such as] trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.'") (quoting People v. Weaver, 909 N.E.2d 1195, 1199 (N.Y. 2009)).

[247] Before the technological revolution of the twentieth century, individuals traditionally relied on three factors to maintain their privacy: (1) forgetfulness, (2) resource limitations, and (3) sorting limitations. On the first point, while the government has always been able to monitor activities, mass data storage now allows the government to aggregate and store data indefinitely, so that information acquired is never lost. The *Jones* opinion itself refers to resource limitations, noting that "[t]he surveillance at issue in this case—constant monitoring of the location of a vehicle for four weeks—would have required a large team of agents, multiple vehicles, and perhaps aerial assistance." *Jones*, 132 S. Ct. at 963 (Alito, J., concurring). Now, of course, GPS devices (among other gadgets) obviate such physical monitor-

embraces both the trespass and the reasonable-expectation tests under a single, broad standard: (1) that the person relied on his Fourth Amendment privacy and/or property rights, and (2) that the reliance was justifiable under the circumstances. Neither the trespass test nor the reasonable-expectations-of-privacy test adequately recognizes the majority holding in *Katz* that the Fourth Amendment protects people regardless of their location. By paralleling the two prongs of Justice Harlan's less secure reasonable-expectations test and emphasizing "the circumstances of the particular case," the justifiable reliance standard presents a broader and more secure basis for protecting Fourth Amendment rights.

Moreover, the justifiable reliance test reframes the trespass test while avoiding the need for courts to assess what society as a whole or a hypothetical reasonable person "expects" to remain private. The justifiable reliance test therefore advances privacy protections beyond subjective determinations of "expectations"—riddled with difficulties because attitudes are constantly in flux as technology advances. The Supreme Court's elaboration on "justifiable reliance" from its usage in the Restatement of Torts, as depending on the individual and circumstances of the case, further suggests that reliance is a more appropriate Fourth Amendment standard.

Justice Alito's concurrence in *Jones* emphasizes the strategy of protecting Fourth Amendment rights through the legislative process. Congress and state legislatures need to enact legislation reaffirming that the government cannot use advancing technology as a tool for intruding upon individuals' property or privacy without a search warrant based on particularized, probable cause. While the California state legislature has already realized this goal,[248] more legislators need to take action by requiring search warrants for technological

---

ing, so the government is no longer limited by its ability to allocate agents and resources, such that millions of Americans are now caught in the web of surveillance. *See* Mark Stanley & Jake Laperruque, *Millions of Americans Now Fall Within Government's Digital Dragnet*, ARSTECHNICA.COM (July 24, 2012, 11:45 AM), http://arstechnica.com/tech-policy/2012/07/millions-of-americans-now-fall-within-governments-digital-dragnet/. Finally, technology such as facial recognition and license plate scanners (among others) have enabled the government to sort through its data more rapidly, and potentially track citizens' locations whenever they enter a public space. *FBI Begins Installation of $1 Billion Face Recognition System Across America*, INFOWARS.COM (Sept. 9, 2012), http://www.infowars.com/fbi-begins-installation-of-1-billion-face-recognition-system-across-america/. While the advent of these technologies may diminish *expectations* of privacy, courts should recognize that individuals can still rely on their privacy, and the Fourth Amendment protects such reliance when it is justifiable.

[248] The California state legislature recently passed the Location Privacy Act of 2012, which requires "law enforcement agencies to obtain a warrant before gathering any GPS or other location-tracking data." Megan Guess, *California State Legislature Approves Location Privacy Act*, ARSTECHNICA.COM (Aug. 22, 2012, 11:40 PM), http://arstechnica.com/tech-policy/2012/08/california-state-legislature-approves-location-privacy-act/.

searches to preserve and protect our Fourth Amendment rights.[249]

Whatever the legislative protections, the Supreme Court needs to articulate a clear restatement that electronic intrusions and the use of sense-enhancing tools constitute searches and require warrants supported by probable cause. The Court also needs to set forth a rule that unequivocally reverses the Sixth Circuit's *Skinner* decision, which improvidently held that the mere purchase and use of a cell phone subjects individuals to warrantless GPS monitoring. In the face of ever-changing technology, the Court has the ability to restore Fourth Amendment jurisprudence by reclaiming the wisdom of the *Katz* majority that privacy protections do not depend on "constitutionally protected areas,"[250] but protect people in public, so long as they seek to preserve something as private. The justifiable reliance metric enables courts to consistently apply Fourth Amendment principles in an electronic age invaded by governmental surveillance, from GPS tracking and aerial drones to full-body scans and searches in airports. Fourth Amendment rights should not be protected only by proscribing trespass and unstable "reasonable expectations" of privacy, but also through justifiable reliance on one's privacy against unwarranted governmental intrusion.

In *Katz*, *Kyllo* and *Jones*, the Court began the process of modernizing Fourth Amendment protections. By drawing on the wisdom of the *Katz* majority, that progress can continue forward. Only then can people securely and justifiably rely on the Fourth Amendment in the face of new and yet-to-be-conceived technologies, regardless of where they may be placed.

---

[249] As of this writing, the Senate Judiciary Committee has approved a proposal "that would require law enforcement agencies to obtain a court-approved search warrant before reviewing any e-mail" or other remotely-stored data. *See* Ellen Nakashima, *Senate Panel Backs E-Mail Privacy Bill*, WASH. POST, Nov. 29, 2012, http://www.washingtonpost.com/world/national-security/senate-panel-backs-e-mail-privacy-bill/2012/11/29/e2dafcd4-3a43-11e2-a263-f0ebffed2f15_story.html.

[250] Katz v. United States, 389 U.S. 347, 351 (1967).