ARTICLES

THE MISSED OPPORTUNITY OF *UNITED STATES V. JONES*: COMMERCIAL EROSION OF FOURTH AMENDMENT PROTECTION IN A POST-GOOGLE EARTH WORLD

Mary G. Leary[*]

"It is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented."[1]

INTRODUCTION

Imagine a community in which a police officer with no actual suspicion, but perhaps a curiosity, or even a vendetta, wants to spy on an individual. Possibly this curiosity is a concern that the individual is laundering money, accepting bribes by way of free home additions, using the curtilage of his home as a meeting place for clandestine groups, or using that space for some illegal activity such as storing stolen vehicles or growing illegal substances. Imagine further that the police officer acts on this curiosity by hiring a high-powered satellite with the capability of orbiting over the individual's home every twenty-four hours and transmitting an image detailed enough to clearly see items on the porch or curtilage as small as the size of a baseball field's home plate. Further, imagine that the people of this community are aware of this spying, but have no knowledge of when the police are doing so, and no mechanism through which they can object. They may fence off their property to conceal the activities conducted in their private curtilage. The police, however, have the ability to review images taken over several months and observe items stored, changes to this area, evidence of secret outdoor meetings, or evidence of unlicensed home improvements, as well as the movement

* Associate Professor, The Catholic University of America, Columbus School of Law. Special thanks to Cliff Fishman and Ann McKenna for their insights; Aaron Glaser, Dan McGraw, and Rebecca Ryan for their research; the staff of the *Journal* for their diligence, and Julie Kendrick and Stephanie Michael for surviving numerous drafts.

1 Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 215 (1890).

and identity of objects. The police can even drive up a public street or private road with a high tech 360-degree camera mounted on the roof of their vehicle and simultaneously record GPS measurements and photograph individuals' homes, vehicles parked in driveways, items such as children's toys on the porch, or anything visible from as close as thirty feet away from the door.

While this may appear to describe the police surveillance system of a military dictatorship or a futuristic Orwellian world, it, in fact, describes our world today. Through satellite imaging technology such as Google Earth (and its companion technologies of Google Street View and Google Maps), law enforcement—or any person with access to a computer—can do just this. Many individuals know of the power of this technology and have lost a sense that they have privacy in the curtilage of their home, the area the Supreme Court has described as that which "harbors the intimate activity associated with the sanctity of a man's home and the privacies of life."[2]

Most individuals would regard such police activity as a government "search" requiring a warrant. However, under current case law, this activity does not constitute a search and people have no protection from it or from its effect of eroding their sense of privacy. While it can be argued this loss of privacy is merely a reflection of our time, this privacy loss poses significant challenges for contemporary Fourth Amendment doctrine.

Technologies like the commercially-available satellite imaging technology, Internet tracking of personal information, or geospatial locating of cell phones, have created a world unforeseen by the Supreme Court. This is a world in which most people have lost a subjective expectation of privacy and thus any expectation of privacy that society is objectively willing to accept has eroded. Yet, for the past forty years, American jurisprudence has primarily defined a search under the Fourth Amendment as a government examination of an area in which a person has a "reasonable expectation of privacy."[3]

The utility of this definition is seriously in question because of the Court's failure to adequately consider technology's influence on privacy expectations. Although the Court has made some adjustments to this search definition over the years, it fails to speak to today's problematic reality. Even the Court's most recent opinion in *United*

2 United States v. Dunn, 480 U.S. 294, 300 (1987) (quoting Oliver v. United States, 466 U.S. 170, 180 (1984)) (internal quotation marks omitted).

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

States v. Jones,[4] where the Court expanded its definition of a search, fails to keep current with technology. The specific effects of this failure include diminished Fourth Amendment protections.

Although the Court has anticipated a future where it will need to adjust its search definition, it has not prepared for the present day reality. The Court announced only that when the *government* conditions people to have no expectation of privacy, will the Court modify its search test[5] to accommodate that reality.[6]

However, today's privacy threat is not from *government* conditioning. Commercial activity has created today's dual reality. First, *private commercial entities* have introduced technologies into daily life which fail to afford individuals the opportunity to demonstrate an expectation of privacy. Without the ability to demonstrate a privacy expectation, the first prong of the *Katz* test cannot be met. Second, private commercial entities have conditioned individuals to have no expectation of privacy. If a "search" requires a subjective expectation of privacy that society as a whole accepts, and technology has stripped individuals of any such expectation, then few of the government examinations will constitute a search and trigger Fourth Amendment protections. Thus, the public lacks Fourth Amendment protections. Such diminishments, mischaracterized as "voluntar[y],"[7] are more aptly labeled the products of *commercial conditioning*.

This Article proposes a legislative solution. Part I examines the Court's existing approaches to privacy protections as well as its proposed alternatives when a traditional *Katz* analysis fails. This review includes a thorough analysis of the recently articulated frameworks announced in the majority and concurring opinions of *Jones*. Part II utilizes the example of satellite imaging technology to demonstrate the ubiquity of such publicly-available technologies and the constitu-

---

4 United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that the government's installation of a global positional system tracking device to a vehicle, and its use of that device to monitor the vehicle's movements, constitutes a search under the Fourth Amendment).

5 *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (describing the test for governmental violations of the Fourth Amendment as consisting of "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognize as 'reasonable'").

6 Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979) (asserting that the Court may engage in a normative inquiry to determine whether a legitimate expectation of privacy exists in certain situations, including those where the government conditions subjective expectations of privacy).

7 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring) (describing the disclosure of phone numbers an individual dials to his or her cellular provider and of the URLs an individual visits to his or her Internet service provider as examples of "information voluntarily disclosed to third parties").

tional problem they pose. Part III identifies that, while the Court's post-*Katz* opinions have recognized the limits of the *Katz* test by anticipating *governmental* "conditioning" that artificially interferes with the test, the Court has not anticipated the diminished subjective and objective expectations of privacy resulting from *commercial* "condition[ing] . . . alien to well-recognized Fourth Amendment freedoms."[8] Here, a comprehensive analysis demonstrates the inadequacy of the Court's alternatives, including those suggested in *Jones*. This Article proposes a new legislative framework for respecting privacy protections in response to these commercial-induced privacy affronts. This framework, supported by analogous American law and European proposals, calls for an opt-in model: before an individual can be assumed to have voluntarily sacrificed his privacy, he must affirmatively opt in to allow the use of his private data. The opt-in must, however, be meaningful and not an unfair component of a terms of service agreement.

I. SEARCH JURISPRUDENCE

A. Katz v. United States

The Fourth Amendment affords people the right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[9] Should the government engage in a search or seizure, it must do so pursuant to a warrant or an exception to the warrant requirement.[10] These constraints apply only to *government* searches and seizures.[11] Therefore, courts must first determine whether the government's actions in a given investigation constitute a "search" at all. If not, then no Fourth Amendment protections are triggered. Yet the Court has struggled in defining a "search."

Perhaps as early as Justice Brandeis's 1890 article, *The Right to Privacy*,[12] these questions have been examined through a lens of privacy. From 1967 through January 2012, the law has almost exclusively ap-

8 *Smith*, 442 U.S. at 740 n.5 (internal quotation marks omitted).

9 U.S. CONST. amend. IV.

10 *Id.* ("[N]o Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."); *see also* Kentucky v. King, 131 S. Ct. 1849, 1856 (2011) (illustrating certain reasonable exceptions to the warrant requirement for home searches).

11 Burdeau v. McDowell, 256 U.S. 465, 467 (1921) ("[T]he Fourth Amendment protects only against searches and seizures which are made under governmental authority, real or assumed, or under color of such authority.").

12 Warren & Brandeis, *supra* note 1.

plied the two-pronged *Katz* test[13] to determine the applicability of the Fourth Amendment to government searches.[14] The test (originally from Justice Harlan's concurrence) demands, absent an exception to the warrant requirement, a search warrant if the government examines an area in which an individual has a "reasonable expectation of privacy."[15] The reasonableness of this expectation is determined by establishing that (1) the individual exhibited an actual expectation of privacy in the location searched (subjective prong); and (2) that expectation is one that society is prepared to accept as reasonable (objective prong).[16] Both prongs must be established for the Fourth Amendment to apply.

Many thought, and the Court at the time of *Katz* articulated, that this approach abandoned the previous property-based test for governmental searches: whether there was a physical trespass onto one's property. Prior to January 2012, the Court explicitly acknowledged that *Katz* discarded a trespass-based analysis, asserting, "[t]he premise that property interests control the right of the Government to search and seize has been discredited."[17] Indeed, both litigants in *Katz* had framed their arguments around whether the public phone booth at issue was a "constitutionally protected area."[18] The Court rejected this formulation and reframed the case.[19] In so doing the Court explained that, "the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own

---

13 Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (describing the Court's Fourth Amendment jurisprudence as imposing "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy, and second, that the expectation be one that society is prepared to recognize as 'reasonable'").

14 *See, e.g.*, United States v. Karo, 468 U.S. 705, 712 (1984) (applying the *Katz* test to the Government's installation and monitoring of an electronic tracking device called a "beeper"); Oliver v. United States, 466 U.S. 170, 177 (1984) (applying the *Katz* test and the open fields doctrine to conclude that, although there was a trespass, there was nevertheless no Fourth Amendment violation); *Katz*, 389 U.S. at 353 (rejecting trespass analysis in favor of privacy analysis, and finding the government had violated the Fourth Amendment, despite the fact that there was no trespass). As the Court noted in *Katz*, "[t]he premise that property interests control the right of the Government to search and seize has been discredited." 389 U.S. at 353 (quoting Warden v. Hayden, 387 U.S. 294, 304 (1967)) (internal quotation marks omitted); *see also Oliver*, 466 U.S. at 183 (quoting the same language from *Katz*).

15 *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

16 *Id.* at 361.

17 *Oliver*, 466 U.S. at 183 (quoting *Katz*, 389 U.S. at 353) (internal quotation marks omitted).

18 Brief for Petitioner at 2, *Katz*, 389 U.S. 347 (No. 35); Brief for the Respondent at 2, *Katz*, 389 U.S. 347 (No. 35).

19 *Katz*, 389 U.S. at 350 ("We decline to adopt this formulation of the issues. . . . [T]he correct formulation of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'").

home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[20] In this analysis, the Court rejected that property-based trespass framework and reframed the legal issue as whether Katz knowingly exposed information to the public or attempted to keep said information private.[21]

However, nearly half a century later, the Court is again struggling with privacy and the Fourth Amendment. In *United States v. Jones*,[22] five Justices recharacterized this jurisprudence to assert that both the privacy analysis and the physical trespass analysis are part of the current framework in determining whether government activity is a search.[23]

B. Reservations Concerning Katz

Almost since *Katz* was decided, the Court, in various forms, recognized its limitations.

1. Justice Harlan

Just four short years after articulating the two-pronged test in his *Katz* concurrence, its author, Justice Harlan, expressed concern about the misuse of the Court's approach.[24] In dissent, Justice Harlan questioned the *White* plurality's analytical framework of searching for "subjective expectations or legal attribution of assumption of risk" in the situation in *White*, where the police used electronic means to hear what was being said by the defendant.[25] The plurality found that the defendant's expectation that his conversation would remain private was unprotected by the Fourth Amendment.[26] It grounded the opinion in, inter alia, the belief that the Amendment "affords no protec-

---

20 *Id.* at 351–52 (citations omitted).

21 *See id.* at 352 ("One who occupies [a 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.").

22 132 S. Ct. 945 (2012).

23 *Id.* at 951 (noting that neither *Katz* nor its progeny terminated the previously recognized property based protection).

24 United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) (noting the shortcomings of the "risk analysis" approach or the "expectations approach of *Katz*").

25 *Id.* In *White*, the police monitored the defendant's conversations by having a confidential informant wear a radio transmitter during conversations in the informant's home, a restaurant, the informant's car, and the defendant's home. *Id.* at 746–47. Police who conducted the surveillance testified at trial when the informant was not able to be located. *Id.* at 747.

26 *Id.* at 749.

tion to a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it."[27] Justice Harlan asserted that the plurality's rote application of these concepts "can, ultimately, lead to the substitution of words for analysis."[28] He saw the limitations of this approach in some situations and insisted that the Court do more than merely assess a defendant's assumption of risk to his privacy.[29] Rather, the Court must determine whether the law *should* require Fourth Amendment protections.[30]

> Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present. Since it is the task of the law to form and project, as well as mirror and reflect, we should not, as judges, merely recite the expectations and risks without examining *the desirability of saddling them upon society.*[31]

Justice Harlan cautioned against rigidly applying a test while losing sight of its purpose. He then urged the search analysis to focus on the fundamental question: *is it right* to allow such governmental activity without the protections of a warrant? He also offered an alternative test rooted in the Court engaging in a more fundamental analysis. For him "[t]he critical question, therefore, is whether under our system of government, as reflected in the Constitution, we should impose on our citizens the risks of the electronic listener or observer without at least the protection of a warrant requirement."[32] Harlan proposed answering this question by a balancing test of: (1) "assessing the nature of a particular practice" and (2) "the likely extent of its impact on the individual's sense of security balanced against" (3) "the utility of the conduct as a technique of law enforcement."[33]

2. Justice Blackmun

In *Smith v. Maryland*, Justice Blackmun, writing for the majority, also recognized some limits to *Katz*'s privacy expectation approach. He acknowledged that "[s]ituations can be imagined, of course, in which *Katz*'s two-pronged inquiry would provide an inadequate index

---

27 *Id.* (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966)) (internal quotation marks omitted).

28 *White*, 401 U.S. at 786 (Harlan, J., dissenting).

29 *Id.*

30 *Id.*; *see also id.* at 788 n.24 ("I am now persuaded that such an approach misconceives the basic issue, focusing, as it does, on the interests of a particular individual rather than evaluating the impact of a practice on the sense of security that is the true concern of the Fourth Amendment's protection of privacy.").

31 *Id.* at 786 (emphasis added).

32 *Id.*

33 *Id.*

of Fourth Amendment protection."[34] He provided examples of such situations, which included "if *the Government* were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry," and "if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations."[35] In each scenario, the individual no longer entertained an actual expectation of privacy. To Blackmun those were circumstances

> where an individual's subjective expectations had been "*conditioned" by influences alien to well-recognized Fourth Amendment freedoms*, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[36]

The Court recognized that the government should not be permitted to curtail privacy expectations by *conditioning* individuals to believe they are under intrusive or constant surveillance. Phrased another way, the government cannot destroy an individual's ability to establish a subjective expectation of privacy.

Of course, this criticism was expounded upon in 1974 by Anthony Amsterdam, who challenged the reasonable expectation of privacy test, which he labeled "the common formula for *Katz*."[37] Professor Amsterdam argues that this two-prong test actually "destroys the spirit of *Katz* and most of *Katz*'s substance."[38] Specifically, he argues, "[a]n actual, subjective expectation of privacy obviously has no place in a statement of what *Katz* held or in a theory of what the [F]ourth [A]mendment protects."[39] Similar to Justice Blackmun's examples in *Smith*, Amsterdam asserts that if "an actual, subjective expectation of privacy" could "add to, . . . [or in] its absence, detract from, an individual's claim to [F]ourth [A]mendment protection," then "the government could diminish each person's subjective expectation of privacy merely by announcing half-hourly on television . . . that we were all forthwith being placed under comprehensive electronic surveil-

---

34 Smith v. Maryland, 442 U.S. 735, 740 n.5 (1979). In *Smith*, the Court held that no search occurred when a telephone company, acting at the request of the police, placed a pen register on Smith's phone, thereby confirming that he was the person placing harassing phone calls to the victim.

35 *Id.* (emphasis added).

36 *Id.* (emphasis added).

37 Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 385 (1974).

38 *Id.* at 383.

39 *Id.* at 384.

lance."[40] Amsterdam shares Blackmun's concern, but even more darkly asserts that the action Blackmun warned of had already occurred. He opines that police surveillance in the 1970s already was ubiquitous and resulted in little, if any, basis for a privacy expectation.[41] Neither Blackmun nor Amsterdam, however, envisioned what appears to be happening today—individuals are being "conditioned" by commercial influences alien to well-recognized Fourth Amendment freedoms. Individuals are losing their right to privacy due to commercial forces removing that expectation without affording individuals the opportunity to demonstrate a privacy expectation.

3. Justice Scalia and Kyllo

Justice Scalia has been a longstanding critic of the *Katz* test, noting at one point that "the only thing . . . established about the *Katz* test . . . is that, unsurprisingly, those actual (subjective) expectations of privacy that society is prepared to recognize as reasonable, bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."[42] In 2001 Justice Scalia continued his criticism of the *Katz* approach in *Kyllo v. United States*.[43] Writing for the majority, Justice Scalia concluded that police use of a thermal imaging device aimed at a private home from a public street to detect relative amounts of heat within a home constituted a search within the meaning of the Fourth Amendment.[44] In so doing, Justice Scalia neither relied upon nor embraced *Katz*, but echoed his previous criticism.[45] Asserting that "[i]t 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," Justice Scalia instead focused his analysis on the fact that officers had surveilled Kyllo's home.[46] The Court held 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

---

40 *Id.*

41 *Id.* ("I have had no actual, subjective expectation of privacy in my telephone, my office or my home since I began handling civil rights cases in the early 1960's [sic].").

42 Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring) (alteration omitted) (citations omitted) (internal quotation marks omitted) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

43 533 U.S. 27, 34 (2001) (Scalia, J.) (citing sources that are critical of *Katz*).

44 *Id.*

45 *Id.* (noting criticisms that describe the *Katz* test as "circular, and hence subjective and unpredictable").

46 *Id.* at 33–34.

(as here) the technology in question is not in general public use."[47] When technology facilitated a search, which previously would have required physical trespass, his analysis considers two important factors: (1) whether the target of the search is a home, and (2) whether the technology was in general public use.[48]

Justice Scalia's return to a common law trespass-based analysis is not without its critics. As will be discussed *infra*, many of these arguments are summarized by Justice Alito in *Jones*. Justice Alito laid out five objections to Justice Scalia's approach in *Jones*, including that it had "little if any support in current Fourth Amendment case law."[49] He also referenced misplaced significance, incongruent results, and a lack of uniformity among states.[50] Justice Alito argued that twenty-first century technology issues should not be settled utilizing eighteenth century tort law.[51] Justice Alito's major critique, that such an approach has been rejected by the Court, is not without merit.[52]

C. United States v. Jones

In *Jones*, the Court had the opportunity to address the government's use of technology to conduct surveillance. In *Jones*, the police suspected the defendant of involvement in the narcotics trade.[53] In an effort to gather information, they subjected him to twenty-four hour surveillance by placing a GPS device on his automobile.[54] This surveillance lasted twenty-eight days and required the police to physically trespass the vehicle a second time to replace the battery.[55] The GPS ultimately produced approximately 2000 pages of information.[56]

---

47 *Id.* at 34 (citation omitted) (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

48 *Id.* at 34, 40.

49 United States v. Jones, 132 S. Ct. 945, 958 (2012) (Alito, J., concurring).

50 *Id.* at 961.

51 *Id.* at 962.

52 *See, e.g.*, Katz v. United States, 389 U.S. 347, 353 (1967) (concluding that "the reach of [the Fourth] Amendment cannot turn upon the presence or absence of a physical intrusion," and that "'trespass' doctrine . . . can no longer be regarded as controlling"); Warden v. Hayden, 387 U.S. 294, 304 (1967) ("The premise that property interests control the right of the Government to search and seize has been discredited."); Amsterdam, *supra* note 37, at 357 (describing the Supreme Court's rejection in *Katz* of the "concept of 'constitutionally protected areas'").

53 *Jones*, 132 S. Ct. at 948.

54 *Id.* Although the vehicle was registered to Jones's wife, it was primarily operated by Jones. *Id.* at 949 n.2. In actuality, the government had obtained a search warrant, but failed to adhere to its terms. *Id.* at 948. Thus, it had to defend its actions as if no warrant had been obtained. *Id.* at 948 n.1.

55 *Id.* at 948.

56 *Id.*

The government used some of this information to link the defendant to the location where narcotics were situated.[57]

The Court granted certiorari to determine, among other questions, whether the attachment of a GPS tracking device to a vehicle for approximately four weeks constituted a search within the meaning of the Fourth Amendment.[58] All nine Justices concluded that such activity constituted a search.[59] Unfortunately, the case produced three separate opinions, which arrived at this result in three very different ways. The Court missed an opportunity to reframe the question of privacy so as to reflect twenty-first century realities.

Justice Scalia, writing for the five-Justice majority, held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'"[60] In so doing, Justice Scalia minimized the importance of the *Katz* test, stating that "Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation."[61] Rather, the majority asserted that the fundamental mission of the Court was not to reflect current privacy expectations, but to "'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'"[62] To reflect this eighteenth century standard, the Court returned to a trespass analysis:

> [F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ("persons, houses, papers, and effects") it enumerates. *Katz did not repudiate that understanding*. . . . "We do not believe that *Katz*, by holding that the Fourth Amendment protects persons and their private conversations, was intended to withdraw any of the protection which the Amendment extends to the home. . . ."[63]

---

57 *Id.* at 948–49.

58 *Id.* at 948. Originally the Court was poised to answer two questions. The question presented by the parties was "[w]hether the warrantless use of a tracking device on respondent's vehicle to monitor its movements on public streets violated the Fourth Amendment." Petition for a Writ of Certiorari at i, *Jones*, 132 S. Ct. 945 (2011) (No. 10-1259). However, the Court added the second question—whether attaching a GPS tracking device to a vehicle for approximately four weeks constituted a Fourth Amendment search—and ultimately only resolved that question, leaving the propriety of the monitoring without physical trespass and a warrant unresolved. *Jones*, 131 S. Ct. at 948.

59 *Jones*, 132 S. Ct. at 949; *id.* at 954 (Sotomayor, J., concurring); *id.* at 964 (Alito, J., concurring).

60 *Id.* at 949 (majority opinion) (footnote omitted).

61 *Id.* at 950.

62 *Id.* (alteration in original) (internal quotation marks omitted) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)).

63 *Jones*, 132 S. Ct. at 950–51 (alterations omitted) (emphasis added) (footnote omitted) (quoting U.S. CONST. amend. IV; Alderman v. United States, 394 U.S. 165, 180 (1969)).

The *Jones* majority explicitly states that trespass is not the exclusive test, or alone sufficient to evaluate Fourth Amendment liability.[64] However, the *Jones* Court also concludes that *Katz* did not erode the physical trespass analysis or the principle that "when the government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment."[65] Thus, although the Court in *Jones* did not overturn *Katz*, Justice Scalia in essence reduced it to a supplement to the primary concern of physical trespass.

Justice Alito, with whom Justices Ginsburg, Breyer, and Kagan joined, concurred in judgment but rejected the reversion to a trespass analysis. Justice Alito concurred that the GPS surveillance in this case was a search by applying the traditional *Katz* test.[66] That is to say he "would analyze . . . this case by asking whether respondent's reasonable expectations of privacy were violated by the long-term moni-

---

64 *Jones*, 132 S. Ct. at 950–51, 951 n.5 ("Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.").

65 *Id.* at 951 (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)) (internal quotation marks omitted). The majority's support for this claim that *Katz* did not replace the trespass analysis but supplemented it is somewhat dubious. The main support for this proposition is the concurring opinions and the responses therein to the cases Justice Alito cites in his concurrence as evidence that the trespass doctrine has been overturned. *Compare Jones*, 132 S. Ct. at 947, 951 (citing Soldal v. Cook County, 506 U.S. 56, 60, 62, 64 (1992); Alderman v. United States, 394 U.S. 165, 180 (1969)) (listing precedential Supreme Court cases as support for the proposition that the *Katz* reasonable expectation of privacy test supplemented the common law trespass test, instead of replacing it); *with Jones*, 132 S. Ct. at 960 (Alito, J., concurring) ("The majority suggests that two post-*Katz* decisions show that a technical trespass is sufficient to establish the existence of a search, but they provide little support." (citations omitted) (citing *Soldal*, 506 U.S. at 56; *Alderman*, 394 U.S. at 165)). For examples of cases cited by Justice Alito in his dissent in support of his claim that *Katz* eliminated the trespass doctrine, see *Jones*, 132 S. Ct. at 959 (Alito, J., concurring) ("This trespass based rule was repeatedly criticized. . . [*Katz*] finally did away with the old approach, holding that a *trespass was not required for a Fourth Amendment violation*." (emphasis added) (citing Katz v. United States, 389 U.S. 347 (1967))); *id.* at 960 ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate. The premise that property interests control the right of the Government to search and seize has been discredited." (quoting Oliver v. United States, 466 U.S. 170, 183 (1984)) (internal quotation marks omitted)); *id.* (quoting Rakas v. Illinois, 439 U.S. 128, 143 (1978) (citing a description that characterized *Katz* as holding that the "capacity to claim the protection of the Fourth Amendment depends not upon a property right in the invaded place but upon whether the person who claims the protection of the Amendment has a legitimate expectation of privacy in the invaded place")); *id.* (quoting Kyllo v. United States, 533 U.S. 27, 32 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property . . . .")); *id.* (quoting United States v. Karo, 468 U.S. 705, 713 (1984) ("[A]n actual trespass is neither necessary nor sufficient to establish a constitutional violation.")).

66 *Jones*, 132 S. Ct. at 964 (Alito, J., concurring) (finding that the GPS surveillance was a search under a test that "appl[ies] existing Fourth Amendment doctrine").

toring of the movements of the vehicle he drove."[67] He concluded under a pure *Katz* analysis "that the lengthy monitoring that occurred in this case constituted a search under Fourth Amendment."[68] Notwithstanding that conclusion, Justice Alito left open the possibility that shorter term monitoring might "accord[] with expectations of privacy that our society has recognized as reasonable."[69] In so doing, Justice Alito vigorously protested the majority's resurrection of the trespass approach, which he regarded as discredited.[70] "In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass-based theory."[71] Nevertheless, Justice Alito acknowledged that a *Katz* analysis is at times inadequate in an era of increasing technological surveillance, and appealed for a legislative response.[72]

Justice Sotomayor joined Justice Scalia's opinion that "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common law trespassory test,"[73] but she also wrote separately, agreeing in substance with much of Justice Alito's opinion.[74]

---

67 *Id.* at 958.

68 *Id.* at 964.

69 *Id.*

70 *See id.* at 959–61 (describing the historical discrediting of the trespass approach); *see also Katz*, 389 U.S. at 353 (discrediting trespass analysis).

71 *Jones*, 132 S. Ct. at 961 (Alito, J., concurring). Justice Alito also cited four additional flaws with the majority opinion; he pointed out that the majority's approach: (1) disregards the significance of long-term GPS tracking but misplaces significance by emphasizing instead the trivial act of placing the device on a car; (2) produces incongruous results in which a GPS attachment, no matter how brief, automatically triggers a search, but comprehensive twenty-four-hour monitoring through aerial and visual surveillance does not; (3) produces different results from state to state based on the property laws of the states; and (4) presents "particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked." *Id.* at 961–62.

72 *Id.* at 964 (citation omitted) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." (citing Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004) (advocating for legislatures, rather than the judiciary, to be the mechanism for creating "the primary investigative rules when technology is changing"))); *see also* Eric Lichtblau, *Police are Using Phone Tracking as Routine Tool*, N.Y. TIMES, Apr. 1, 2012, at 1, 20 (discussing law enforcement's use of cell phone technology in surveillance and tracing for both emergencies and routine investigations).

73 *Jones*, 132 S. Ct. at 952 (emphasis omitted); *see id.* at 955 (Sotomayor, J., concurring) ("As the majority's opinion makes clear, however, *Katz*'s reasonable-expectation-of-privacy test augmented, but did not displace or diminish, the common-law trespassory test that preceded it.").

74 *Id.* (Sotomayor, J., concurring) ("Under that rubric [wherein technological advances make nontrespassory surveillance possible and shape societal privacy expectations], I agree with Justice Alito that, at the very least, 'longer term GPS monitoring in investiga-

Like Justice Scalia, she asserted that Fourth Amendment protections include, at a minimum, protection from physical trespass, as well as the *Katz* protection of privacy when the trespass analysis is not applicable.[75] However, she did not seem assured that the sole answer to these contemporary challenges lay in eighteenth century truisms. Justice Sotomayor, more so than either Justice Scalia or Justice Alito, was particularly concerned about the increased ability of law enforcement to use modern techniques to search without physical intrusion through technological advancement.[76] She went further than Justice Alito, stating that "cases involving even short-term monitoring . . . require particular attention."[77] She explicitly expressed a desire that the jurisprudence reflect an understanding of the technological realities of contemporary surveillance. She noted concern about the high volume of information which could be obtained from twenty-four hour monitoring of one's vehicle through a GPS device,[78] the danger of entrusting the government to use a tool "so amenable to misuse,"[79] and the questionable validity of the Third Party Doctrine[80] in an age when technology requires people to "reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[81]

II. SURVEILLANCE, OBTAINING INFORMATION, AND SATELLITE IMAGING TECHNOLOGY

The Supreme Court majority's recent articulation in *Jones* that the Fourth Amendment can be implicated when the government trespasses and engages in an "attempt to find something or to obtain in-

tions of most offenses impinges on expectations of privacy.'" (citing *Jones*, 132 S. Ct. at 964 (Alito, J., concurring))).

75 *Id.* at 954–55.

76 *Id.* at 955. ("[P]hysical intrusion is now unnecessary to many forms of surveillance. . . . GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations.").

77 *Id.*

78 *Id.*

79 *Id.* at 956.

80 The Third Party Doctrine asserts that the Fourth Amendment allows "the obtaining of information revealed to a third party and conveyed by [the third party] to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." United States v. Miller, 425 U.S. 435, 443 (1976).

81 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

formation"[82] possibly has significant implications. This description of the Fourth Amendment may implicate technologies that allow the same access to information that a physical trespass would permit. By way of example, police use of satellite imaging technology to examine an individual's private property is "an attempt to obtain information" without a physical trespass.

Today, law enforcement, and any individual with Internet access for that matter, has the ability to use a high-powered satellite to examine the property of another in some detail, no matter where in the world the property is located. No warrant is required because this likely will not constitute a search under the Court's current definition. The individual subject of such surveillance has no choice in this, regardless of what he does to deny public access to his property. While such examinations are not real time video footage of property, they do allow observation of relatively recent images of one's property and comparison of these images over time. Thus, the viewer could observe the presence or absence of structures, machinery, crops, meeting places, vehicles, activities, etc. Furthermore, examination of real time imaging is certainly technologically possible and may soon also reach commercial viability.[83] While a detailed analysis of how this technology works is beyond the scope of this Article, a brief understanding of the technology is helpful in analyzing its impact on privacy.

The ability to engage in this surveillance is possible through a combination of satellite imaging technology and software processing. Satellite imaging technology is a component of currently-existing technology that allows one to access images of a specific location in the world and zoom in to obtain a view from the equivalent of approximately five meters away. A common example of this is Google Earth, one of the many commercially-available services that provides

---

82 *Id.* at 951 n.5 (majority opinion) ("Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.").

83 This could occur through satellite images or, more likely, drones. *See* JAY STANLEY & CATHERINE CRUMP, AM. CIVIL LIBERTIES UNION, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 2–10 (2011), *available at* http://www.aclu.org/technology-and-liberty/report-protecting-privacy-aerial-surveillance-recommendations-government-use (examining the use of drones at all levels of law enforcement and FAA efforts to develop policy to facilitate such use); Brian Bennett, *Police employ Predator drone spy planes on home front*, L.A. TIMES, Dec. 10, 2011, http://articles.latimes.com/print/2011/dec/10/nation/la-na-drone-arrest-20111211 (discussing the use of U.S. Customs and Border Protection drones by local police).

access to satellite images and enhances them for more detail.[84] Combined with Google Street View,[85] this technology allows law enforcement—or anyone else—to access pictures of one's property through a powerful satellite and observe how said area changes over time. Google Earth images are sourced from not only satellite imagery, but also from aerial photography and data from many imagery providers.[86] Google describes its service as allowing one to "[v]iew satellite imagery, maps, terrain, 3D buildings, galaxies far in space, and the deepest depths of the ocean."[87] While other companies provide this service, Google Earth is paramount among them due to the large amount of media coverage it receives.[88]

The road to this technology becoming commonly available at no cost to the customer began in 2004, when Google acquired the software company Keyhole Corporation.[89] At the time of this acquisition, the parties described Keyhole as allowing one to "fly like a superhero from your computer at home to a street corner somewhere else in the world."[90] At that time, Google described the acquisition as giving Google users

> a powerful new search tool, enabling users to view 3D images of any place on earth as well as tap a rich database of roads, businesses and many other points of interest. . . . With an Internet connection, users enter an address or other location information and Keyhole's software accesses the database and takes them to a digital image of that location on their com-

84 GOOGLE EARTH, http://www.google.com/earth/index.html (last visited Sept. 9, 2012); *see also* BING MAPS, http://www.bing.com/maps/ (last visited Sept. 20, 2012); YAHOO! MAPS, http://maps.yahoo.com (last visited Sept. 9, 2012).

85 *Street View*, GOOGLE MAPS, http://www.google.com/streetview (last visited Oct. 21, 2012) ("Google Maps with Street View lets you explore places around the world through 360-degree street-level imagery.").

86 *See Support FAQs: "What data does TerraMetrics provide to Google Earth and Google Maps?"*, TERRAMETRICS, http://truearth.com/support/faqs_content_google.htm (last visited Sept. 19, 2012) (detailing the composited data of which Google Earth and Google Maps are comprised, and attributing the satellite imagery provided to by TerraMetrics).

87 *Google Earth for Desktop*, GOOGLE EARTH, http://www.google.com/earth/explore/products/desktop.html (last visited Sept. 9, 2012).

88 *See, e.g.*, Dan Fletcher, *Top 10 Google Earth Finds*, TIME, http://www.time.com/time/specials/packages/article/0,28804,1881770_1881787_1881774,00.html (last visited Sept. 9, 2012) (devoting an online slideshow to ten "of the most unusual discoveries" found by Google Earth users); Andrew C. Revkin, *Google Earth Dives Deep, Filling In Its Maps' Watery Gaps*, N.Y. TIMES, Feb. 3, 2009, at D3 (detailing the functionality and newly developed features of Google Earth); Iain Thomson, *Upgrade eliminates Atlantis from Google Earth*, REGISTER (Feb. 6, 2012), http://www.theregister.co.uk/2012/02/06/google_earth_atlantis/ (reporting an update to the Google Earth software that eliminated an image which some had believed to be evidence of the lost city of Atlantis).

89 *Google Acquires Keyhole Corp*, NEWS FROM GOOGLE (Oct. 27, 2004), http://googlepress.blogspot.com/2004/10/google-acquires-keyhole-corp.html.

90 *Id.*

> puter screen. The interactive software then gives users many options, including the ability to zoom in from space-level to street-level, tilt and rotate the view or search for other information . . . .[91]

Google later contracted with high resolution satellite companies, such as DigitalGlobe and GeoEye, which launch satellites and provide the imagery to Google.[92] These companies describe these images as "high-quality images."[93] Some of the satellites owned by such companies have the capacity to record images at fifty centimeter resolution.[94] One such company explains that this level of detail allows customers to "map natural and man-made features to within five meters (about sixteen feet) of their actual location on the surface of the Earth."[95] Another describes this level of detail as allowing a viewer to discriminate between grass and trees, and to examine a road and determine whether it is in need of resurfacing.[96] However, Google also supplements these images with other images obtained by aircraft, some of whose resolutions are as high as thirty to sixty centimeters.[97]

Today, Google Earth has continued to grow in its abilities to develop images from anywhere in the world. Google uses satellites owned by third-party operators, most of which are private, but at least

---

91 *Id.*

92 *See GeoEye & Google*, GEOEYE, http://www.geoeye.com/GeoEye101/GeoEye-Google/Default.aspx (last visited Sept. 9, 2012) (promoting Google's use of GeoEye-1 satellite imagery on its Google Earth and Google Maps platforms); *see also History: The Growth of the Business*, DIGITALGLOBE, http://www.digitalglobe.com/about-us/history#/the-growth-of-the-business (last visited Sept. 9, 2012) (noting the digital satellite imagery agreement between DigitalGlobe and Google, which dates back to 2002); *Support FAQs: "What data does TerraMetrics provide to Google Earth and Google Maps?"*, http://truearth.com/support/faqs_content_google.htm (last visited Sept. 19, 2012) (attributing the "baselayer imagery" provided to Google Earth and Google Maps to TerraMetrics TruEarth technology).

93 *SPOT: Looking Down On Earth*, CNES, http://www.cnes.fr/web/CNES-en/1415-spot.php (last updated Aug. 2009) (chronicling the history of the "Satellite Pour l'Observation de la Terre" (SPOT satellites)).

94 *See High-Resolution Imagery, Resolution Modes*, GEOEYE, http://www.geoeye.com/GeoEye101/satellite-imagery/high-resolution-imagery.aspx (last visited Sept. 21, 2012) (observing that though the GeoEye-1 satellite can record images at forty-one centimeter resolution, which allows one to view "home plate on a baseball field," the National Oceanic and Atmosphere Administration requires satellite imaging companies to convert these images to fifty centimeter resolution for commercial use).

95 *Collecting Images with GeoEye-1*, GEOEYE, http://www.geoeye.com/GeoEye101/satellite-imagery/collection-method.aspx (last visited Sept. 9, 2012).

96 DIGITALGLOBE, THE BENEFITS OF THE EIGHT SPECTRAL BANDS OF WORLDVIEW-2, at 3–7 (Mar. 2010), *available at* http://www.digitalglobe.com/downloads/white-papers/DG-8SPECTRAL-WP.pdf ("The high spatial resolution enables the discrimination of fine details, like vehicles, shallow reefs and even individual trees in an orchard . . . .").

97 *Precision Aerial*, DIGITALGLOBE, http://www.digitalglobe.com/downloads/AerialProgram-DS-AP-Web.pdf (last visited Sept. 21, 2012).

some of which are related to some government agencies.[98] Each of these third parties has numerous satellites, which vary in ability to record data. Generally, these satellites travel a certain orbit that allows them to orbit the Earth as many as fifteen times a day, with a more typical frequency of from once every 1.1 days to once every 5.9 days.[99] While in orbit, they can observe land for a lengthy period of time. They do not provide live pictures with a live feed to the Internet. Rather, the images are collected, uploaded, stored, transmitted, and processed before being placed on the Internet.[100] Although not live, the ability to quickly produce photographs has been demonstrated by recent satellite images from the capsizing of the Costa Concordia, as well as satellite images relating to national security concerns, such as images of the Chinese aircraft carrier Varyag.[101]

---

98 *See History: The Early Years*, DIGITALGLOBE, http://www.digitalglobe.com/about-us/history (last visited Sept. 9, 2012) ("In 1993, the United States Department of Commerce granted DigitalGlobe . . . the first license allowing a private enterprise to build and operate a satellite system to gather high-resolution digital imagery of the Earth for commercial sale."); *About CNES*, CNES, http://www.cnes.fr/web/CNES-en/3773-about-cnes.php, (last visited Sept. 9, 2012) ("[T]he Centre National d'Etudes Spatiales (CNES) is the government agency responsible for shaping and implementing France's space policy in Europe."); *About Us*, GEOEYE, http://www.geoeye.com/CorpSite/about-us/Default.aspx (last visited Sept. 9, 2012) ("The Company's growing global sales network currently comprises 12 strategic business partners (government and commercial) . . . ."); *About Us: Company Info*, TERRAMETRICS, http://www.truearth.com/about_info/company_content.htm (last visited Sept. 9, 2012) ("TerraMetrics provides . . . technologies to a broad customer base including U.S. Department of Defense agencies, the National Aeronautics and Space Administration (NASA), . . . [and] international governments . . . .").

99 *See Collecting Images with GeoEye-1*, GEOEYE, http://www.geoeye.com/GeoEye101/satellite-imagery/collection-method.aspx (last visited Sept. 9, 2012) (listing the features and specifications of the GeoEye-1 satellite); *Design and Specifications*: *Quickbird*, DIGITALGLOBE, http://www.digitalglobe.com/downloads/QuickBird-DS-QB-Web.pdf (last visited Sept. 21, 2012) (listing the features and specifications of the Quickbird satellite); *Design and Specifications*: *WorldView-1*, DIGITALGLOBE, http://www.digitalglobe.com/downloads/WorldView1-DS-WV1-Web.pdf (last visited Sept. 21, 2012) (listing the features and specifications of the WorldView-1 satellite); *Design and Specifications*: *WorldView-2*, DIGITALGLOBE, http://www.digitalglobe.com/downloads/WorldView2-DS-WV2-Web.pdf (last visited Sept. 21, 2012) (listing the features and specifications of the WorldView-2 satellite); *SPOT satellite technical data*, CNES, http://spot5.cnes.fr/gb/programme/111.htm (last visited Sept. 9, 2012) (listing the features and specifications of the SPOT-5 satellite).

100 *See A highly effective operational system*, CNES, http://spot5.cnes.fr/gb/systeme/systeme.htm (last visited Sept. 21, 2012) (specifying that two operators that conduct a series of separate processes are required to produce final images from the SPOT satellites, including a satellite operator that manages the performance of the satellite and a commercial operator that processes, generates, and distributes the resulting images); *Technical features and operation*, CNES, http://www.cnes.fr/web/CNES-en/1420-technical-features-and-operation.php (last visited Sept. 21, 2012) (explicating the technical processes by which SPOT satellites record and transmit images to stations on the ground).

101 *Satellite Spots Costa Concordia Shipwreck from Space*, SPACE.COM (Jan. 18, 2012), http://www.space.com/14273-satellite-photo-costa-concordia-cruise-shipwreck.html (re-

DigitalGlobe, one of the third-party satellite operators, has promised that its next generation of satellites will possess enough speed to re-examine the same geographical location within twenty-four hours.[102] Another company, Centre National d'Etudes Spaciales ("CNES"), asserts that its satellites can work in tandem to cover a 120 kilometer swath of land in a single pass, and in some cases can acquire imagery of any point in the globe in less than three days.[103] Another asserts that its satellites have average revisit times of 1.1 day for the entire globe.[104]

While these satellites are owned primarily by third parties, some possess a nexus with government activity. For example, the Spot 5 Program is run by CNES, the French government agency responsible for shaping France's space policy.[105] Indeed, CNES argues that its "Earth observation satellites are vital asset [sic] for science, industry and the military alike. Carrying ever-enhanced viewing instruments, they can acquire repeat coverage of vast areas systematically and yield very detailed images."[106] Similarly, Google has an exclusive contract for online use of imagery supplied by GeoEye,[107] a company that was also awarded a 3.8 billion dollar contract with the National Geospa-

---

porting on a photograph taken on January 17, 2012 by DigitalGlobe satellites of the capsized Costa Concordia, a cruise ship that wrecked off the coast of Italy on January 13, 2012); Stephen Wood, *Capturing the Varyag*, DIGITALGLOBE BLOG (Dec. 19, 2011), http://www.digitalglobeblog.com/2011/12/19/capturing-the-varyag-stephen-wood-vp-analysis-center/ (discussing the documentation in DigitalGlobe satellite images of the second sea trial of the Chinese aircraft carrier known as the Varyag).

102 *See WorldView-3*, DIGITALGLOBE, http://www.digitalglobe.com/downloads/WorldView3-DS-WV3-Web.pdf (last visited Sept. 21, 2012) (attesting that "WorldView-3 has an average revisit time of [less than one] day").

103 *Instrument Features*, CNES, http://spot5.cnes.fr/gb/satellite/42.htm (last visited Sept. 9, 2012) (explaining that, although HRG "instruments generally operate independently to observe separate targets," they can "view in tandem to cover a 120-kilometre swath in a single pass" and "can acquire imagery of any point on the globe within less than five days, or even in less than three days at temperate latitudes").

104 *See* DIGITALGLOBE, THE BENEFITS OF THE EIGHT SPECTRAL BANDS OF WORLDVIEW-2, at 3 (Mar. 21, 2012), *available at* http://www.digitalglobe.com/downloads/white-papers/DG-8SPECTRAL-WP.pdf (advertising that, among other features, DigitalGlobe's "second next generation" satellite, WorldView-2, will "offer average revisit times of 1.1 days around the globe").

105 *See About CNES*, CNES, http://www.cnes.fr/web/CNES-en/3773-about-cnes.php (last visited Sept. 9, 2012) ("Founded in 1961, the Centre National d'Etudes Spatiales (CNES) is the government agency responsible for shaping and implementing France's space policy in Europe. Its task is to invent the space systems of the future, bring space technologies to maturity and guarantee France's independent access to space.").

106 *Observing Earth*, CNES, http://spot5.cnes.fr/gb/applications/21.htm (last visited Sept. 9, 2012).

107 Stephen Shankland, *Google to buy GeoEye Satellite Imagery*, CNET NEWS (Aug. 29, 2008, 7:27 AM), http://news.cnet.com/8301-1023_3-10028842-93.html.

tial-Intelligence Agency,[108] which is GeoEye's largest customer, accounting for 65% percent of its revenue in 2009.[109]

Google has expanded this effort through Google Street View, which was launched in the United States in 2007 and is now available throughout the world.[110] This service provides "360-degree panoramic views" of streets on all seven continents.[111] Google obtains these images through a fleet of vehicles with nine cameras and Wi-Fi antennas mounted upon them that capture and store wireless data.[112] For locations inaccessible to vehicles, Google creates smaller vehicles described as "Google Trikes."[113] According to Google, "the latest car has [fifteen] lenses taking 360 degrees of photos. It also has motion sensors to track its position, a hard drive to store data, a small computer running the system, and lasers to capture 3D data to determine distances . . . ."[114] The cameras are stationed nearly nine feet high and "allow[] Google to peer over fences to photograph [images not visible] to an ordinary person walking down the street."[115] Additionally, the Street View user can zoom in on images well beyond what the ordinary observer can see.[116]

With this technology in the hands of government officials, the implications for police surveillance are significant. A common sense approach would suggest that police use of these satellites to examine an individual's property from five meters above the ground is a search. However, under a traditional analysis, it may not be a search. First, people cannot demonstrate subjective expectations of privacy because companies like Google never afford them the opportunity to demonstrate such expectations by opting out of the imaging. Second, many individuals are aware of the technology's use, and society,

---

108 *GeoEye Wins National Geospatial-Intelligence Agency Enhanced View Award*, SPACE DAILY (Aug. 10 2010) http://www.spacedaily.com/reports/GeoEye_Wins_National_Geospatial_Intelligence_Agency_Enhanced_View_Award_999.html.

109 A. Ananthalakshmi, *UPDATE 1–GeoEye Q2 profit beats Street view*, REUTERS (Aug. 10, 2009), http://www.reuters.com/article/2009/08/10/geoeye-idUSBNG50871620090810.

110 *See In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011) (noting that Google Street View has expanded to more than thirty countries worldwide).

111 *Id.* at 1070–71; *Street View: Cars, Trikes, and More*, GOOGLE MAPS, http://maps.google.com/help/maps/streetview/learn/cars-trikes-and-more.html (last visited Sept. 20, 2012).

112 *Google*, 794 F. Supp. at 1071.

113 *Id.*

114 *Street View: Cars, Trikes, and More*, *supra* note 111.

115 Roger C. Geissler, Note, *Private Eyes Watching You: Google Street View and the Right to an Inviolate Personality*, 63 HASTINGS L.J. 897, 902 (2012).

116 *Id.* at 902–03.

therefore, lacks an objective acceptance of any expectation of privacy. Thus, individuals are powerless to stop this privacy encroachment.

III. THE PROBLEM IS NOT TRESPASS OR GOVERNMENT USE OF TECHNOLOGY: THE PROBLEM IS UBIQUITOUS ELECTRONIC SURVEILLANCE BY COMMERCIAL ENTITIES AND ITS EFFECT ON INDIVIDUALS

As recognized to some degree by Justices Alito and Sotomayor in their *Jones* concurring opinions, technological advances have altered the landscape significantly since 1967. This role of technology is not a new revelation. As early as 1890, Warren and Brandeis recognized that technological advances demand the law move toward privacy protection.[117] In 2010 the Court acknowledged the role of technology in determining conceptions of privacy, stating that "[r]apid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior."[118] The Court further cautioned against ruling on such questions until a new technology's role in society becomes clear.[119] Technological development of the telephone pushed Fourth Amendment jurisprudence forward in *Katz* to recognize that the old way of measuring a search, the physical trespass, was no longer solely sufficient to protect what was deemed as private under the Fourth Amendment.[120] So too we now find ourselves in need of a twenty-first century solution.

Although there is significant disagreement between Justices Scalia and Alito as to whether *Katz* discarded the trespass approach to searches, it appears that post-*Jones*, courts must first engage in a trespass analysis, and if that fails, they can then apply a *Katz* analysis. Justice Scalia explicitly asserts that "we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would remain subject to *Katz* analysis."[121]

---

117 Warren & Brandeis, *supra* note 1, at 195. ("Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing . . . the right 'to be let alone.'").

118 City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010) (declining to rule on whether one has a reasonable expectation of privacy in text messages).

119 *Id.* ("The judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear.").

120 Katz v. United States, 389 U.S. 347, 352–53 (1967) (suggesting that a refusal to protect telephone communications would "ignore the vital role that the public telephone has come to play in private communication," and going on to reject strict trespass analysis as the sole measure for whether the Fourth Amendment has been violated).

121 United States v. Jones, 132 S. Ct. 945, 953 (2012) (emphasis omitted).

However, his lack of further discussion of this category suggests that he views such situations as uncommon. As the two concurring opinions underscore, however, transmission of electronic signals without trespass comprises the vast majority of surveillance methods today. Therefore, whichever test is applied is flawed. If no physical trespass occurs, then the trespass approach provides no protection. If no opportunity to demonstrate a privacy expectation exists, then *Katz* also fails to protect.

A. Neither the Jones *nor* Katz *Approaches Respond Adequately to This Reality*

The satellite imaging technology exemplifies the shortfall of the Court's current approach in defining a search. Without physical trespass, law enforcement—or anyone else—can attempt to gain information regarding an individual and his personal activities that occur out of public view. It is the fact that anyone can do so that provides the largest challenge to current Fourth Amendment privacy protections. Because individuals are aware of the power of this technology and its widespread use, many believe they actually have no privacy. This perception can exist both because of the existence of such technology, as well as because of its misuse. For example, Google has apologized for, and admitted to, utilizing a wireless sniffer on its Google Street View vehicles,[122] obtaining data packets of information including user name and passwords, and storing said information.[123] The FCC fined Google for obstructing its investigation of Street View[124] and German officials characterized the data collection

122 A wireless sniffer is a data collection system that samples, collects, decodes, and analyzes types of data broadcast through Wi-Fi connections. *In re* Google Inc. Street View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1071 (N.D. Cal. 2011) (defining a data sniffer and noting that Google "issued an apology" and "admitted to intercepting" data through Street View vehicles); Kevin J. O'Brien & David Streitfeld, *Swiss Court Orders Modifications to Google Street View*, N.Y TIMES (June 8, 2012) www.nytimes.com/2012/06/09/technology/09iht-google09.html ("Google has maintained that the collection of private information was accidental . . . . [and] was not intended for or used in any Google product.").

123 *Google*, 794 F. Supp. 2d at 1071 ("The wireless sniffer secretly captures data packets . . . [which] must be stored on digital media and then decoded using . . . complicated technology."); *see also* Geissler, *supra* note 115, at 906 (noting that, in May and October of 2010, Google admitted that its camera-fitted cars had collected data from private, non-password protected WiFi networks, and that "entire emails and URLS were captured, as well as passwords") (quotation marks omitted) (quoting *Creating stronger privacy controls inside Google*, GOOGLE OFFICIAL BLOG (Oct. 22, 2010), http://googleblog.blogspot.com/2010/10/creating-stronger-privacy-controls.html).

124 O'Brien & Streitfeld, *supra* note 122 ("[T]he F.C.C. fined Google $25,000, saying it had obstructed an investigation into Street View."); David Streitfeld & Kevin J. O'Brien, *Google*

as "one of the biggest violations of data protection laws that [they] had ever seen."[125] While regulators have sought the data collected, no U.S. regulator has seen it despite efforts by over thirty states' Attorneys General.[126] In this kind of reality, individuals lose the expectation of privacy under our current jurisprudence.

At first glance, it may appear that these technologies cause no new Fourth Amendment ramifications because of precedent allowing substantial law enforcement surveillance. The combined caselaw that permits law enforcement to examine curtilage from navigable airspace;[127] to monitor one's movements on public thoroughfares;[128] and to accept information disclosed to third parties (Third Party Doctrine)[129] initially suggests that government use of satellite imaging technology may be without constitutional significance. However, this argument misses the issue. The issue is not the propriety of law enforcement's use of satellite imaging technologies (which itself does raise questions). Rather, the issue is a more fundamental question regarding the *effect of these technologies* on the *subjective expectation* of privacy. Namely, what happens when the reasonable expectation of privacy is compromised or diminished not by government "conditioning," but rather by the inescapable reality of the commercial use of

---

Privacy Inquiries Get Little Cooperation, N.Y. TIMES (May 22, 2012), www.nytimes.com/2012/05/23/technology/google-privacy-inquiries-get-little-cooperation.html ("[The F.C.C.] tagged Google with a $25,000 fine for obstructing the [Street View data collection] investigation.").

125 O'Brien & Streitfeld, *supra* note 122 (quoting Johannes Caspar, a German data protection official).

126 *Id.*

127 Florida v. Riley, 488 U.S. 445, 450 (1989) (suggesting that law enforcement is "free to inspect the yard from the vantage point of an aircraft flying in the navigable airspace"); *see also* California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye . . . .").

128 *See* United States v. Karo, 468 U.S. 705, 721 (1984) (explaining that, although monitoring of a beeper—a type of electronic surveillance device—is impermissible while the beeper is within the confines of a private residence, gathering information from beeper surveillance while the beeper is on public streets is constitutionally permissible under the Fourth Amendment); United States v. Knotts, 460 U.S. 276, 281 (1983) ("A person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another.").

129 Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (finding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"); United States v. Miller, 425 U.S. 435, 443 (1976) (acknowledging that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

surveillance technology and the commercial or social conditioning that accompanies it?

One ramification of this conditioning is the evisceration of privacy. It could mean that no individual possesses a subjective expectation of privacy in the curtilage of his or her home. In effect, all yards, patios, porches, decks, rear driveways, fenced in structures, or plantings—i.e., anything not covered by a roof or thick canopy of trees, even if completely removed from public view—have become "open fields," and therefore searchable. Similarly, the data collected from individuals online, at times unbeknownst to them, is available for capture and review.[130] Indeed, in a recent Court of Appeals case regarding Google Street View, Google reportedly argued that, in light of satellite imaging technology, "[c]omplete privacy does not exist."[131] Similarly, the CEO of Google rather famously quipped in response to privacy concerns, "If you have something you don't want anyone to know, maybe you shouldn't be doing it in the first place."[132] These assertions suggest that this lack of privacy holds true even when an individual has no opportunity to demonstrate a subjective expectation of privacy by opting out of Google Earth or retaining his or her private information.

Furthermore, even if an individual possessed a subjective expectation of privacy, such a claim would likely fail the second prong of *Katz* as it is difficult to imagine society would be able to accept such an expectation as objectively reasonable in light of the broad use of this technology. What is needed today is a reframing of the issue to reflect contemporary reality.

---

130 *See Updating our privacy policies and terms of service*, GOOGLE OFFICIAL BLOG (Jan. 24, 2012), *available at* http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html, (describing the cross-sharing of individual information between different Google products).

131 Defendant Google Inc.'s Memorandum of Law in Support of its Motion to Dismiss Amended Complaint at 2, Boring v. Google Inc., 598 F. Supp. 2d 695 (W.D. Pa. 2009) (No. 08-cv-694) (quoting RESTATEMENT (SECOND) OF TORTS § 652D cmt. C (1977)); *see also* Steven Musil, Google wins Street View privacy suit, CNET NEWS (Feb. 18, 2009), *available at* news.cnet.com/8301-1023_3-10166532-93.html.

132 *Inside the Mind of Google* (CNBC television broadcast Dec. 9, 2009), *available at* http://video.cnbc.com/gallery/?video=1409844721&play=1.

IV. ALTERNATIVE APPROACHES OFFERED BY THE JUSTICES FALL SHORT IN ADDRESSING TODAY'S DECREASING EXPECTATION OF PRIVACY

A. Justice Harlan's Balancing Test

Justice Harlan's balancing approach in *White* has significant drawbacks in light of commercially-available surveillance. When the subjective expectation of privacy is lost, Justice Harlan would likely abandon the *Katz* two-prong test and address the issue by asking a different question: whether it is desirable to allow law enforcement to utilize these publicly-available technologies. As a threshold matter, this important value judgment is almost irrelevant because of the practical considerations. Even if one were to decide that individuals should not be "saddled" with the ability of law enforcement to utilize said technologies, how would this be enforced? It is hard to imagine a workable rule that forbids law enforcement from using Google Earth but allows others to do so. While such a solution may be workable when addressing a more narrow technology such as wiretapping or GPS placement on vehicles, many other readily available technologies such as satellite imaging technology are different. This technology is ubiquitous and available through the Internet to anyone free of charge. Limiting it to non-law enforcement use would be artificial.

More narrowly, the specific prongs of his proposed balancing test are also inadequate. The first requires an assessment of the "nature of the practice." Given the ubiquitous nature of this technology, there is nothing out of the ordinary when the police use it. Although highly intrusive, the *nature* of the government's use of satellite imaging technology is indistinguishable from private persons' utilization of the free Internet program.

The second prong of Justice Harlan's balancing test would also fail. It requires an examination of the extent of the impact of law enforcement's use of technologies on society's sense of security. The extent of the impact of satellite imaging technology would be impossible to measure when the complaint is itself that the technology is readily available to anyone at any time. As such, law enforcement's use of it is unlikely to more severely impact one's sense of security than the technology itself.

The third prong—the utility of the police action—also provides little assistance. As with many forms of surveillance, the ability to observe the private property of an individual without alerting said individual has great utility to the law enforcement. Because the first two prongs are unworkable, they cannot be balanced against a prong that

will always be in favor of the government. Therefore, Justice Harlan's test fails to adequately respond to this twenty-first century problem.

B. Justice Blackmun's Normative Inquiry

Justice Blackmun's normative approach in *Smith* may be a solution for the problem he envisioned: a deterioration of privacy expectations caused by *government* "conditioning." However, when the expectation is lost by all of society being conditioned by *commercial entities*, this normative inquiry solution seems unworkable. By definition, if all of society has lost a subjective expectation of privacy, then a normative approach will be circular, as the normative expectation will likely duplicate the subjective. This circularity is troubling when that societal choice "is 'conditioned' by influences alien to well-recognized Fourth Amendment freedoms" from private commercial entities and social forces. Furthermore, because many of these technologies offer no ability for an individual to demonstrate an expectation of privacy by opting out of this monitoring, a measurement of what the social norm is or should be is likely impossible.

This normative approach is similar to Amsterdam's proposed condemnation of an expectations analysis.[133] Yet, both suffer the same fate because they fail to acknowledge the relevance of whether a suspect, claiming privacy in court, sought privacy initially. While many have criticized the subjective prong of the *Katz* test, it serves a purpose. There *is* a role for understanding whether the defendant thought his actions or items were private.[134] If the Fourth Amendment protects privacy rights, then the role of the judge is to determine if the government violated a defendant's privacy rights. Although it is not determinative, a judge is guided in that decision by determining what the defendant actually considered private. If he did not consider his actions or the searched location private, it is hard to imagine how his privacy was violated.[135] Accordingly, the subjective expectation, when given a meaningful opportunity to be

---

133 *See* Amsterdam, *supra* note 37.

134 *Cf.* Thomas K. Clancy, United States v. Jones*: Fourth Amendment Applicability in the 21st Century*, 10 OHIO ST. J. CRIM. L. (forthcoming Fall 2012) (arguing that to receive Fourth Amendment protection, one must take steps to exclude the government from accessing private areas, objects, and data), *available at* http://papers.ssrn.com/abstract=2097811.

135 *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508–09 (2007) (suggesting a blend of four models for Fourth Amendment protections, including the probabilistic model where "a person has a reasonable expectation of privacy when the odds are very high that others will not successfully pry into his affairs" and "[a]s those odds drop, the individual's expectation of privacy becomes less and less reasonable").

demonstrated, can serve an important goal of enhancing privacy. Furthermore, a purely objective approach that "resist[s] captivation in any formula"[136] is intellectually seductive, but in the realm of technology, impractical. In contemporary society, digital divides based on income, age, and geography lead to different understandings of privacy when it intersects with technology. Therefore, determining a normative understanding of privacy is impossible.

C. Justice Scalia's Opinion in Kyllo

Justice Scalia's approach in *Jones*, which echoes his opinion in *Kyllo*,[137] was strongly criticized as applying an eighteenth century solution to a twenty-first century problem.[138] Prior to *Kyllo*, when faced with an issue involving enhanced technology being used by law enforcement, the Court almost always narrowed the protections of the Fourth Amendment.[139] Justice Scalia, writing for the majority in *Kyllo*, found the police use of thermal imaging constituted a search.[140] Conspicuously absent from the majority opinion was any endorsement of *Katz*. Rather, Justice Scalia described the *Katz* opinion as "circular."[141] Justice Scalia based his *Kyllo* analysis of new technology on two factors: (1) whether the technology ascertained information from a constitutionally protected area that would normally require a physical intrusion, and (2) whether the technology was publicly available. "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

---

136 Amsterdam, *supra* note 37, at 385.

137 Kyllo v. United States, 533 U.S. 27 (2001).

138 United States v. Jones, 132 S. Ct. 945, 957–58 (Alito, J., concurring) ("Ironically, the Court has chosen to decide this case based on [eighteenth] century tort law. 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 to chattels. And for this reason, the Court concludes, the installation and use of the GPS device constituted a search." (footnotes omitted)).

139 Smith v. Maryland, 422 U.S. 735, 742 (1979) (finding that the use of a pen register by a telephone company does not constitute a "search"); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that observation of a fenced-in backyard within curtilage of home from an airplane was not an unreasonable search under the Fourth Amendment); Dow Chem. Co. v. United States, 476 U.S. 227, 238–39 (1986) (holding that aerial mapping photography of an industrial complex by a government agent was not an unreasonable search).

140 *Kyllo*, 533 U.S. at 34–35 (holding that the use of a thermal imaging device from a public street to detect heat from within a private home constitutes a search).

141 *Id.* at 34 ("The *Katz* test . . . has often been criticized as circular . . . .").

protected area' constitutes a search—at least where (as here) the technology in question is not in general public use."[142]

However, this approach suffers two fundamental flaws. First, many modern threats to privacy do not involve physical trespass. Whether it is satellite imaging technology, triangulating cell phone signals,[143] government-operated video cameras,[144] or surveillance drones,[145] the police today are able to intrude more and more deeply into individual's lives with less actual physical encroachment.

Furthermore, notwithstanding the resurrection of the notion of a constitutionally protected area, such areas are difficult if not impossible to identify in today's technology-driven world. Although all would agree that the home is an area that its occupants consider highly private,[146] technology allows searching of many more areas, from which a treasure trove of information can be obtained. For example, consider GPS surveillance, which

> generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it

---

142 *Id.* (quoting Silverman v. United States, 365 U.S. 505, 512 (1961)).

143 Triangulation of cell phone signals "is the process of determining the coordinates of a point based on the known location of two other points. If the direction (but not distance) from each known point to the unknown point can be determined, then a triangle can be drawn connecting all three points." *In re* Application of U.S. for an Order for Prospective Cell Site Location Info. on a Certain Cellular Tel., 460 F. Supp. 2d 448, 451 n.3 (S.D.N.Y. 2006). "Knowledge of the locations of multiple towers receiving signals from a particular telephone at a given moment permits the determination, by simple mathematics, of the location of the telephone with a fair degree of precision" through triangulation. *Id.* at 451.

144 *See, e.g.,* Margaret Harding, *Pittsburgh police laud Downtown surveillance cameras*, TRIBLIVE NEWS (Oct. 11, 2012, 12:01 AM), http://triblive.com/news/2753247-74/police-cameras-surveillance-video-avenue-downtown-whetsell-camera-charged-detectives#axzz2A3B3I4Sb (describing a "network of private and public security cameras" used by the Pittsburgh police in the course of investigations); Karen Hopkins, *Police Want to Quadruple Surveillance Cameras at Oceanfront*, WVEC.COM (Oct. 16, 2012, 6:21 PM), http://www.wvec.com/mycity/vabeach/Police-want-to-upgrade-expand-surveillance-cams-at-Oceanfront-174387091.html (reporting on the Virginia Beach Police Department's attempts to "install higher tech, digital cameras in trouble spots").

145 *See generally*, STANLEY & CRUMP, *supra* note 83, at 8–9 (discussing the strong desire by law enforcement to employ drone aircrafts, and pressure on the Federal Aviation Administration to develop policies to allow such use); Brian Bennett, *Police employ Predator drone spy planes on home front*, L.A. TIMES, Dec. 10, 2011, http://articles.latimes.com/print/2011/dec/10/nation/la-na-drone-arrest-20111211 (discussing the use of U.S. Customs and Border Protection drones by local police).

146 *But see* California v. Carney, 471 U.S. 386, 391 (1985) (finding that a mobile home, even when used as a home, is a vehicle and therefore has a reduced expectation of privacy).

> evades the ordinary checks that constrain abusive law enforcement practices . . . .[147]

Similarly, satellite imaging technology observes curtilage, but the Court has previously held that as long as such images are taken from legal airspace with no interference in the possessory interest of the property, then no violation occurs.[148]

Second, access to such technology is now readily available to the general public. Satellite imaging technology is accessible through free programs such as Google Earth and available to anyone with an Internet connection.[149] GPS devices are available for public purchase. So much of the technology utilized by law enforcement is indeed publicly available. Thus, limiting its use on such a basis to civilians creates a legal fiction that attempts to cabin commonly used technologies as unavailable for government use, while considering the very same action unproblematic when done by a neighbor.[150]

D. Justice Scalia's Opinion in Jones

The majority opinion in *Jones* is also not responsive to these new technological realities. An initial read of the opinion's assertion that "the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test,"[151] may incorrectly lead one to conclude that *Jones* offers increased privacy protection. Perhaps this is so, in the narrow context of GPS tracking. As a practical matter, however, it adds no protection in the vast majority of surveillance techniques. While the Court made passing reference to the government's "attempt to find something or to obtain infor-

---

147 United States v. Jones, 132 S. Ct. 945, 955–56 (2012) (Sotomayor, J., concurring) (citations omitted) (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th. Cir. 2010) (Kozinski, C.J., dissenting)).

148 *See, e.g.*, Florida v. Riley, 488 U.S. 445, 450 (1989) (noting that where one's property is viewable from public airspace, no reasonable expectation to privacy exists); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("The Fourth Amendment simply does not require the police traveling in the public airways . . . to obtain a warrant in order to observe what is visible to the naked eye.").

149 273.1 million people in North America are reported as users of the Internet. *Internet Usage Statistics for the Americas*, INTERNET WORLD STATS, http://www.Internetworldstats.com/stats2.htm (last visited Sept. 28, 2012).

150 *See* Alan Levin, *Commercial Drones: A Dogfight at the FAA*, BUS. WK. (Feb. 9, 2012), www.businessweek.com/magazine/commercial-drones-a-dogfight-at-the-faa-02092012.html (noting that Federal Aviation Administration rules permit the use of unmanned drone aircraft by hobbyists, and that such drones will soon be "widely available for sale in the U.S.").

151 *See Jones*, 132 S. Ct. at 952 (emphasis omitted).

mation,"[152] the Court made clear that such activity becomes a search only when it is "conjoined" with a trespass.[153] As mentioned, with satellite imaging technology, online data collection, and other technologies, there is no physical trespass, unlike GPS technology. Thus, as Justices Alito and Sotomayor point out, the majority's opinion in *Jones* does nothing to enhance privacy protections in general.[154] However, none of the opinions adequately address the effect on the subjective expectation of privacy.

E. Justice Sotomayor's Concerns

Of the opinions articulated in *Jones*, Justice Sotomayor's is the most aware of the implications of ubiquitous technology on society's expectations. She joined Justice Scalia's majority opinion. However, she wrote separately, stating she joined the majority because she viewed Justice Alito's approach as perhaps more privacy-limiting. Not without reason, she then wrote separately, stating:

> Justice Alito's approach, which discounts altogether the constitutional relevance of the Government's physical intrusion on Jones' Jeep, erodes that longstanding protection for privacy expectations inherent in items of property that people possess or control. By contrast, the 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.[155]

Justice Sotomayor's concurrence does, however, find common ground with some of Justice Alito's approach. She agrees with Justice Alito's "incisive[]" observation that "the same technological advances that have made possible nontrespassory surveillance techniques will also affect the *Katz* test by shaping the evolution of societal privacy expectations."[156] Her main concern, however, is the government's unrestrained ability to collect data.[157] She recognizes that the *Katz*

---

152 *Id.* at 951 n.5 ("Likewise with a search. Trespass alone does not qualify, but there must be conjoined with that what was present here: an attempt to find something or to obtain information.").

153 *Id.*

154 *See id.* at 957 (Sotomayor, J., concurring) (questioning the validity of the Third Party Doctrine in today's technology driven world, as "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks"); *id.* at 963 (Alito, J., concurring) (commenting on devices that permit the monitoring of people's movements, including closed circuit television, GPS services installed in vehicles and cell phones, and personal locator technology).

155 *Id.* at 955 (Sotomayor, J., concurring) (citation omitted).

156 *Id.*

157 *Id.* at 955–56 ("In cases involving even short-term monitoring, some unique attributes of GPS surveillance relevant to the *Katz* analysis will require particular attention. GPS moni-

approach may be "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties."[158] More so than Justice Alito, she has a strong appreciation for the effect of this technology on perceptions of privacy. She then somewhat narrowly characterizes this effect as implicating the individual's relationship with his government.

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. 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."[159]

Justice Sotomayor is alone in discussing these deeper issues. Her response is almost a hybrid of those offered by both Justice Harlan in *White* and Justice Blackmun in *Smith*. She first seems to suggest that it is proper to consider societal norms. She then suggests that it is important to follow Justice Harlan's lead and examine the desirability of saddling society with such an intrusion by the police without a warrant.[160] She next states she "would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[161]

It is here that her solution falters. In expanding her discussion to other technologies, she targets the Third Party Doctrine.[162] In so doing she characterizes the problem as a *voluntary* disclosure to a third party, as opposed to an involuntary gathering of data by business. She frames the digital reality of today as one in which information is

---

toring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. . . . The Government can store such records and efficiently mine them for information years into the future." (citing United States v. Pineda-Moreno, 617 F.3d 1120, 1124 (9th Cir. 2010) (Kozinski, C.J., dissenting))).

158 *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

159 *Id.* at 956 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

160 *Jones*, 132 S. Ct. at 956 ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

161 *Jones*, 132 S. Ct. at 956.

162 *Id.* at 957 (arguing that it should not invalidate Fourth Amendment privacy protections when information is "voluntarily disclosed" to third parties).

"voluntarily disclosed" by the public for a limited purpose and concludes that such information should not be "disentitled to Fourth Amendment protection."[163] In doing so, she seems to join Justice Alito in framing the issue as a "'tradeoff' of privacy for convenience."[164]

In the satellite imaging technology context, as well as with many other technologies, people do not *themselves* voluntarily disclose any such information to the public. They never make the choice to participate in such technology. They never have the opportunity to make such a "tradeoff" of losing privacy in exchange for other social gains. To the contrary, even their consent is never obtained. In fact, at times, companies such as Google have actively circumvented the "third party cookie blocking" privacy feature of web browsers to obtain information without users' knowledge.[165] Therefore, Justice Sotomayor's solution of abandoning the Third Party Doctrine offers only a partial accounting for this problem. While it may address scenarios where the information is exchanged voluntarily, it does nothing when the information is obtained unbeknownst to the individual.

D. Justice Alito's Retention of a Compromised Katz

Justice Alito asserts plainly that *Katz* avoids the problems of the Scalia approach.[166] For the reasons previously discussed in Part I.B, this two-pronged approach is flawed in the context of some of these technologies. Therefore, this assertion that a properly applied *Katz* analysis avoids problems is not without weakness. Even Justice Alito is

---

163 *Id.*

164 *Id.* (quoting *Jones*, 132 S. Ct. at 962 (Alito, J., concurring)).

165 Jonathan Mayer, *SafariTrackers*, WEB POLICY (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/ (analyzing the Internet browser Safari's "cookie blocking" feature, and efforts by companies like Google and Vibrant to circumvent Internet browser privacy settings); *see also* Defendant Google Inc.'s Memorandum of Law in Support of its Motion to Dismiss Amended Complaint at 1, Boring v. Google, Inc., 598 F. Supp. 2d 695 (W.D. Pa. 2009) (defending Google's practice of taking pictures of private homes for its Internet "Street View" feature); *Google's Circumvention of Browser Privacy Settings*, EPIC, http://epic.org/privacy/google/tracking/googles_circumvention_of_brows.html (last visited Sept. 28, 2012) (reporting on Google's efforts to circumvent Internet privacy safeguards in order to target advertising more specifically); Steven Musil, *Google wins Street View Privacy Suit*, CNET NEWS (Feb. 18, 2009), http://news.cnet.com/8301-1023_3-10166532-93.html (reporting Google's successful legal defense of its "Street View" process of taking pictures of private homes against a reasonable expectation of privacy challenge).

166 *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) ("The *Katz* expectation-of-privacy test avoids the problems and complications noted above . . . .").

forced to acknowledge some weakness in the *Katz* approach.[167] He recognizes that

> [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 in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile.[168]

Again, here Justice Alito assumes there is a "tradeoff." How that can be assumed is questionable in the context of satellite imaging technology or other data collection mechanisms that do not allow for user notice or consent. In many instances, a tradeoff can be assumed if there is an opportunity to demonstrate an expectation of privacy and but the individual chooses not to take that opportunity. For example, the decision to participate in social networking, even on a limited basis with a small network of contacts, brings with it some collection of data by companies such as Facebook.[169] However, it may not bring with it an agreement to be tracked by third parties. With the Library of Congress archiving all public tweets,[170] the decision to engage in Twitter involves trading off some privacy. But increasingly, individuals are having private data taken from them and assuming there is nothing they can do. For these reasons, Justice Alito correctly demands a legislative solution.[171]

V. NEW PROPOSAL: OWNERSHIP OF DIGITAL FOOTPRINTS AND OPT-IN PROVISION TO SHARE SUCH DATA

While these alternative approaches may be viable in certain circumstances, they are inadequate for this contemporary problem of a loss of a *Katz* subjective expectation of privacy due to commercial conditioning. On one end of the spectrum of solutions is to do nothing. Justice Alito's reluctant application of *Katz* would result in no

---

167 *Id.* (acknowledging that the *Katz* test "is not without its own difficulties").

168 *Id.*

169 *See* Juan Carlos Perez, *Facebook Admits Ad Service Tracks Logged-Off Users*, PCWORLD (Dec. 3, 2007, 12:00 PM), http://www.pcworld.com/article/140225/article.html (reporting that Facebook admitted to allowing an ad service to track its users activities even while logged-off from the site).

170 *News Releases: Twitter Donates Entire Tweet Archive to Library of Congress*, LIBRARY OF CONGRESS (Apr. 15, 2010), http://www.loc.gov/today/pr/2010/10-081.html (announcing Twitter's agreement to donate its digital archive of public tweets to the Library of Congress).

171 *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring) ("In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.").

expectation of privacy, even in data exposed to the public without express consent of the individual. In the satellite imaging context, this would mean the curtilage of the home.[172] This rather draconian result provides clarity and may support an originalist view of the Amendment as protective of the interior of the home. However, this severe limitation on Fourth Amendment protections, caused by commercial activity, fails to satisfy. There is something fundamental about Brandeis's "right to be left alone." That right is honored when society decides that an individual loses said right when he demonstrates a willingness to sacrifice it. Ruling that one loses this central right when a commercial entity takes it with impunity affronts this core value.

The other extreme would be a new constitutional test for a government search. Just as the technology of the telephone drove the opinion in *Katz*, so too could the technological development of satellite imaging or other similar technologies drive a new approach. However, tying a new test for reasonableness to technological advances is always problematic, as the effectiveness of the new approach is likely outdated before the ink outlining said test is dry. While this may have been more manageable in 1967, today's technology is changing so rapidly that the ability of the law to respond with the needed alacrity is questionable. Indeed, the Court noted as much in 2010, cautioning that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[173]

A. Functionality

The most viable and less extreme solution is a statutory one. Justice Alito comes the closest to recognizing this as a required solution. He concedes that some privacy losses are not the product of value tradeoff, but rather of a situation in which "the public does not welcome the diminution of privacy that new technology entails, [though] they may eventually reconcile themselves to this development as inevitable."[174] Justice Alito urges Congress to act, as it is "well situated to gauge changing public attitudes, to draw detailed lines,

---

172 Although Justice Scalia obtained five votes for his approach in *Jones*, this arguably does not affect the proposed scenario by supplanting Justice Alito's model. As Justice Scalia concedes, with data intrusions there is often no physical trespass, so *Katz* would apply. *Jones*, 132 S. Ct. at 953 ("Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.").

173 City of Ontario v. Quon, 130 S. Ct. 2619, 2629 (2010).

174 *Jones*, 132 S. Ct. at 962 (Alito, J., concurring) (footnote omitted).

and to balance privacy and public safety in a comprehensive way."[175] Although such a statutory approach is plagued by the same problem as a new Fourth Amendment test—the rapid pace of changing technology—it should not target the technology. Any such approach should be a *functional* one and not a *technological* one.

Functionally, the actual problem is commercial conditioning. It is here where the Court has failed to correctly identify the issue and thus the solution. Justice Sotomayor describes an individual's data that has been exposed to and assembled by the government as "voluntarily disclosed to some member of the public for a limited purpose . . . ."[176] Justice Alito frames the issues as a "tradeoff" which also suggests a voluntary choice.[177] However, in the satellite imaging technology model and others, the disclosure of information is not voluntary, as the individual has been afforded no opportunity to refuse. This is where Congress must focus.

The problem is really who *owns* a person's "digital dossier" or "digital identity." Professor Solove coined the term "digital dossier," noting that it includes information about individuals compiled by "companies [they] have never established any contact with," through which others "can glean information relating to [a person's] financial transactions, debts, creditors, and checking accounts[,] . . . . race, income, opinions, political beliefs, health, lifestyle, and purchasing habits[,] . . . . supermarket purchases, ... inventory of one's groceries, over-the-counter medications, hygiene supplies, and contraceptive devices," among other things.[178] Palfrey and Glasser describe it as all the personally identifiable digital information associated with one's name, and they further discuss one's digital identity as a subset of information "composed of all those data elements that are disclosed online to third parties, whether it is by [one's] choice or not."[179] Our current system of Fourth Amendment protection seems to accept that the "digital dossier" or "digital identity" of an individual is considered abandoned when possessed by a third party. Current law does not take into account how a third party collects that data or

175 *Id.* at 964.

176 *Id.* at 957 (Sotomayor, J., concurring).

177 *Id.* at 962 (Alito, J., concurring).

178 Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1092 (2002); *see also id.* at 1095 (describing digital dossiers as "digital biographies, a horde of aggregated bits of information combined to reveal a portrait of who we are based upon what we buy, the organizations we belong to, how we navigate the Internet, and which shows and videos we watch").

179 JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 40 (2008).

that often the individual had no *meaningful* opportunity to consent to either the initial collection of that data or the subsequent sharing of it.[180] A legislative solution must focus on *this* problem.

Such legislation should focus on commercial services that collect information from digital dossiers and expose it to the public or other third parties. In the satellite imaging context, this would mean companies that visually expose concealed private property. In the search engine world it includes companies that record information about users and share it with advertisers.[181] Such businesses should not be allowed to condition individuals that this information exposure will just happen, so any expectation of privacy is lost. Rather, the law should require a meaningful "opt-in" provision prior to making the information publicly available. Congress must enact legislation that precludes publication of private data, including images of private property, when the individual does not opt in to such disclosure.

B. Precedence

While this may at first appear unprecedented, there is a rich history of such a response. Justice Alito most recently called for a legislative response to these inexpensive and intrusive technological abilities.[182]

Historic precedent supports this approach. After *Smith*, Congress enacted laws that effectively required procedural review prior to mon-

---

180 For example, Austrian law student Max Schrems has spearheaded a movement to disclose the amount of information Facebook collects from its users. *See* Kashmir Hill, *Max Schrems: The Austrian Thorn in Facebook's Side*, FORBES (Feb. 7, 2012, 10:03 AM), http://www.forbes.com/sites/kashmirhill/2012/02/07/the-austrian-thorn-in-facebooks-side/. Using a provision in European privacy law referred to as the "right to access," Schrems requested that Facebook disclose the dossier collected on him. *Id.* He received over 1200 pages of information that he was unaware Facebook had been collecting, including: e-mail addresses he never provided, deleted messages, records of who else signed on to Facebook from his computer, etc. *Id.*

181 Cecilia Kang, *Google announces privacy changes across products; users can't opt out*, WASH. POST (Jan. 24, 2012), http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html (describing Google's plan to integrate data collected across its sites, including its search engine, YouTube, and Gmail, ostensibly to allow Google to "better tailor its ads to people's tastes"); Hiawatha Bray, *Google policy brings privacy worry*, THE BOSTON GLOBE (Feb. 24, 2012), http://www.bostonglobe.com/business/2012/02/24/critics-google-changes-threaten-privacy/xIpso7CMd143KjvlC7FyqN/story.html?camp=pm (reporting on the changes to Google's privacy policies that will allow information gathered about users of any one of its products, including its Android operating system on smartphones, to be shared across other Google platforms in order to "deliver more accurate search results and advertising that is more relevant to individual customers").

182 *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

itoring dialed phone numbers.[183] Congress, through Title III of the Electronic Communication Privacy Act, drafted provisions governing the use of pen registers, including imposition of a requirement that government officials first certify before an authorized magistrate that "the information likely to be obtained is relevant to an ongoing criminal investigation."[184] The Children's Online Privacy Protection Act ("COPPA") forbids the collection of personal information from a child by website operators unless they obtain verifiable parental consent.[185] In other words, parents must opt in to that disclosure. More recently, the federal implementation of a "Do Not Call List" provides firmer ground for such a solution.[186] Such legislation and rules forbid direct automatic dialing systems contacting any cellular phone or phone that would be charged.[187] Similarly it forbids telemarketing phone calls without prior consent of party.[188] Such legislation and regulations balance consumer protection with commercial interests. Although an opt-out approach, this legislation supplies precedence for the proposed governmental regulation.

There is compelling support, not just historical precedent, for such an approach both abroad and more recently domestically. The strongest support for this legislative solution comes from overseas. While here in the United States, the Court has seemingly thrown up its hands at the reality of the collection of personal data and its implications for privacy, Europeans have taken a different position.[189] Eu-

183 Electronic Communications Privacy Act of 1986, 18 U.S.C. § 3122 (2006) (describing procedures for applications to the courts by government lawyers for the installation and use of pen registers or trap and trace devices).

184 18 U.S.C. §§ 3122(a)(2), 3122(b)(2) (2006).

185 15 U.S.C. § 6502 (2006).

186 15 U.S.C. § 6151 (2006).

187 47 C.F.R. § 64.1200(a)(iii) (2011).

188 47 C.F.R. § 64.1200(a)(2) (2011).

189 An example of European resistance to privacy intrusion is reflected in its response to Google Street View technology. Some European countries disallowed the collection of data pending an investigation; in other nations, the individuals physically blocked roads to keep the vehicles from gathering information. *See* Geissler, *supra* note 115, at 899. Still others fined Google. *Id.* at 917. Google has been fined by the FCC, sanctioned in France and Switzerland, banned from collecting images in Greece, and suspended in Austria and the Czech Republic. *Court rules in favour of Google Street View*, SWISSINFO.CH (June 8, 2012, 1:41 PM), http://www.swissinfo.ch/eng/swiss_news/Court_rules_in_favour_of_Google_Street_View.html?cid=32861794 (reporting on the ruling of a Swiss Federal Court requiring Google to implement blurring of faces and car license plates with an accessible process for requests to be filed without red tape, and commenting that in Austria and the Czech Republic, Google Maps Street View has been suspended since 2010); Geissler, *supra* note 115, at 899, 917 (noting that Greece and the Czech Republic forbade Google from taking additional images while those countries investigated possible privacy violations, and that France fined Google 100,000 euros for improperly collecting personal da-

ropeans have combated the invasion of privacy not by precluding its disclosure, but by increasing individual control over the data.[190]

The Charter for Fundamental Rights of the European Union affords privacy protection a hallowed place, fundamental to the freedoms inherent in being human. Article Eight provides that "[e]veryone has the right to the protection of personal data concerning him or her."[191] This includes the right to have the data processed "fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law."[192] It further includes the right of access to any data collected.[193] Since 1995, the main European Union legislation in this area has been the Data Protection Directive, Directive 95/46/EC, which regulates the processing of personal data.[194] Personal data includes "any information relating to an individual, whether it relates to his or her private, professional or public life."[195] However, the European Commission recognized the limits of this directive due to the reality that "[t]echnological progress and globalisation have profoundly changed the way our data is collected" as well as that each European Union member state implemented it with different rules and regulations.[196]

---

ta); Hayley Tsukayama, *Google fined by FCC for impeding Street View probe*, WASH. POST (Apr. 16, 2012), http://www.washingtonpost.com/business/technology/google-fined-by-fcc-for-impeding-street-view-probe/2012/04/16/gIQAePySLT_story.html (describing the FCC's decision to fine Google $25,000 for obstructing the Commission's investigation by not responding to requests for material information or provide certifications or verifircations of its responses). Most of the forty countries in which the application is available have expressed concern over Street View. *Court rules in favour of Google Street View, supra.*

190 *Court rules in favour of Google Street View*, *supra* note 189 (explaining recent decision by Swiss Federal Administrative Court requiring Google Street View to attend to all requests by individuals to have their images blurred and anonymity protected).

191 Charter of Fundamental Rights of the European Union, art. 8(1), 2000 O.J. (C 364) 10. This concept of digital protection has been said to be linked to privacy as a "personality right, . . . predicated on dignity." Karen Eltis, *Breaking Through the "Tower of Babel": A "Right to be Forgotten" and How Trans-Systemic Thinking Can Help Re-Conceptualize Privacy Harm in the Age of Analytics*, 22 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 69, 93 (2011). Such an idea also harkens back to Brandeis and Warren's description of privacy as a principle of "inviolate personality." Warren & Brandeis, *supra* note 1, at 211.

192 Charter of Fundamental Rights of the European Union, *supra* note 191, at art. 8(2).

193 *Id.*

194 Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 31, *available at* http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf.

195 Press Release, European Commission, Data Protection Reform: Frequently asked questions at 1 (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/41&format=PDF&aged=1&language=EN&guiLanguage=en.

196 Press Release, European Comission, Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for business-

Consequently, on January 25, 2012 the European Commission introduced several proposed reforms to its 1995 Data Protection Directive.[197] The reforms relevant to this Article focus not on government use of data, but further upstream on both data collection and the use of data once collected. The touchstone for this approach is *not* a nebulous concept of privacy; rather, its framework is more akin to assessing the right of the individual to own his own data, and the corresponding lack of a right of commercial entities to take data without consequences. It is an extension of the "right of personality."[198]

The proposal is part of a three-fold regime. The first allows a minimum amount of data to be collected.[199] The second demands that privacy-enhancing default settings be the norm.[200] This is known as "privacy by default."[201] The third involves a concept of "data protection by design."[202] A hallmark of this is the concept of the individual's apparent right to continuous control over one's own information. For example, this includes the requirement of a data subject's consent to processing of information.[203] Notably, this consent necessarily would seem to be more than an agreement to a "terms of use" docu-

---

es (Jan. 25, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=IP/12/46&format=PDF&aged=1&language=EN&guiLanguage=en.

197 *See id.*

198 Rolf H. Weber, *The Right to Be Forgotten: More than a Pandora's Box?*, 2 JIPITEC 120, 121 (2011), *available at* http://www.jipitec.eu/issues/jipitec-2-2-2011/3084/jipitec%202%20-%20a%20-%20weber.pdf (explaining that the European concept of "the right to be forgotten can be considered as contained in the right of the personality [sic], encompassing several elements such as dignity, honor, and the right to private life").

199 *Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, at 43–44, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf (Articles 5 and 6).

200 European Commission, *How does the data protection reform strengthen citizens' rights?*, http://ec.europa.eu/justice/data-protection/document/review2012/factsheets/2_en.pdf (last visited Oct. 22, 2012) (explaining "privacy by design" and "privacy by default" as principles that require that "data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm").

201 Press Release, European Commission, Security industry: Commission proposes Action Plan to enable growth—further details (July 30, 2012), *available at* http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/12/605&format=PDF&aged=0&language=EN&guiLanguage=en; *Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, *supra* note 199, at 56 (Article 23).

202 *Commission Proposal for a Regulation of the European Parilament and of the Council on the protection of Individuals with regard to the processing of personal data and on the free movement of such data*, *supra* note 199, at 56 (Article 23).

203 *Id.* at 43–44 (Articles 5 and 6).

ment. Such "terms of use" agreements do little to effectively inform the consumer of her rights due to their length and complicated language. Additionally, they also hold the individual hostage by precluding the use of the service if he does not agree to the privacy infringements. The reforms address this by stating that "[c]onsent shall not provide a legal basis for the processing, where there is a significant imbalance between the position of the data subject and the controller."[204] Further, the individual does not lose his rights to his information once consent is given. Rather, he has the right to withdraw consent at any time.[205] Even after made public, the individual retains a "right to be forgotten and to erasure."[206] This allows individuals the right to request their data be deleted and compels the Internet service provider to completely delete all personal data belonging to an individual and communicate that request to third parties.[207] The rights of individuals include rights to transparent information, to information about and access to data collected, as well as rectification, and erasure.[208]

More recently, the federal government has also moved closer to conceptualizing the need for more individual control over one's personal data. In February 2012, the White House announced the *Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy*.[209] Here, the White House recognized that "additional [privacy] protections are necessary."[210] This framework contains a "Consumer Privacy Bill of Rights" that states: "Consumers have a right to exercise control over what personal data companies collect from them and how they use it."[211] Additionally, the Bill of Rights includes the "right to expect that companies will collect, use, and dis-

204 *Id.* at 45 (Article 7).

205 *Id.*

206 *Id.* at 51 (Article 17).

207 *Id.;* European Commission, *supra* note 200.

208 *Commission Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection, or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data* at 8, COM (2012) 10 final (Jan. 25, 2012), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:PDF (stating the rights of the data subject).

209 Press Release, The White House, We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online (Feb. 23, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.

210 THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

211 *Id.* at 47 (delineating the "Consumer Privacy Bill of Rights").

close personal data in ways that are consistent with the context in which consumers provide the data."[212]

This proposal is a move in the right direction; however, it falls short. For example, the White House proposal directs the Commerce Department's National Telecommunications and Information Administration ("NTIA") to develop the implementation of these rights. Unlike the European approach, the White House approach appears to intend a voluntary system for those affected companies. In its request for comment, the NTIA discussed "encouraging" companies to develop voluntary codes of conduct that would only be legally enforced if participants commit to them and then fail to comply.[213] However, voluntary regimes have not been successful.[214] For example, Google and other such companies change privacy policies with impunity to decrease the amount of protection provided by privacy terms from what it was when customers first signed on with the company.[215] Recently, the Europeans also warned Google that the new

212 *Id.*

213 Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct, 77 Fed. Reg. 43, 13098 (Mar. 5, 2012).

214 For example, Google had voluntarily agreed to a consent order in October 2011, following an FTC investigation. Elec. Privacy Info. Ctr. v. F.T.C., 844 F. Supp. 2d 98, 100 (D.D.C. 2012), *aff'd*, 2012 WL 1155661 (D.C. Cir. Mar. 5, 2012). Three months later, Google announced that it would change its privacy policy to allow much increased tracking of information, leading to the Electronic Privacy Information Center ("EPIC") filing a lawsuit that such action is in a violation of an October 2011 consent order in a previous lawsuit. *Id.* ("Google announced in January 2012 that it would implement changes to its user privacy policies for all of its services. EPIC contends that this intended policy change, which is scheduled to take effect on March 1, 2012, will violate the Consent Order. Although EPIC is not a party to the Consent Order, it filed a motion for temporary restraining order and preliminary injunction on the grounds that the FTC has a 'mandatory, nondiscretionary duty' to enforce it."); *see also EPIC v. FTC (Enforcement of the Google Consent Order)*, EPIC, http://epic.org/privacy/ftc/google/consent-order.html (last visited Oct. 30, 2012) (summarizing the background and news surrounding EPIC's lawsuit to enforce the Google consent order, as well as giving an overview of the legal proceedings); Somini Sengupta, *Consumer Rights Groups Says Google Broke Its Promise*, N.Y. TIMES BITS BLOG (Feb. 8, 2012, 8:45 PM), http://bits.blogs.nytimes.com/2012/02/08/consumer-rights-group-says-google-broke-its-promise/ (reporting on the respective positions of EPIC and Google on the litigation surrounding the potential violation of Google's consent order with the FTC by Google's announced data collection changes).

215 *See* John P. Mello Jr., *Facebook Changes Privacy Policy Again*, PC WORLD (Mar. 21, 2012, 11:17 AM), http://www.pcworld.com/article/252289/facebook_changes_privacy_policy_again.html (reporting on Facebook's decision to eliminate its "privacy policy" in favor of a "data-use policy" that allows more extensive collection and use of data by the company, and going on to note that users agree to the statement "simply by using Facebook" (quoting Sarah A. Downey, a Boston-area online privacy attorney)); Kang, *supra* note 181 (describing the plight of a Gmail user who "might never have imagined that the content of his or her [e-mail] messages could affect the experience on seemingly unrelated Web

policy "does not meet the requirements of the European Directive on Data Protection,"[216] but to no avail.

Additionally, the White House proposal is lacking specifics. As a technical matter, commercial entities could claim that today's users are given a choice not to be tracked that is arguably consistent with these vague White House concepts. But the choice is false. Consent must be meaningful for it to be a legitimate protection of privacy. It currently is not meaningful. Consent is not voluntary if obtained through a coercive or imbalanced terms of service agreement. By placing the consent provisions in such an agreement, use of the service is conditional on the "consent." That is hardly a voluntary consent; it seems more akin to coercion. Embedding consent in the terms of service is simply not a viable option for privacy protection if individuals cannot avail themselves of the service if they do not consent to the terms. While that may be appropriate for optional preferences, such as consenting to Internet service providers disclosing information when lawfully subpoenaed, it is not reasonable to demand consent to sell personal information to unknown third parties for profit in exchange for a needed service. For consent to be legitimate, it must be a result of an opt-in structure.

The concept of an opt-in provision has some support in the United States Congress. "Do Not Track" bills have been proposed in both the House and Senate.[217] The Do Not Track Me Online Act proposed to have the Federal Trade Commission promulgate rules for an "online opt-out mechanism" to allow consumers to effectively and easily prohibit the collection or use of "covered information."[218] However, it applied to limited entities whose primary business is collecting such information, covered only limited information, and carried an insignificant penalty.[219] Such a narrow focus does nothing to prevent the dissemination of one's image or images of items or prop-

---

sites such as YouTube" as an illustrative example of the potential privacy consequences of Google's decision to integrate data collected across its different services).

216 Letter from Isabelle Falque-Pierrotin, President, Commission Nationale de l'Informatique et des Libertés, to Larry Page, CEO, Google Inc. (Feb. 27, 2012), *available at* http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20120227_letter_cnil_google_privacy_policy_en.pdf.

217 For the House of Representatives bill, see Do Not Track Me Online Act, H.R. 654, 112th Cong. (2011). A similar bill was also introduced in the Senate. Do-Not-Track Online Act of 2011, S. 913, 112th Cong. (2011). A narrower third bill targeting the prevention of tracking of information regarding minor children was also proposed. *See* Do Not Track Kids Act of 2011, H.R. 1895, 112th Cong. (2011).

218 Do Not Track Me Online Act, H.R. 654, 112th Cong. § 3(a) (2011).

219 *Id.* at §§ 2(2), 2(3), 5(b).

erty that one has attempted to keep private.[220] The Senate version, the Do Not Track Online Act of 2011, is perhaps even weaker. It authorizes the Federal Trade Commission to promote regulations that allow individuals to indicate "whether [they] prefer to have personal information collected . . . ."[221] Even current coercive terms of service agreements would seem to comply with this vague proposal. Moreover, it seems to cover only the initial collection of information, and not subsequent use.

An opt-in system also appears to be technically possible. For example, in the context of satellite imaging, Google has the capability of obscuring images.[222] Google Earth and Google Street View have voluntarily complied with requests from governments to blur images for security reasons. These include blurring the entire city of North Oaks, Minnesota, whose roads are private, as well as locations such as governmental residences, military locations, research facilities, and energy sources which could be the target of a terrorist attack.[223] In Germany, Google will blur a resident's building at his request and over 244,000 Germans have requested such.[224] The Swiss Federal Supreme Court, in reversing an order requiring automatic removal of all Google Street View images, did require that 99% percent of the images be anonymized and that Google anonymize the remaining images upon request in an "efficient and unbureaucratic manner."[225] The court did require complete blurring of images of persons and

220 *See* Geissler, *supra* note 115, at 915.

221 Do-Not-Track Online Act of 2011, S. 913, 112th Cong. § 2(a)(1) (2011).

222 *See, e.g.*, Kelly Hearn, *Terrorist Use of Google Earth Raises Security Fears*, NAT'L GEOGRAPHIC (Mar. 12, 2007), http://news.nationalgeographic.com/news/2007/03/070312-google-censor.html (reporting that Google replaced detailed images of British military bases with pre-Iraq war data).

223 Lora Pabst, *North Oaks tells Google Maps: Keep Out—we mean it*, STARTRIBUNE (May 31, 2008) www.startribune.com/lifestyle/19416279.html (reporting on Google's compliance with the unanimous request of the citizens of North Oaks, in which roads are privately owned by residents, to be removed from Google Maps); *see also* IT Security Editors, *Blurred Out: 51 Things You Aren't Allowed to See on Google Maps*, IT SEC., http://www.itsecurity.com/features/51-things-not-on-google-maps-071508/.

224 Kevin J. O'Brien, *244,000 Germans Opt Out of Google Mapping Service*, N.Y. TIMES (Oct. 21, 2010), http://www.nytimes.com/2010/10/21/technology/21google.html. This would include allowing people to opt out of photo archives.

225 Press Release, Swiss Federal Supreme Court, Data protection matters in the context of Google Street View: Federal Supreme Court partially upholds Google's appeal (June 8, 2012), *available at* http://www.bger.ch/mm_1c_230_2011_d.pdf; *see also* Marta Falconi, *Swiss Court Hands Win to Google*, WALL ST. J., June 9–10, 2012, at B4 (reporting on the Swiss court's decision to uphold the privacy ruling requiring Google to manually blur out the 1% of faces that are not already blurred).

vehicle number plates prior to publication.[226] This ruling will require Google to lower its cameras to prevent viewing over walls and hedges because the ruling forbids publication of images not visible by passersby.[227] After public outcry, Google Maps Street View agreed to blur depictions of people and license plates in its images.[228] Furthermore, several Internet companies have expressed support for weak regulations and have not raised technical objections,[229] thus implying the regulations are technically possible.

The debate within the industry has focused not on infeasibility, but on definitions. In 2012, the World Wide Web Consortium, an international organization dedicated to the long-term growth of the web, convened a Working Group on Tracking Protection.[230] The purpose of their group was to develop standards for a "Do Not Track" policy to protect personal privacy, which allows one to use a one-click browser setting to set up an HTTP header that will tell websites one does not want to be tracked.[231] This discussion focused on definitions and challenges, and distinguished itself from industry-only efforts.[232] Interestingly, according to the privacy organization Electronic Frontier Foundation, the objection to this "Do Not Track" policy comes from online advertising organizations, who claim it will destroy their profits.[233] In contrast, Microsoft has announced its next version of In-

---

226 Press Release, Swiss Federal Supreme Court, Data protection matters in the context of Google Street View: Federal Supreme Court partially upholds Google's appeal (June 8, 2012), *available at* http://www.bger.ch/mm_1c_230_2011_d.pdf.

227 O'Brien & Streitfeld, *supra* note 122; *Google Partially Wins in Swiss Street View Privacy Row*, LAW360 (June 8, 2012), http://www.law360.com/privacy/articles/348310/google-partially-wins-in-swiss-street-view-privacy-row (reporting on the limitations imposed on Google by the highest Swiss court).

228 Elinor Mills, *Google now zaps faces, license plates on Map Street View*, CNET (Aug. 22, 2007, 2:02 PM), http://News.cnet.com/8301-10784_3-9764512-7.html#! (explaining that "partly in response to criticism," Google has changed its privacy policies so that "anyone can alert the company and have an image of a license plate or a recognizable face removed").

229 Julia Angwin, *Web Firms to Adopt 'No Track' Button*, WALL ST. J., Feb. 23, 2012, at B1 (reporting on the decision of a "coalition of Internet giants" to support the adoption of no-tracking buttons).

230 Rainey Reitman, *April 2012, the State of Do Not Track: Lead Up to Tracking Protecting Working Group Negotiations in Washington, DC*, ELEC. FRONTIER FOUND. (Apr. 5, 2012), https://www.eff.org/deeplinks/2012/04/april-2012-state-do-not-track-lead-tracking-protecting-working-group-negotiations (providing an overview of the World Wide Web Consortium Tracking Protection Working Group meeting).

231 *Id.*

232 *Id.*

233 *Id.* (describing the Interactive Advertising Bureau's annual leadership meeting in which President and CEO Randall Rothenberg criticized the efforts of those working for Do Not Track, stating it had the potential to destroy their business); *see also* Peter Eckersley, *Will Industry Agree to a Meaningful Do Not Track?*, ELEC. FRONTIER FOUND. (Apr. 16, 2012), https://www.eff.org/deeplinks/2012/04/will-industry-agree-meaningful-do-not-track

ternet Explorer, IE10, will have "do not track" as its default browser setting, requiring users to affirmatively opt-in to tracking.[234] This seems to fly in the face of the Association of National Advertisers argument that such a move will destroy businesses.[235]

C. Future

These initiatives, both domestic and international, provide support for legislation requiring an "opt-in" to information sharing based on a conceptualization of ownership of digital information. Such legislation must have certain characteristics. It must address functionality, not technology. Here the functionality is commercial grooming to eradicate the reasonable expectation of privacy by obtaining information and displaying it. It must have a meaningful opt-in provision that is not tied to the terms of service. Finally, it must incorporate concepts of data ownership by the individual.

In the satellite imaging technology scenario, this could similarly be accomplished. The individual would by default be assumed *not* to disclose property to the entities that image and publish it. The automatic setting is to minimum disclosure. If this information is collected, the individual owns the image of his private property and has the right to preclude its publication.

This legislation, combined with current Fourth Amendment jurisprudence, would restore the necessary privacy protections. It would not only protect privacy, but it would do so by providing the mechanism by which one can demonstrate one's expectation of privacy. Thus, application of the *Katz* test would be appropriate because a court would have some way of determining if a person demonstrated his expectation by selecting not to opt in to disclosure.

Interestingly, Justice Scalia's trespass-based solution may then prove viable, if combined with the concept of *ownership of data*. If the law were to recognize that individuals *own* their digital footprints, then when the government obtains this data in collecting information, it has "engag[ed] in physical intrusion of a constitutionally

---

(stating that advertising industry representatives insist that they be allowed to continue third-party tracking, even on browsers which have the "Do Not Track" HTTP header for marketing and online advertising purposes).

234 David Goldman, *Microsoft turns on 'do not track' by default in IE10*, CNN MONEY (June 1, 2012), http://money.cnn.com/2012/06/01/technology/Internet-explorer-do-not-track/index.htm (reporting on Microsoft's decision to implement "Do Not Track" as a default in the new version of Internet Explorer).

235 *Id.* (reporting on the argument of the Association of National Advertisers that Microsoft's plan is "irresponsible").

protected area in order to obtain information . . . ."[236] As such, a search has occurred under *Jones*. Such a marrying of concepts—ownership of digital information and a trespass-based analysis—may then provide additional protection. The landscape would be as follows: an individual owns her digital footprint when it is information about herself or about papers, houses, or effects which she has demonstrated a desire to keep private by not actively disclosing that information. A company may not condition her expectation of privacy. Rather, information will be private if she has *not* opted for its disclosure. Should the government use technology to gain that information, it has conducted a search.

CONCLUSION

The contemporary problem is that individuals no longer possess true subjective expectations of privacy due to an awareness of the possibility that information about them will be gathered through publicly available technologies. The consequences of this must be altered. Under today's regime, the consequences include a lack of Fourth Amendment protection. Such should not be the case, particularly when that lack of expectation is due to commercial conditioning. Instead, our legislative response should adopt a data ownership model for data exposed either through no action of the individual or collaterally to a transaction. This model should require an opt-in approach for information sharing and an ability to retrieve published information when desired. This ownership model works with our fundamental Fourth Amendment understandings. Thus, the individual has an option to demonstrate her privacy expectations and trigger Fourth Amendment protection.

236 United States v. Jones, 132 S. Ct. 945, 951 (2012) (quoting United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)).