The Court Misses the Point Again in United States v. Jones: An Opt-In Model for Privacy Protection in a Post Google-Earth World

Mary G Leary, The Catholic University of America

Available at: https://works.bepress.com/mary_leary/1/
THE COURT MISSES THE POINT AGAIN IN

**United States v. Jones:**
AN OPT-IN MODEL FOR PRIVACY PROTECTION IN A POST-
GOOGLE EARTH WORLD

MARY G. LEARY*

**INTRODUCTION**

Imagine a community in which a police officer with no suspicion at all, but a curiosity, or even a vendetta, wanted to spy on a citizen. Perhaps this curiosity was a concern that the citizen was laundering money, accepting bribes by way of free home additions, using the curtilage of his yard as a meeting place for large (or illegal) groups, or using that space for illegal activity such as storing stolen vehicles or growing illegal narcotics. Imagine further, that he effectuated this suspicionless spying by hiring a high powered satellite with the capability of orbiting over the citizen’s home every 24 hours and recording an image close enough to that private property to clearly see items the size of home plate. Further, imagine that the citizens of this community are aware of the ability to spy in this manner, but have no knowledge of when the police are doing so or a mechanism through which they can object. They may have fenced off their property to conceal the activities conducted in the private curtilage of their property. The police, however, have the ability to review images taken over several months and observe changes to this area such as the presence of possibly stolen materials, evidence of a secret outdoor meeting spaces, or evidence of unlicensed home improvements. The police could even drive up a public street or private road with a high tech 360 degree camera mounted on the roof of their vehicle which simultaneously records GPS measurements and photographs citizens’ homes, vehicles parked in front of them, 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 sound like the police surveillance system of a military dictatorship or a futuristic Orwellian world, it, in fact, describes our

---

* Associate Professor, Co-Director of Law and Public Policy Institute, The Catholic University of America Columbus School of Law.
world today. Through satellite imaging technology, such as Google Earth (and its companion technologies of Google Street View and Google Maps) or Microsoft’s Virtual Earth, law enforcement and indeed any citizen can do just this. Many citizens 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.’”  

Most citizens would likely regard such police activity as a government “search” requiring a warrant. However, under current caselaw it is not a search and citizens have no protection from it or from its effect of eroding their sense of privacy. Some may argue that this state is merely a reflection of our times. This reality, however, 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: a world in which most people have lost a subjective expectation of privacy and thus eroded any expectation of privacy society is objectively willing to accept. Yet, for the past forty years, our jurisprudence has defined a search worthy of Fourth Amendment protection as a government examination of an area in which a citizen has a “reasonable expectation of privacy.”

The Court has failed 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. Most notably in United States v. Jones the Court’s expanded definition of a search, by resurrecting its former trespass analysis, fails to keep current with technology. The specific effect of this failure is diminished Fourth Amendment protections.

The Court has stated that when the government has conditioned citizens to have no expectation of privacy it will modify its test to accommodate. However, the Court has not contemplated today’s reality that private corporations, not the government, have conditioned citizens to have no expectation of privacy. Corporations have further afforded ordinary citizens no opportunity to demonstrate any remaining subjective expectations, thus stripping them of Fourth Amendment protections. If a “search” requires a subjective expectation of privacy, and technology has stripped citizens of any such expectation, then little of what the government does will be a search and trigger Fourth Amendment protections.

1 United States v. Dunn, 480 U.S. 294, 300 (1987)  
Such diminishments, mischaracterized as “voluntary,”5 are more aptly labeled the products of corporate conditioning. United States v. Jones,6 is the most recent example of the inability of current Fourth Amendment search doctrine to respond to 21st century surveillance.

This article suggests a legislative solution to this reality. 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 publicly available technology and the Constitutional problem it poses. Part III identifies a threat to privacy expectations unanticipated by the Court. 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 scenario of today. Namely, it did not contemplate diminished subjective and objective expectations of privacy resulting from commercial “conditioning…alien to Fourth Amendment freedoms.” Here, a comprehensive analysis demonstrates the inadequacy of the Court’s alternatives, including those in in Jones. This article proposes a new legislative framework for respecting privacy protections in response to these corporate induced privacy affronts.

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.”7 Should the government engage in a search or seizure, it must do so pursuant to a warrant or an exception to the warrant requirement.8 These constraints apply only to governmental searches and seizures.9 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

---

5 Jones, 132 S.Ct. at 957 (Sotomayor, J., concurring) (“People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers…I would not assume that all information voluntarily disclosed to some member of the public for a limited to purpose is, for that reason alone, disentitled to Fourth Amendment protection”).
6 Id. at 945.
7 U.S. Constitution, Amendment IV.
8 “…no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Constitution, Amendment IV. Kentucky v. King, 131 S. Ct. 1849, 1856 (2011) (presumption of warrant to search home can be overcome under certain reasonable exceptions).
protections are triggered. Yet the Court has struggled in defining a “search.”

Perhaps as early as Justice Brandeis’ 1890 article “The Right to Privacy” these questions have been examined through a lens of privacy. From 1967 through January of 2012, the law has almost exclusively applied the two pronged Katz test to determine the applicability of the Fourth Amendment to governmental searches. 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 a citizen has a “reasonable expectation of privacy.” The reasonableness of this expectation is determined by establishing that (1) the citizen demonstrated 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). 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 on 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.” Indeed, both litigants in Katz had framed their arguments around whether the public phone booth at issue was a “constitutionally protected area.” The Court rejected that and replaced it with the notion that, “the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not subject to Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public may be constitutionally protected.…” In this analysis, the Court rejected that trespass framework and reframed the legal issue as whether Katz knowingly exposed information to the public or attempted to keep said information private.

---

13 Katz, 389 U.S. at 361.
16 Katz, 389 U.S. at 352.
17 Originally the Court was poised to answer two questions: the question presented by the parties was “whether the warrant has use of a tracking device on
However, in *United States v. Jones*, five justices recently recharacterized this jurisprudence to assert that both the privacy analysis as well as the physical trespass analysis is the current framework for a determination of whether government activity is a search.

**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 the *Katz* test, its author, Justice Harlan, expressed concern about the misuse of this two pronged test. In dissent, Justice Harlan questioned the plurality’s application of the *Katz* test to a situation in which a government agent hid in a closet listening to a conversation between the defendant and confidential informant, and later testified to the overheard conversations. Justice Harlan asserted that the plurality’s rote application of this test (which found no expectation of privacy) “…can, ultimately, lead to the substitution of words for analysis.” He demanded a more value-laden question be asked, namely whether the law should require Fourth Amendment protections.

Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules and 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.

Justice Harlan 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 cautioned against rigidly applying a test while losing sight of its purpose. He also offered an alternative test when the two pronged *Katz* test failed. The alternative was rooted in the Court engaging in this more fundamental analysis. For him “[t]he critical

---

19 See infra n.______.
21 White, 401 U.S. at 788
22 White, 401 U.S. at 788 (emphasis added).
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.” 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.”

2. Justice Blackmun

In Smith v. Maryland, Justice Blackmun, writing for the majority, acknowledged “[s]ituations can be imagined, of course, in which Katz’ two-pronged inquiry would provide an inadequate index of Fourth Amendment protection.”

For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such 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 case, a normative inquiry would be proper.

Thus, the Court cautioned that the government could not limit privacy expectations merely by conditioning citizens to believe they are subject to surveillance, and thus destroy their ability to establish a subjective expectation of privacy. The Court, however, did not envision what appears to be happening today - individual citizens are being “conditioned” by corporate influences alien to well-recognized Fourth Amendment freedoms. Citizens are losing their right to privacy due to commercial forces removing that expectation without affording citizens the opportunity to demonstrate a privacy expectation.

23 White, 401 U.S. at 788.
24 White, 401 U.S. at 786.
3. Justice Scalia and Kyllo

Justice Scalia has been a longstanding critic of the Katz test, rather famously noting that “the only thing the past three decades have established about the Katz test...is that, unsurprisingly, those ‘actual (subjective) expectation[s] of privacy’ ‘that society is prepared to recognize’ as ‘reasonable,’ bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable.”27

In 2001 Justice Scalia continued his dismissal of the Katz approach in Kyllo v. United States.28 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.29 In so doing, however, Justice Scalia did not rely on nor embrace Katz, but echoed his previous criticism.30 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 seemed to draw an important distinction when the home itself is the target of police information gathering even if done from a public place. Ultimately 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 (as here) the technology in question is not in general public use.”31

Justice Scalia’s return to a common law trespass based analysis is not without its critics. Justice Alito laid out five objections to Justice Scalia’s approach in Jones, including the “little if any support in current Fourth Amendment caselaw.”32 These include misplaced significance, incongruent results, and a lack of uniformity among states. Justice Alito found the 21st Century technology issues should not be settled based on 19th Century tort law.34 Justice Alito’s major critique that such an approach has been rejected by the court is not without merit.35

C. United States v. Jones

29 Kyllo, 533 U.S. at 31, 34.
30 Kyllo, 533 U.S. at 34.
31 Kyllo 533, U.S. at 35.
32 Id. (Alito, J., concurring).
33 Id. (Alito, J., concurring).
34 Id. (Alito, J. concurring).
35 Katz, 389 U.S. at 352-353 (“the premise that property interests control the right of the government to search and seize has been discredited.”) Id. (“the reach of that Amendment cannot turn upon the presence or absence of a physical intrusion...), Id. (“‘trespass’ doctrine …can no longer be controlling.”)
In *Jones*, the Court had the opportunity to address the current use of technology by the government to conduct surveillance on citizens. 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.\(^{36}\) Nine Justices concluded that such activity constituted a search.\(^{37}\) However, the Court was divided as to the approach and missed an opportunity to reframe the question of privacy so as to reflect 21\(^{\text{st}}\) Century norms.

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.”\(^{38}\) In so doing, Justice Scalia diminished the importance of the *Katz* test, stating that “Jones’s Fourth Amendment rights do not rise or fall with the *Katz* formulation.”\(^{39}\) Rather, the majority asserted the fundamental mission of the Court was not to reflect current privacy expectations, but to “assur[e] preservation of that degree of privacy against the government that existed when the Fourth Amendment was adopted.”\(^{40}\) To reflect this 18\(^{\text{th}}\) 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*…. “[W]e [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.”\(^{41}\)

The *Jones* majority explicitly states that trespass is not the exclusive test, or alone sufficient.\(^{42}\) However, it 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, the intrusion may constitute a violation of the Fourth Amendment.”\(^{43}\)

\(^{36}\) 132 S.Ct. at 949.

\(^{37}\) Id.

\(^{38}\) Id.

\(^{39}\) Id. at 950.

\(^{40}\) Id. (citing *Kyllo v. United States*, 533 U.S. 27, 34 (2001)).

\(^{41}\) Id. at 950 – 1 (citing *Alderman v. United States*, 394 U.S. 165, 180 (1969)).

\(^{42}\) Id. at 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 obtain information.’”)

\(^{43}\) Id. at 951 (citing *United States v. Knotts*, 460 US 276, 286 (1983) (Brennan, J., concurring)). The majority’s support for this claim that *Katz* did not replace the
Justice Alito, writing for Justices Ginsburg, Breyer, and Kagan, concurred in judgment but rejected the reversion to a trespass analysis. Justice Alito concurred that the GPS surveillance was a search, but “would analyze this case by asking ‘whether the respondent’s reasonable expectations of privacy were violated by the long term monitoring of the movement.” He concluded under a pure *Katz* analysis “that lengthy monitoring that occurred in this case constituted a search under Fourth Amendment.” Notwithstanding that conclusion Justice Alito left open the possibility that shorter term monitoring might be constitutionally permissible. In so doing, Justice Alito rejected the majority’s breathing new life into the trespass approach which he regarded as discredited. “In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass based theory.” Justice Alito acknowledged that a *Katz* analysis was somewhat inadequate in an era of increasing technological surveillance, and appealed for legislative response.

trespass analysis but supplemented it is somewhat dubious. The main authority for this proposition is of concurring opinions and their responses to the cases cited by Justice Alito. *Id.* (citing *Soldal v. Cook County*, 506 U.S. 56, 60, 62, 64 (1992) (“The majority the cites to *Soldol*, which the majority characterized as establishing ‘property rights are not the sole measure of Fourth Amendment violations,’ but ‘did not snuff out the previously recognized protection for property’); *Id.* 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); see also *Katz v. United States*, 389 U.S. at 357, 353 (1967)); *see also Rakas v. Illinois*, 439 U.S. 128, 143 (1978) (“The premise that property interests control the right of the Government to search and seize has been discredited.”); *see also Kyllo v. United States*, 533 U.S. 27, 32 (2001); *see also United States v. Karo*, 468 U.S. 705,713 (1984).

*Id.* at 958 (Alito, J., concurring).

*Id.* at 964 (Alito, J., concurring).

*Id.* (Alito, J., concurring).

*Id.* at 961 (Alito, J., concurring) (“In sum, the majority is hard pressed to find support in post-*Katz* cases for its trespass-based theory); *see Katz*, 389 U.S. at 353 (discrediting trespass analysis).

*Id.* at 961 – 2 (Alito, J., concurring) (Justice Alito also cited four additional problems with the majority opinion: (1) the majority disregards the significance of long term GPS tracking but misplaces significance to the trivial act of placing the device on a car; (2) this approach produces incongruous results in which a GPS attachment automatically triggers a search, not matter how brief, but comprehensive 24-hour monitoring through aerial and visual surveillance does not; (3) this approach will produce different results from state to state based on the property laws of the state; and (4) “the Court’s reliance on the law of trespass will present particularly vexing problems in case involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.”)

*Id.* at 964 (Alito, J., concurring) (“In circumstances involving dramatic technological chance, the best solution to privacy concerns may be legislative. *See*, e.g., Kerr, 102 Mich. L.Rev., at 805 – 806. A legislative body is well situated to
Although 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,” she wrote separately, agreeing in substance with much of Justice Alito’s opinion. In so doing, Jones arguably possesses two five justice opinions. Like Justice Scalia, she asserted that privacy protections include both the minimum trespass analysis, as well as the Katz approach where the trespass analysis was not applicable. However, unlike Justice Scalia, she did not seem assured that the sole answer to these contemporary challenges lay in 18th Century truisms. Justice Sotomayor more so than either Justices Scalia or Alito, was particularly concerned about the increased ability of law enforcement to search without physical intrusion but through technological advancement. She went further than Justice Alito, stating that “cases involving even short-term monitoring… require particular attention.” She explicitly expressed a desire that the jurisprudence reflect an understanding of the technological realities of contemporary monitoring. She noted concern about the high volume of information which could be obtained from 24 hour monitoring of one’s vehicle through a GPS device, the inappropriateness of entrusting the government to use a tool “so amenable to misuse,” and the questionable validity of the Third Party Doctrine in an age when technology requires people to “reveal great deal of information about themselves to third parties in the course of carrying out mundane tasks.”

II. Surveillance, Obtaining Information, and Satellite Imaging Technology

The Supreme Court’s recent articulation that the Fourth Amendment can be implicated when the government engages in an “attempt to find

gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.”).

50 Id. at 952; 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”).
51 Id. (Sotomayor, J. concurring) (“Under that rubric, I agree with Justice Alito that, at the very least, ‘longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.’ Post, at 964”).
52 Id. at 955 (Sotomayor, J., concurring) (…physical 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.”).
53 Id. (Sotomayor, J., concurring).
54 Id. (Sotomayor, J., concurring).
55 Id. at 956 (Sotomayor, J., concurring).
56 Id. at 957 (Sotomayor, J. concurring).
something or to obtain information”57 has significant implications. By way of example, police use of satellite imaging technology when used to examine the private property of a citizen surely does so.

Today, law enforcement, and any citizen with Internet access for that matter, has the ability to use a high powered satellite to examine the property of another in some detail anywhere in the world. No warrant is required. The citizen who is the subject of such surveillance has no choice in this no matter what they do to deny public access to their property. While such examinations are not real time video footage of one’s property, they do allow observation of relatively recent images of one’s property and compare them 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 if history is any lesson, may reach commercial viability.58 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 activity is through a combination of satellite imaging technology and software processing. Satellite imaging technology is a component of the technology which allows one to access images of a specific location in the world and zoom into obtain a view approximately 5 meters away. A common example of this is Google Earth. Combined with Google Street View, this allows law enforcement or civilians to access pictures of one’s property through a powerful satellite and observe how said area changed over time. Google Earth is one of a group of services which allow one access to satellite imaging technology and enhance it for more detail.59 Google Earth images are sourced from not only satellite imagery but also aerial photography and data from many imagery providers.60 Google describes its service in this way, “Google

57 Id. at 951, n. 5 (“Like 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.”).
58 Brian Bennett, Police Employ Predator Drone Spy Planes on the Home Front, Los Angeles Times, December 10, 2011 (discussing use of U.S. Border Patrol drones by local police); ACLU, Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, December 2011 (discussing use of drones at all levels of law enforcement and FAA efforts to develop policy to make such use easier).
Earth lets you fly anywhere to view satellite imagery, maps, terrain, 3D buildings, galaxies in outer space, and the depths of the ocean.61 While other companies provide this service, Google Earth is paramount among them due to the large amount of media coverage it receives.62

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. 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.”63 At the time of the acquisition, Google described the acquisition as giving Google users

“a powerful new tool, enabling users to view 3D images of any place on earth as well as to 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 computer 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.”64

Google later contracted with high resolution satellite companies such as Digital Globe and Geo Eye which launch satellites and provide the imagery to Google.65 These companies describe these images as “high

---

64 Id.
resolution” producing “high quality images.”

Some of the satellites owned by such companies have the capacity to record images at 50 cm resolution. One such company explains that this level of detail allows customers to “map natural and man-made features to within five meters (about 16 feet) of their actual location on the surface of the Earth.” 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.

However, Google also supplements these images with those obtained by aircraft which is as high as 15 cm resolution.

Today, Google Earth has continued to grow in its abilities to monitor images from anywhere in the world. Google uses satellites owned by third party operators, most of whom are private but at least some are related to some government agencies. Each of the parties has numerous satellites which vary in ability to record data. Generally, these satellites travel a certain orbit which allows them to orbit the earth as many as 18 times a day and return to a specific location once every 1.1-3.7 days. While in orbit,


67 GeoEye – Elevating Insight, “High-Resolution Imagery – Resolution Modes,” GeoEye, Inc., http://www.geoeye.com/GeoEye101/satellite-imagery/high-resolution-imagery.aspx (Site last visited February 10, 2012, 11:21 am) (The GeoEye-1 satellite can record images at 41 cm resolution - which allows one to “see home plate on a baseball field.” However, the NOAA requires satellite imaging companies to convert these images to 50 cm resolution for commercial use).


they can observe land for a lengthy period of time. These are not live pictures with a live feed to the Internet. These images are collected, uploaded, stored, transmitted and processed before being placed on the Internet. Although not live, the ability to quickly turn around photographs has been demonstrated by recent world disasters such as the 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*. DigitalGlobe, one of the third party satellite operators, has promised that its next generation of satellite will possess enough speed to re-examine the same geographical location within 24 hours. Indeed CNES (“Centre National d’Etudes Spaciales”) asserts that its satellites can work in tandem to cover a 120 km swath of land, acquire imagery of any point in the globe in some cases in less than 3 days; another asserts its can cover almost the entire globe every day.

While these satellites are owned primarily by third parties, with some there is 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. Indeed, CNES argues that its “Earth observation

http://www.digitalglobe.com/downloads/WorldView1-DS-WV1-Web.pdf,


75 “WorldView-3 – Data Sheet,” DigitalGlobe, Inc.,

76 “SPOT-5 Instrument Features,” CNES, Inc., http://spot5.cnes.fr/gb/systeme/42.htm (Site Last Visited February 10, 2012) (Each HRG instrument has a field of view of 4°, meaning that it can observe a swath of 60 kilometers on the ground, and can be pointed off-vertical 27° both ways for oblique viewing. Like on SPOT 4, the two instruments generally operate independently to observe separate targets, but they can also view in tandem to cover a 120-kilometre swath in a single pass. The HRG instruments' oblique viewing capability means that SPOT 5, like its predecessors, can acquire imagery of any point on the globe within less than five days, or even in less than three days at temperate latitudes.”); “Diplomatic Facility Support Package,” DigitalGlobe, Inc. http://www.digitalglobe.com/downloads/DipFac-DS-DFSP-Web.pdf (Site Last Visited February 10, 2012) (DigitalGlobe’s “Diplomatic Facility Support Package” which “assists the evacuation of citizens and others by providing web based access to consistently refreshed imagery and feature information of diplomatic facilities and important local infrastructure.”).
satellites are vital assets for science, industry and the military alike. Carrying ever enhanced viewing instruments, they can acquire repeat coverage of vast areas systematically and yield detailed images."77 Google has an exclusive contract for online use of imagery supplied by Geo Eye.78 Geo Eye, the satellite provider which provides said information to Google was also awarded 3.8 billion dollars contract with the National Intelligence Agency (NGA)80 which is GeoEye’s largest customer accounting in 2009 for 65% of its revenue.81

With this technology in the hands of government officials, the implications for police examinations are significant. Yet the evidence of such technology is known to the citizenry. Therefore, they have not demonstrated a subjective expectation that the government will not use the technology. However, they have not demonstrated that expectation because Google never afforded them the opportunity to demonstrate it by opting out of the imaging. So they are powerless to stop this privacy encroachment.

III. The Problem Is Not Trespass or Government Use of Technology: It is the Problem of Ubiquitous Electronic Surveillance Ability by Corporations and its Effect on Citizenry

As recognized to some degree by Justices Alito and Sotomayor in their Jones concurring opinions, technological advances have altered the landscape significantly since 1967. Technological development of the

telephone pushed Fourth Amendment jurisprudence forward to *Katz*\textsuperscript{82} to recognize that the old way of measuring a search, the physical trespass, was not longer solely sufficient to protect what was deemed as private under the Fourth Amendment. So too we again find ourselves in need of a 21st century solution.

Justice Sotomayor was most attuned to and alarmed at technology’s alteration of privacy expectations in *Jones*. Her main concern, however, was the government’s unrestrained ability to collect data.\textsuperscript{83} She recognized that the *Katz* approach may be “ill-suited to the digital age” in which people reveal a great deal of information about themselves to third parties.\textsuperscript{84}

This recognition of technological change is absent from the majority opinion. Although there is significant disagreement between Justices Scalia and Alito as to whether *Katz* discarded the trespass approach to searches, at a minimum, post *Jones*, the Court can either apply a *Katz* analysis or a trespass analysis. Justice Scalia explicitly asserts that, “[w]e do not make trespass the exclusive test. Situations involving merely the transmission of electric signals without trespass will remain the subject of the *Katz* analysis.”\textsuperscript{85} However, in doing so he suggests that is not common. But as the two concurring opinions underscore, that is the vast majority of surveillance technologies today. Once understood, that such a reality has led to a lack of subjective expectation of privacy, the need to rethink our framework is apparent.

A. This Problem is Exemplified Visually with the Satellite Imaging Technology but Many Other Technologies As Well

The satellite imaging technology exemplifies such a reality of the nature of technology and indeed, its effect on privacy expectations. Without physical trespass, law enforcement or any citizen can attempt to gain information regarding a citizen and his living or business habits which occur out of public view. It is the latter half of that statement, i.e. the fact that anyone can do so, which provides the largest challenge to current Fourth Amendment attempts to protect privacy. The reason for this is that the knowledge that the technology exists leads the citizen to the area around the home is not private. As such, under our current jurisprudence, he loses the expectation of privacy. For his reason, there have been attempts to adjust and proposed alternatives to *Katz*, but they have all fallen short.

\textsuperscript{82} United States v. Jones, 132 S.Ct. 945, 955 – 6 (Sotomayor, J. concurring) (“In cases involving even short-term monitoring, some unique attributes GPS surveillance relevant to the Kats analysis will require particular attention. 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...The Government can store such records and efficiently mine them for information years into the future.”).

\textsuperscript{83} *Id.* at 957 (Sotomayor, J., concurring).

\textsuperscript{84} *Id.* at 953.
B. Neither the Jones nor Katz Approaches Respond Adequately to this Scenario

At first glance, it may appear that there are no Fourth Amendment ramifications of these technologies because of precedent allowing substantial law enforcement surveillance. The combined caselaw that permits law enforcement to examine curtilage from navigable airspace,\(^{86}\) to monitor one’s movements on public thoroughfares;\(^{87}\) and to accept information disclosed to third parties (third party doctrine) initially indicates government use of satellite imaging technology is without constitutional significance. However, this argument misses the issue which is not the propriety of law enforcement’s use of satellite imaging technologies, which itself raises questions. Rather, this 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 commercial or social conditioning?

One ramification of this conditioning could be that no citizen possesses a subjective expectation of privacy in the curtilage of his or her home. In effect, our yards, back patios, fenced in structures, or plantings all completely removed from public view have become “open fields” and, therefore, searchable. Similarly, the data collected from us online, at times, unbeknownst to us, is available for review. Indeed, in a recent Court of Appeals case regarding Google Street View, Google reportedly argued that in light of satellite imaging technology, “complete privacy does not exist.”\(^{88}\) This assertion suggests such is true even when an individual has no opportunity to demonstrate a subjective expectation of privacy by opting out of Google Earth or retaining their private information. Furthermore, even if an individual possessed such a subjective expectation, such a claim would likely fail the second prong of Katz as it is difficult to imagine society would be willing to accept such an expectation in light of the broad use of this technology.

What is needed today is a reframing of the issue to reflect contemporary reality. Justice Scalia’s approach in Jones, which echoes of his opinions in Kyllo,\(^{89}\) was strongly criticized as applying an 18\(^{th}\) century solution to a 21\(^{st}\) century problem.\(^{90}\) Prior to Kyllo, when faced with an

---

90 Id. at 957 – 8, nn. 1 – 2 (Alito, J., concurring) (“Ironically, the Court has chosen to decide this case based on 18\(^{th}\)-century tort law. By attaching a small GPS device
issue involving enhanced technology being used by law enforcement, the Court almost always narrowed the protections of the Fourth Amendment. Justice Scalia, no friend of the *Katz* test, writing for the majority in *Kyllo*, found the police use of thermal imaging constituted a search. Curiously absent from the majority opinion was any endorsement of *Katz*. Rather, Justice Scalia described the *Katz* opinion as “circular.” Justice Scalia based his *Kyllo* analysis of new technology on two factors: (1) whether the technology ascertained information from a constitutionally protected area which 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 protected area’ constitutes a search—at least where (as here) the technology in question is not in “general public use.”

However, this approach misses two fundamental realities. First, the bulk today’s privacy threats do not appear to involve physical trespass. Whether it is satellite imaging technology, triangulating cell phone signals, government operated video cameras, or drone operation, the police are able to search more deeply into citizen’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. While the home may be an area in which all would agree its occupants would consider highly private technology allows the searching of many more areas in which one can obtain a treasure trove of information. For example, Justice Sotomayor describes GPS surveillance,

… generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her

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). *Jones*, No. 10-1259, slip. op., (Alito, J. concurring).

---

91 *Smith* 422 U.S. 745 (pen register); Cilraolo 476 U.S. 207 (airplane surveillance); *Dow Chemical v. United States* 476 U.S. 227 (1986) (mapping photography of an industrial complex).
92 *Kyllo*, 533 U.S. 27.
95 *Katz*, 389 U.S. 347.
96 But see *California v. Carney*, 471 U.S. 386.
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 evades the ordinary checks that constrain abusive law enforcement practices.97

Similarly, satellite imaging technology observes curtilage, but the Court has previously held that as long as done from legal airspace with no interference in the possessory interest of the property, then no violation occurs.98

Secondly, access to such technological abilities is now frequently generally public use. Satellite imaging technology is accessible through free programs such as Google Earth and Virtual World and available to anyone with an Internet connection.99 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 in which one attempts to cabin off commonly used technologies from government use, yet the very same action is constitutional when done by a neighbor.

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 test has been added to, not substituted for, the common law trespassory test,”100 may incorrectly lead one to conclude that Jones offers increased privacy protection. As a practical matter is does not for the vast majority of surveillance techniques. Similarly, the Court’s passing suggestion that when the government is “attempting to find something or obtain information,”101 it engages in a search is also deceptively broad. The Court clarifies by stating that for that particular definition, such activity must be “conjoined” with a trespass.102 With satellite imagining technology, online data collection, and other technologies, unlike GPS technology, there is no physical trespass. As such, the majority’s opinion does nothing to enhance privacy protections in such a context. Indeed this is the caution offered by Justice Sotomayor and

99 273 million people in America are reported as users of the Internet, www.internetworldstats.cin/stats.htm.
101 Jones, 132 S.Ct. 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.”).
102 Id.
However, none of the opinions adequately address the effect on the subjective expectation of privacy.

V. Alternative Approaches Offered by Justices Fall Short in Addressing Today’s Reality of the Decreasing Subjective Expectation of Privacy

A. Justice Harlan’s Balancing Test

Justice Harlan’s balancing approach has significant drawbacks in this situation. When the subjective expectation of privacy is lost, Justice Harlan would 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. While an important philosophical question, its answer 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 citizen use would be artificial. 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. Regarding satellite imaging technology, such would be impossible to measure when the complaint is that there is no subjective belief in the privacy at all. As such, law enforcement’s use of it is unlikely to more severely impact one’s sense of security than the technology itself. Therefore Justice Harlan’s test fails to adequately respond to this 21st century problem.

B. Justice Blackmun’s Normative Inquiry

Justice Blackmun’s normative approach may be a solution for the problem he envisioned: a deterioration of privacy expectations caused by

---

103 *Id.* at 957 (Sotomayor, J., concurring) (Justice Sotomayor calls into question the validity of the Third Party Doctrine in today’s technology driven world. “This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying on mundane tasks.”). *Id.* at 963 (Alito, J., concurring) (Justice Alito focuses his comments on devices that permit monitoring people’s movement including closed circuit television, GPS services installed in vehicles and cell phone, personal locator technology.).
government “conditioning.” However, when the expectation is lost by all of society being conditioned by corporations, 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 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 corporations and social forces. Furthermore, because many of these technologies offer no ability for a citizen to demonstrate an expectation of privacy, by opting out of this monitoring, a measure of what the social norm is or should be is likely impossible.

C. Justice Sotomayor’s Rejection of Government Data Collection

Of the opinions articulated in Jones, Justice Sotomayor is most aware of the implications of ubiquitous technology on society’s expectations. While she joined Justice Scalia’s majority opinion, she indicates she did so, because she viewed Justice Alito’s approach as perhaps more privacy limiting, although she agreed with much of its reasoning.

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.104

She is the most aware of the three opinion writers about the effect of this technology on societal and individual expectations. She agrees with Justice Alito’s “incisive” observation that “the same technological advances that have made possible non-trespassory surveillance techniques will also affect the Katz test by shaping the evolution of societal privacy expectations.”105 Unlike Justice Alito, however, she has the most appreciation for the effect of this technology, not on the government’s ability to conduct surveillance, but on the deeper question identified in this article - its effect on subjective and objective expectations.

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government’s unrestrained power to assemble data that

104 Id. at 955 (Sotomayor, J., concurring).
105 Id. (Sotomayor, J., concurring).
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.”

Justice Sotomayor is alone in recognizing this fundamental issue. Her response is almost a hybrid of those offered by both Justices Harlan and Blackmun. She first seems to suggest that it is proper to review societal norms. However, she then suggests that it is important to follow Justice Harlan’s lead and examine the desirability of “saddling” police power to search in such a way upon society. She 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.”

However, it is here where her solution crumbles. She characterizes the problem as a voluntary disclosure to a third party, as opposed to an involuntary gathering of data by business and becomes too narrowly focused on the Third Party Doctrine. She frames the digital reality of today as one in which information is “voluntarily disclosed” to the public for a limited purpose and concludes that such information should not be “disentitled to Fourth Amendment protection.” She goes onto frame the issue as one in which people “trade off privacy for convenience.” However, in the satellite imaging technology context as well as many other technologies people have not themselves voluntarily disclosed any such information to the public. They never made any choice to participate in such technology. They never had the opportunity to make such a “tradeoff” of losing privacy in exchange for other social gains. To the contrary, even their consent was 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 the users knowledge. Therefore, her solution of abandoning the third party

106 Id. at 956 (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (9th Cir. 2011) (Flaum, J., concurring)).
107 Id. (Sotomayor, J., concurring) (“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 ‘too permeating police surveillance’) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
108 Id. at 956 (Sotomayor, J., concurring).
109 Id. at 957 (Sotomayor, J., concurring).
110 Id. at 957 (Sotomayor, J., concurring).
111 Johnathan Mayer, Web Policy, February 17, 2012, available at webpolicy.org/20120/02/17/safari-trackers/; see also Google’s Circumvention of
doctrine is only partial. While it may address scenarios where the information is exchanged voluntarily, it does nothing when the information is obtained unknown to the citizen.

D. Justice Alito’s Retention of a Compromised Katz

Justice Alito asserts plainly that Katz avoids the problems of the Scalia approach. However, he acknowledges some weakness in the Katz approach. 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.

Again, here Justice Alito assumes there is a “tradeoff.” How that can be assumed is questionable in the satellite imaging technology or other data collection discussion. In many instances it can be assumed if there is an opportunity to demonstrate such an expectation, but the citizen chooses not to so do. 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. With the Library of Congress archiving all public tweets, the decision to engage in Twitter involves trading off some privacy. But increasingly citizens are having private data taken from them and assuming there is nothing they can do.

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 seem inadequate for this contemporary problem of a
loss of a *Katz* subjective expectation of privacy due to corporate conditioning. Justice Alito’s reluctant exploration of applying *Katz* would result in no expectation of privacy even in data exposed to the public without express consent of the citizen. In the satellite imaging context, this would mean the curtilage of the home.\textsuperscript{117} 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 being caused by corporate activity fails to sit well. There is something fundamental about Brandeis’ “right to be left alone.” It is honored when society decides a citizen loses said right when he demonstrates a willingness to sacrifice it. Ruling one loses this central right when a corporation 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 on *Katz*, so too could the technological development of satellite imaging or other similar technologies drive a new approach. However, tying a new test of reasonableness to technological advances is always problematic as the effectiveness of the new approach is likely outdated before the ink is dry. While this may have been manageable in 1967, today’s technology is changing so rapidly, the ability of the law to respond is questionable. Indeed, the Court noted as much in 2010, cautioning “[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology use before its role in society has become clear.”\textsuperscript{118}

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 trade off, but rather, of a situation in which “the public does not welcome the diminution of privacy that new technology entails, [but] they may eventually reconcile themselves to this development as inevitable.”\textsuperscript{119} Justice Alito compels the Congress to act, as it is “best situated to measure what society is willing to give up and what it is not.” Although such a statutory approach is plagued by the same problems as a new Fourth Amendment test: the rapidly 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 that private corporations are “conditioning” citizens’ expectations of privacy without input from the citizen. It is here where the Court has failed to correctly identify the issue and thus the solution. Justice Sotomayor is concerned with governmental

\textsuperscript{117} Although Justice Scalia governed five votes for his approach, this could be labeled the status quo. As Justice Scalia concedes, with data intrusions, there is often no physical trespass, so *Katz* would apply.

\textsuperscript{118} *Ontario v. Quon*, 08-1332, slip. op. at 10 (June 17, 2010).

“unrestrained power to assemble data.” She describes the data exposed by the citizen as “voluntarily disclosed to some member of the public for a limited purpose.” Justice Alito frames the issues as a “trade off” which also suggests a voluntary choice. However, in the satellite imaging technology model, as well as others, the disclosure of information is not voluntary as the citizen has been afforded no opportunity to opt out. No such option exists for satellite imaging technology, cloud computing, required electronic academic research, required online bill payment, etc. This is where Congress must focus.

The problem is really who owns one’s digital ‘dossier.’ Our current system of privacy protection accepts that the ‘digital dossier’ of a citizen is abandoned when possessed by a third party. Professor Solove coined “digital dossier” and Palfrey and Glasser expanded it to include “all the digital tracks one leaves to include photos, messages, but also data collected about a citizen with no affirmative consent.” The problem is, however, that current law does not take into account how that party accumulated that data. Specifically, the real issue is the obtaining of data by companies which do not give the individual a meaningful opportunity to consent to sharing the data, primarily or the secondarily sharing by the initial recipients. A legislative solution must focus on this problem.

Such legislation should focus on commercial services which collect information from digital dossiers and expose it to the public or others. In the satellite imaging context, this would mean companies that visually expose concealed private property. In the search engine world it includes a company like Google which records information about a user and sells it. Such business should not be allowed to condition the citizen that this 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, to include images of private property, when the citizen does not opt in to such disclosure.

While this may at first appear unprecedented there is a rich history and a future of such a response. Justice Alito all but called for legislative response to these technological abilities which are inexpensive and intrusive. He acknowledged the reality that people unhappy with technological change may indeed simply accept it, stated “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

120 Jones, 132 S.Ct. at 956 (Sotomayor, J., concurring).
121 Id. at 957 (Sotomayor, J., concurring).
122 Id. at 962. (Alito, J., concurring).
123 Palfrey and Glasser, Born Digital (2010).
125 Id. at 964 (Alito, J., concurring).
public safety in a comprehensive way.”

Historic precedent supports this approach. After Smith, Congress created laws which effectively required procedural review prior to monitoring dialed phone numbers. 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. More recently, the federal implementation of a “Do Not Call List” provides firmer ground for such a solution. Such legislation and regulation balances consumer protection with corporate rights. It also appears to be technically possible. For example, Google Earth has voluntarily complied with requests from governments to blur images for security reasons. After public outcry, Google Maps Street View agreed to blur depictions of people and license plates in its images. Similarly, several Internet companies have expressed support for weak regulations and have not raised technical objections.

There is compelling support for such an approach both abroad and more recently domestically. The most compelling 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 turning over of personal data and its significance to privacy, Europeans have taken a different position. Justice Sotomayor acknowledges the disclosure of personal data to third party corporations, but does not concede that such activity signals ambivalent citizens as to what is done with that data. The Europeans have combatted the invasion of privacy not by precluding its disclosure, but by increasing individual control over the data.

The European Union has taken a fundamentally different approach to privacy than in the United States. The Charter for Fundamental Rights of the European Union affords privacy protection a hallowed place, fundamental to the freedoms inherent in being human. Article 8 provides that “Everyone has the right to protection of personal data concerning him or her.” 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.” It further includes the right of access to any data collected. 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. Personal data includes, “any information relating to an individual, whether it relates to his or her private, professional, or public life.” However, the

126 Id. (Alito, J., concurring).
127 15 USC §6502.
128 15 USC 6151 et seq.
129 European Union Charter for Fundamental Rights, Article 8 (1).
130 Id. at Art. 8(2).
131 Id.
132 Id.
European Commission recognized the limits of this directive due to the reality that “[t]echnological progress and globalization have profoundly changed the way our data is collected” as well as that twenty-seven European Union member states had divergent rules meant implementing the measure and this causing confusion in the business community.\footnote{European Commission Press Releases 2P12/46 (January 25, 2012).}

Consequently, on January 25, 2012 the European Commission introduced several comprehensive reforms to its 1995 Data Protection Directive.\footnote{European Commission Press Releases 2P12/46 (January 25, 2012).} The reforms relevant to this article focus not on government use of data, but further upstream to both data collection as well as 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 citizen to own his own data, and the corresponding lack of right of commercial entities to take it without responsibility for the consequences.

The proposal is part of a three-fold regime; the first allows a minimum amount of data to be collected.\footnote{Art. 6 January 24, 2012 Directive.} The second demands an automatic setting of privacy controls to be the most private. This is known as "privacy by default."\footnote{European Union Preferred Option, EN at 2.} The third involves a concept of "data protection by design."\footnote{European Union Preferred Option, EN at 2.} 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.\footnote{Id. at Art. 7.} Notably, this consent would seem to need to be more than an agreement to a “terms of use” document. 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 citizen hostage by precluding the use of the service if no agreement to the privacy infringements. The reforms address this by stating “consent shall not provide a legal basis for the processing, where this is a significant imbalance between the position of the data subject and the controller.”\footnote{Id. at Art. 7 (4).}

Further, the individual does not lose her rights to her information once consent is given. Rather, she has the right to withdraw consent at any time.\footnote{Id. at Art 7 (3).} Even after made public, the individual retains a “right to be forgotten and to erasure.”\footnote{January 26, 2012, Directive Art 17.} This allows citizens the right to request their data be deleted and compels the Internet service to completely delete all personal data belonging to an individual and communicate that request to third parties.\footnote{European Union Preferred Option, EN at 2.} The rights of citizens include rights to transparent information, to information and access to data collected, rectification,
erasure, portability, to object profiling.  

More recently, the federal government has also moved closer to conceptualizing the need for more control over a citizen’s personal data. In February 2012, the White House announced a *Framework for Protecting Privacy and Promoting Innovation In the Global Digital Economy*. Here, the White House recognized “additional [privacy] protections are necessary.” This Framework contains a Consumer Privacy Bill of Rights which states: “Consumers have the right to exercise control over what personal data companies collect from them and how they use it.”

Additionally, the Bill of Rights includes the “right to expect companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.”

This proposal is a move in the right direction, however, they fall short. For example, these rights are to be developed into a code of conduct by the Commerce Department’s National Telecommunications and Information Administration. Unlike the European approach, this appears to be voluntary. Voluntary regimes have not been successful. For example, Google and other such companies change privacy policies with impunity. Recently, the Europeans also warned Google that the new policy “does not meet the requirements of the European Directive on Data Protection”, but to no avail. Additionally, the proposal is lacking specifics. As a technical matter, users today are given a choice not to track, but the choice is false. Consent must be meaningful. Consent cannot be meaningful if it is within the terms of service. By placing it there, the service is conditional on the consent. That is hardly a voluntary consent, but it is coercion. It is simply not a viable option if one cannot avail themselves of the service if they do not consent. While that may be appropriate for optional preferences, such as consenting to following the law with one’s email account, it is not reasonable to demand consent to disclose and sell personal information to unknown third parties in exchange for a needed service.

This concept of an opt-in provision has further support in the United States Congress. “Do Not Track” bills have been proposed in both the House and Senate. The Do Not Track Me Online Act proposed to have

144 January 24, 2012, Directive Ch. III.
145 Id. at 1.
146 Id. at 1.
147 Id. at 47, Appendix A: The Consumer Privacy Bill of Rights.
148 Id.
149 Google announced effective March 1 that it would change privacy policy to allow much increased tracking of information, leading to the Electronic Privacy Information Center filing a law suit that such action is in a violation of an October 2011 consent order in a previous lawsuit *EPIC v. FTC*.
150 Letter from Commission Nationale d’l’information et ces Libertes To Google, (February 27, 2012).
151 112 HR654 (2011); 112SR 913 (2011). A more narrow third bill targeting the prevention of tracking of information regarding minor children, the “Do Not Track Kids Act of 2011” was also proposed. 112 HR 1895.
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 “certain formation.”\footnote{152} However, it applies to limited entities whose primary business is collecting such information and covers only limited information, and carries an insignificant penalty.\footnote{153} 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 citizens to indicate “whether they prefer to have personal information collected.”\footnote{154} This vague proposal would seem to be complied with by use of the correct coercive terms of service agreements. Moreover, it seems to cover only the initial collection of information but not the subsequent use of it.

Nonetheless, 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 corporate grooming to eradicate the reasonable expectation of privacy by obtaining information and displaying it. It must have a meaningful opt-in provision which is not tied to the terms of service. Finally, it must incorporate concepts of data ownership of the citizen.

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

This legislation combined with current Fourth Amendment jurisprudence, would restore the balance. It does so by not only protecting privacy, it also provides the mechanism by which one can demonstrate one’s expectation of privacy. Thus, application of the \textit{Katz} test would be applicable because a court would have some way of determining of a person demonstrated his expectation.

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 citizens own their digital footprints, then when the government obtains this data it has “engag[ed] in physical intrusion of a constitutionally protected area in order to obtain information.”\footnote{155} As such, under \textit{Jones} a search has occurred. Such a marrying of concepts: ownership of digital information and a trespass based analysis may then provide the most comprehensive coverage. The landscape would be as follows. A citizen owns her digital footprint when it is information about herself.
papers, houses, or effect which she has demonstrated a desire to remain private by not actively disclosing it. A company may not condition her expectation of privacy. Rather, it 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 citizens no longer possess true subjective expectations of privacy due to an awareness of the ability to gather information about them 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 corporate conditioning. Instead, our legislative response should adopt a data ownership model for data exposed either through no action of the citizen or as collateral to the transaction. This model should require an opt in approach for its sharing and an ability to retrieve when desired. This ownership model works with our Fourth Amendment fundamental understandings. Thus the citizen has an option to demonstrate their privacy expectations and trigger Fourth Amendment protection.