



## Case Western Reserve Law Review

---

Volume 65 | Issue 2

---

2014

# Essay: Eight Nails into Katz's Coffin

Amitai Etzioni

Follow this and additional works at: <https://scholarlycommons.law.case.edu/caselrev>



Part of the [Law Commons](#)

---

### Recommended Citation

Amitai Etzioni, *Essay: Eight Nails into Katz's Coffin*, 65 Case W. Res. L. Rev. 413 (2014)

Available at: <https://scholarlycommons.law.case.edu/caselrev/vol65/iss2/6>

This Additional Piece is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Law Review by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

# EIGHT NAILS INTO *KATZ*'S COFFIN\*

*Amitai Etzioni*†

## ABSTRACT

From a social science viewpoint, that the United States courts keep drawing on *Katz v. United States*<sup>1</sup> in their rulings about whether or not privacy has been violated is difficult to comprehend. This legal case is clearly based on untenable sociological and psychological assumptions. Moreover, many fine legal scholars have laid out additional strong reasons that establish beyond a reasonable doubt that it is unreasonable to draw on “the reasonable expectations of privacy” as a legal concept. Continuing to draw on this concept, especially in the cyber age, undermines the legitimacy of the courts and hence of the law. This Article reviews these arguments in order to further nail down the lid on *Katz*'s coffin so that this case—and the privacy doctrine that draws on it—will be allowed to rest in peace.

## CONTENTS

I. <i>KATZ</i> IS TAUTOLOGICAL.....	413
II. <i>KATZ</i> IS SUBJECT TO INSTITUTIONAL INFLUENCE.....	415
III. SURVEYS TO THE RESCUE?.....	416
IV. EXPECTATION OR RIGHT?.....	419
V. TWO PRONGS OFFER LESS PROTECTION THAN ONE.....	420
VI. <i>KATZ</i> IS CONFRONTED BY THE CYBER AGE.....	421
VII. <i>KATZ</i> IS UNDERCUT BY THE THIRD PARTY DOCTRINE.....	423
VIII. <i>KATZ</i> STAYS HOME.....	424

## I. *KATZ* IS TAUTOLOGICAL

The Fourth Amendment “reasonable expectation of privacy” standard is tautological and circular. Both the individual and the societal expectations of privacy depend on judicial rulings—while judges, in turn, use these expectations as the basis for their rulings. Mr. *Katz* had no reason to assume a conversation he conducted in a public phone booth would be considered private or not—until the

---

\* I am indebted to Rory Donnelly for research assistance on this Article.

† University Professor and Director of the Institute for Communitarian Policy Studies at The George Washington University; Ph.D. in Sociology from the University of California Berkeley; former President of the American Sociological Association; and founder of the Communitarian Network.

1. 389 U.S. 347 (1967).

court ruled that he had such an expectation.<sup>2</sup> In other words, when the court holds that it heeds the *vox populi*, it actually follows the echo of its own voice. Several leading legal scholars find *Katz's* tautological nature highly problematic. Richard Posner, for example, notes that “it is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is.”<sup>3</sup> Richard A. Epstein maintains this:

It is all too easy to say that one is entitled to privacy because one has the expectation of getting it. But the focus on the subjective expectations of one party to a transaction does not explain or justify any legal rule, given the evident danger of circularity in reasoning.<sup>4</sup>

Anthony G. Amsterdam points out that the “actual, subjective expectation of privacy . . . can neither add to, nor can its absence detract from, an individual’s claim to fourth amendment protection.”<sup>5</sup> As Professor Amsterdam notes, “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 surveillance.”<sup>6</sup>

Jed Rubinfeld adds wisely that if expectations of privacy are “tied to what a citizen ought to know about the [law], Fourth Amendment law becomes a self-validating logical circle in which . . . any judicial decision will vindicate reasonable expectations of privacy (because the judicial decision will itself warrant the expectations or lack of expectations it announces).”<sup>7</sup> By this logic, he concludes, a totalitarian society with government informants in every workplace and household would satisfy the current interpretation of the Fourth Amendment.<sup>8</sup>

Richard Seamon extends this criticism, arguing that a “reasonable expectations” test that concludes certain government privacy intrusions do not count as searches “for Fourth Amendment

---

2. *Id.* at 351–53.

3. Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188.

4. RICHARD A. EPSTEIN, *PRINCIPLES FOR A FREE SOCIETY: RECONCILING INDIVIDUAL LIBERTY WITH THE COMMON GOOD* 210 (1998).

5. Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974).

6. *Id.*

7. Jed Rubinfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 115 (2008).

8. *Id.* at 134.

purposes” is “not just circular” but causes a “downward spiral” in which restrictions on searches and seizures are reduced over time by virtue of the Court’s semantics, thereby undermining the “purpose of the Fourth Amendment’s guarantee against unreasonable searches.”<sup>9</sup> According to Seamon, the reasoning used by the Court in *Kyllo v. United States*<sup>10</sup> demonstrates that the justices are aware of and struggling to deal with this dilemma.<sup>11</sup> The majority admitted that “[t]he *Katz* test—whether the individual has an expectation of privacy that society is prepared to recognize as reasonable—has often been criticized as *circular, and hence subjective* and unpredictable.”<sup>12</sup>

It is difficult to comprehend why the well-established observation that *Katz* is tautological is not itself sufficient to lay *Katz* to rest. Nevertheless, this Article provides several other reasons for ending the *Katz* standard.

## II. KATZ IS SUBJECT TO INSTITUTIONAL INFLUENCE

The reasonable expectation of privacy standard is not only highly malleable by the courts but also is subject to influence by various institutions. Statements made by elected officials, especially the President; laws enacted by Congress; and normative positions developed by religious authorities and public intellectuals all affect what people consider private or an open book.

Along these lines, Shaun Spencer points out that the “expectation-driven conception of privacy” facilitates the erosion of privacy overall by “large institutional actors.”<sup>13</sup> That is because powerful institutions can influence the social practices that affect the expectations of privacy “by changing their own conduct or practices, by changing or designing technology to affect privacy, or by

- 
9. Richard H. Seamon, *Kyllo v. United States and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013, 1023–24 (2001).
  10. 533 U.S. 27 (2001).
  11. See Seamon, *supra* note 9, at 1023 (“I believe that the *Kyllo* majority avoided the *Katz* test to avoid the [circular] problem that is so well illustrated by its application to the facts of *Kyllo*.”).
  12. *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (emphasis added).
  13. Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843, 844 (2002); see also Marissa A. Lalli, Note, *Spicy Little Conversations: Technology in the Workplace and a Call for a New Cross-Doctrinal Jurisprudence*, 48 AM. CRIM. L. REV. 243, 245 (2011) (arguing that given the “growing popularity of employer-provided personal communication devices” of ambiguous shared ownership between employee and employer, the “expectation of privacy” standard undermines the protection of individuals from unreasonable search and seizure by institutions).

implementing laws that affect society's expectation of privacy."<sup>14</sup> When employers monitor their employees' computer use, for example, they "diminish the expectation of privacy in the workplace," and when "merchants routinely sell consumers' personal data, they diminish the expectation of privacy in one's transactional information."<sup>15</sup>

Jed Rubinfeld shows that the reasonable expectation of privacy test would allow a simple government announcement that "all telephone calls will henceforth be monitored" to deprive people of their "reasonable expectations of privacy in such calls," retroactively justifying the decree.<sup>16</sup> Put simply by Erwin Chemerinsky, the government "seemingly can deny privacy just by letting people know in advance not to expect any."<sup>17</sup> Richard Julie adds importantly that the ability of legislation and regulation to affect the scope of the Fourth Amendment in this way violates "the core principle of constitutional law, that the legislature may not alter the Constitution by an ordinary statute."<sup>18</sup>

Thus, the public's "reasonable expectations" may be altered by any number of factors. The fact that the *vox populi* is affected not only by the courts but also by myriad other institutions hardly makes it a more reliable, trustworthy or independent criterion for determining a reasonable expectation of privacy.

### III. SURVEYS TO THE RESCUE?

Assuming judges try to live up to the standard they have set and seek to figure out what reasonable people consider private beyond looking into their own innards, to whom should they turn? There are more than three hundred million Americans. Even if one excludes minors and others whose opinion, for one reason or another, the law excludes, a very hefty number remains. There is no reason, and even less evidence, to hold that they all will have the same expectations.

---

14. Spencer, *supra* note 13, at 860.

15. *Id.*

16. Rubinfeld, *supra* note 7, at 132–33.

17. Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 650 (2007); see also Raquel Aldana, *Of Katz and "Aliens": Privacy Expectations and the Immigration Raids*, 41 U.C. DAVIS L. REV. 1081, 1089 (2008) (arguing that "immigrants have become so regulated that any *Katz* expectation of privacy [for immigrants] to occupy spaces in silence without detection becomes unreasonable").

18. Richard S. Julie, Note, *High-Tech Surveillance Tools and the Fourth Amendment: Reasonable Expectations of Privacy in the Technological Age*, 37 AM. CRIM. L. REV. 127, 132 (2000) (citing *Marbury v. Madison*, 5 U.S. 137, 177 (1803)).

Some have suggested that using opinion surveys could make the reasonable expectation of privacy test less circular and subjective by actually finding out what people believe.<sup>19</sup> Christopher Slobogin and Joseph Schumacher, for example, have suggested that the Supreme Court should factor empirical sources such as opinion surveys into the *Katz* test.<sup>20</sup> Henry Fradella et al. likewise hold that survey data would provide “a far richer and more accurate” basis for determining whether an expectation of privacy is “objectively reasonable.”<sup>21</sup>

Actually, social scientists tend to agree that such surveys may not provide a reliable and appropriate tool on which the courts can rely. Survey results vary depending on (a) who is surveyed, (b) the ways the questions are worded, (c) the sequence in which the questions are asked, (d) the context in which they are asked (e.g., at home versus at work), and (e) the attributes of those who ask the questions. Even when the same question is asked of the same people by the same people twice, rather different answers can follow.<sup>22</sup> These inherent problems are magnified when one seeks opinions about complicated, abstract issues like “privacy” and “surveillance.”<sup>23</sup>

People tend to give answers they believe are expected of them, especially regarding issues that are politically or ideologically divisive. Respondents tend to exaggerate their income, popularity, happiness, and political engagement.<sup>24</sup> Merely changing the phrasing of a

19. This view relies in part on Justice Rehnquist’s statement that “[l]egitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.” *Rakas v. Illinois*, 439 U.S. 128, 144 n.12 (1978). Empirical data would be used to shed light on the latter.
20. Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at “Understandings Recognized and Permitted by Society,”* 42 DUKE L.J. 727, 757–58 (1993).
21. Henry F. Fradella et al., *Quantifying Katz: Empirically Measuring “Reasonable Expectations of Privacy” in the Fourth Amendment Context*, 38 AM. J. CRIM. L. 289, 294 (2011).
22. See Inst. for Statistics Educ., *Glossary of Statistical Terms: Test-Retest Reliability*, STATISTICS.COM, [http://www.statistics.com/glossary&term\\_id=867](http://www.statistics.com/glossary&term_id=867) (last visited Oct. 22, 2014) (discussing the concept of test-retest reliability in surveys).
23. See, e.g., Oscar H. Gandy Jr., *Public Opinion Surveys and the Formation of Privacy Policy*, 59 J. SOC. ISSUES 283, 284 (2003) (explaining that the difficulty of framing neutral questions is “especially problematic in the realm of privacy policy”); Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 23 (stating that questions on privacy might be “too complicated and too easily skewed” to give accurate results).
24. See Ruut Veenhoven, *Why Social Policy Needs Subjective Indicators*, 58 SOC. INDICATORS RES. 33, 40 (2002) (“[R]esponses may be distorted in

question yields rather different results. A 2003 poll, for example, found that a strong majority (68%) of Americans favored invading Iraq, but this number fell to a minority (43%) if the possibility of U.S. military casualties was mentioned in the question.<sup>25</sup> Along the same lines, a medical study found that patients were almost twice as likely to reject surgery when the predicted outcome was phrased in terms of “mortality rate” rather than “survival rate.”<sup>26</sup> These issues present formidable obstacles to determining what the American people actually expect.<sup>27</sup> Although social scientists have developed ways to mitigate these issues,<sup>28</sup> the technological transition from landlines to

---

a systematic way, such as by a tendency for respondents to conform to social desirability.”).

25. *Question Wording*, PEW RES. CENTER FOR THE PEOPLE & THE PRESS, <http://www.people-press.org/methodology/questionnaire-design/question-wording/> (last visited Oct. 26, 2014). Examples of such bias include “social desirability bias,” in which people give “inaccurate answers to questions that deal with sensitive subjects” like drug use or church attendance, especially in face-to-face interviews; “acquiescence bias,” illustrated by a poll that found when people were asked whether military strength was the best way to secure peace, 55 percent were in favor when phrased as a “yes or no” question, but only 33 percent were in favor when “diplomacy” was offered as an alternative; and question order effects, demonstrated by a 2008 poll that found that an additional 10 percent of respondents expressed dissatisfaction with current affairs if they were previously, rather than subsequently, asked if they approved of the President’s performance. *Id.* See also Andrew R. Binder et al., *Measuring Risk/Benefit Perceptions of Emerging Technologies and Their Potential Impact on Communication of Public Opinion Toward Science*, 21 PUB. UNDERSTANDING SCI. 830, 832–33 (2012) (suggesting that short opinion polls may yield different results than longer academic surveys).
26. Barbara J. McNeil et al., *On the Elicitation of Preferences for Alternative Therapies*, 306 NEW ENG. J. MED. 1259, 1261 (1982).
27. The archetypal example of survey error leading to false results was the famous “Literary Digest poll” that falsely predicted Roosevelt’s loss of the 1936 presidential election results by relying solely on telephone and car owners, a disproportionately Republican group. See also Elizabeth Mehren, *The War Over Love Heats Up Again: Author Shere Hite’s Third Report on Sexuality Fuels an Old Debate Over Her Methodology*, L.A. TIMES, Oct. 29, 1987 (discussing that while a 1987 mail-in survey on love found that 98% of women were unhappy in their relationships, a telephone poll found that 93% were happy, and suggesting this was possibly because the unhappy had more motivation to mail in their responses); Russell D. Renka, *The Good, the Bad, and the Ugly of Public Opinion Polls* (Feb. 22, 2010), available at [http://cstl-cla.semo.edu/rdrenka/Renka\\_papers/polls.htm](http://cstl-cla.semo.edu/rdrenka/Renka_papers/polls.htm) (discussing the idea that Internet polls, which tend to attract an unrepresentative sample of the population and to lack safeguards against multiple voting, can be particularly susceptible to these types of errors).

cell phones and e-mail, coupled with the declining response rate to polls, has made accurate polling increasingly difficult.<sup>29</sup>

Particularly problematic is defining which “society” the Court has in mind when it seeks to determine the societal expectation of privacy.<sup>30</sup> Simply put, *whose* reasonable expectation matters? Katz’s peers? The members of his gambling community? Or the people of the United States of America?

#### IV. EXPECTATION OR RIGHT?

Drawing on the societal expectation of privacy in effect amounts to drawing on consensus. This raises a preliminary question: how much agreement is needed to qualify as “societal” expectation? Total consensus is not found in any society of complexity, even in ones much smaller than the United States. Is an 80 percent agreement enough? A two-thirds majority?

Much more important is the question of whether the courts should be guided by consensus even when it can be accurately determined. True, consensus has a prudential value. The courts should not stray too far from public consensus, lest they lose their legitimacy or stray into a bitter culture war of the kind that occurred around reproductive rights (i.e., decisional privacy). However, consensus has no standing from a normative viewpoint when fundamental rights are at stake. Thus, if an overwhelming majority of Americans agrees that women are second-class citizens or that “fishing expeditions” by the police are fully acceptable because “those who did nothing wrong have nothing to hide,” this does not mean that a court should accept this consensus and allow it to trump the court’s judgment as to what the Constitution entails and what is just and right. In short, from a normative viewpoint, the expectation of the public as to what and who may or may not be searched should matter little.

Because this point is crucial, an elaboration follows. *Katz* runs roughshod over the elementary but essential fact that the political system of the United States is not a simple democracy but a liberal democracy.<sup>31</sup> The essence of this regime is that it combines two very distinct principles. The first is majoritarianism: when we differ, we choose our course based on which position garners more votes. The

---

28. See, e.g., FLOYD J. FOWLER JR., *SURVEY RESEARCH METHODS* 49–55 (5th ed. 2014).

29. Jason Zengerle, *The Polls Have Stopped Making Any Sense.*, N.Y. MAG., Sept. 30, 2012; Thomas Fitzgerald, *Rethinking Public Opinion*, NEW ATLANTIS, Summer 2008, at 45, 60.

30. Spencer, *supra* note 13, at 847–51.

31. Others call it a “republic”; I would prefer a “constitutional democracy.”



second is liberalism: a set of rights are deliberately ensconced in the Constitution, making them so difficult to amend that one should usually take them as a given. To put it differently, the majority can decide what it prefers as long as this preference does not entail violating anybody's rights to speak freely, to worship, to assemble, to petition, and so on. The right to privacy is one of these rights. Therefore, if the courts were to decide whether a particular situation is covered by the right to privacy based on what the masses told a pollster or what the courts somehow determine the societal view to be—the courts would in effect turn a fundamental right into a mass-driven, pliable, ephemeral, ever-changing concept.

Thus, Americans showed very little concern for privacy in the months that followed the September 11th attacks on America and much more concern when no new major attacks took place over the next ten years.<sup>32</sup> They are sure to change their collective mind one more time if another attack occurs. If one bases a constitutional right on such a foundation, one might as well tie it to a weather vane. In short, if *Katz* is allowed to stand and the courts continue to follow it, the result would be to reduce the right of privacy at best to a mere matter of democratic majority rule.

I write “at best” because *Katz* is not more aligned with the democratic half of the United States regime than it is with the liberal/constitutional half. In deciding those public policy issues that are not covered by rights and are subject to majority rule, the United States counts noses. That is, each person has a vote—whether or not they are reasonable. *Katz* is decided without any actual votes by the public; the people's views are merely divined.

In short, *Katz* is either a convenient fiction or a serious violation of the most basic principles of our polity and should be allowed to expire, the sooner the better.

## V. TWO PRONGS OFFER LESS PROTECTION THAN ONE

Originally, the *Katz* test consisted of two “prongs” used jointly to determine whether a “reasonable expectation of privacy” existed.<sup>33</sup> In the words of Justice Harlan, “[T]here is 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.’”<sup>34</sup> Of course, such a dual standard raises this question: what is a court to do when the two standards are in conflict? If the courts ignore the first standard on the

---

32. AMITAI ETZIONI, HOW PATRIOTIC IS THE PATRIOT ACT?: FREEDOM VERSUS SECURITY IN THE AGE OF TERRORISM 14 (2004).

33. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

34. *Id.*

grounds that every defendant will claim an expectation of privacy in the matter at hand—why introduce two prongs in the first place? In practice, courts have increasingly ignored the first prong as a “practical matter,” for “defendants virtually always claim to have a subjective expectation of privacy” and such claims are difficult to disprove.<sup>35</sup> Thus, David Cunis notes that “[t]he Court in [*California v. Greenwood*, as in [*California v. Ciraolo*, *Oliver v. United States*], and [*Maryland v. Smith* . . . summarily dismissed the first prong of the *Katz* test.”<sup>36</sup> Thus, the expectation of privacy test relies almost exclusively on an objective determination of society’s “reasonable” expectations. Among all *Katz*’s flaws, this two-pronged approach is a relatively minor one; it merely adds one more reason to allow this legal concept to fade away. After all, if half the prongs of the *Katz* test are irrelevant, there is no compelling reason to continue following it.

## VI. KATZ IS CONFRONTED BY THE CYBER AGE

The reasonable expectation of privacy standard is further undermined by recent technological developments. The rise of social media, Facebook in particular, is a prime example of this trend. Originally intended and promoted as a social networking tool for college students, Facebook’s privacy implications have expanded in line with its broadening user base and functionality. There are numerous documented instances of employees being fired over material they, not expecting to share it with their employer, had posted on Facebook.<sup>37</sup> A 2012 survey found that more than a third of employers use Facebook and similar sites to screen candidates,<sup>38</sup> while 70 percent of business managers admitted ruling out candidates based

- 
35. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 933 n.35 (2005) (discussing the lack of attention courts have given to the first prong of *Katz*).
36. David W. Cunis, Note, *California v. Greenwood: Discarding the Traditional Approach to the Search and Seizure of Garbage*, 38 CATH. U. L. REV. 543, 565 (1989).
37. *E.g.*, *Patriots Cheerleader Fired After Facebook Swastika Photo*, FOX NEWS (Nov. 6, 2008), <http://www.foxnews.com/story/2008/11/06/patriots-cheerleader-fired-after-facebook-swastika-photo/>; Bloomberg News, *Facebook Chat Gets 13 Virgin Airlines Employees Fired*, N.Y. DAILY NEWS (Nov. 1, 2008, 8:12 PM), <http://www.nydailynews.com/news/money/facebook-chat-13-virgin-airlines-employees-fired-article-1.335199>.
38. *Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey*, CAREERBUILDER (Apr. 18, 2012), <http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr691&sd=4%2f18%2f2012&ed=4%2f18%2f2099>.

on information found online.<sup>39</sup> Although such evaluations are typically done through Internet searches or mutual friends, in some cases employers and universities demand Facebook passwords from current or prospective employees and students, a practice that, despite controversy, remains legal in the majority of United States.<sup>40</sup> On the other hand, evading this scrutiny by restricting access to or removing personal information from Facebook may also hurt one's job prospects.<sup>41</sup> In addition, Facebook is monitored by intelligence<sup>42</sup> and law enforcement agencies.<sup>43</sup>

Following *California v. Greenwood*,<sup>44</sup> in which the Supreme Court determined that material left outdoors in trash bags was accessible to the public and thus could not reasonably be expected to be private,<sup>45</sup> the Supreme Court has tended to find it reasonable to expect privacy only in acts or spaces unobservable to the general public.<sup>46</sup> As shown by Facebook, however, the evolution and mass adoption of new communications and other technologies tends over time to increase the public visibility of acts people consider private. The Supreme Court has in effect held in recent rulings such as *Dow Chemical Co. v. United States*<sup>47</sup> that "the effect of modern life, with its technological and other advances, serves to eliminate or reduce a person's justified expectation of privacy."<sup>48</sup> Along these lines, Helen Nissenbaum notes

- 
39. Laura Vanderkam, *How Social Media Can Affect Your Job Search*, CNN (Oct. 9, 2012, 9:56 AM) <http://www.cnn.com/2012/10/09/living/real-simple-social-media-job/index.html>.
  40. Jonathan Dame, *Will Employers Still Ask for Facebook Passwords in 2014?*, USA TODAY (Jan. 10, 2014, 2:03 AM), <http://www.usatoday.com/story/money/business/2014/01/10/facebook-passwords-employers/4327739/>.
  41. Jade Pech, *Social Networking Sites and Selection Decisions: The Impact of Privacy Settings of Facebook Profiles on Hiring* (June 11, 2013) (unpublished M.A. thesis, University of Central Oklahoma), available at UMI Dissertation Publishing 1543734.
  42. Kimberly Dozier, *AP Exclusive: CIA following Twitter, Facebook*, EL PASO TIMES (Jan. 4, 2011, 9:45 AM), [http://www.elpasotimes.com/newupdated/ci\\_19264270](http://www.elpasotimes.com/newupdated/ci_19264270).
  43. Sean Gallagher, *Staking Out Twitter and Facebook, New Service Lets Police Poke Perps*, ARS TECHNICA (Nov. 13, 2013, 6:25 PM), <http://ars.technica.com/information-technology/2013/11/staking-out-twitter-and-facebook-new-service-lets-police-poke-perps/>.
  44. 486 U.S. 35 (1988).
  45. *Id.* at 40.
  46. See Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 316–20 (1998).
  47. 476 U.S. 227 (1986).
  48. Clancy, *supra* note 46, at 335.

that the “expectation of privacy” test prevents the Court from ruling against the increasingly prominent practices of public surveillance, which include searching online public records, consumer profiling, data mining, and the use of location technologies such as radio frequency identification (RFID). This is because the test defines movement or activity in public arenas as “implicitly” abandoning “any expectation of privacy.”<sup>49</sup> Nissenbaum views this as evidence that “traditional theoretical insights” yield unsatisfactory conclusions in the case of public surveillance.<sup>50</sup>

## VII. KATZ IS UNDERCUT BY THE THIRD PARTY DOCTRINE

*Katz* is further damaged by the combination of recent technological developments with the “third party doctrine.” As stated in *United States v. Miller*,<sup>51</sup> this doctrine asserts that the “Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities” and that “issuance of a subpoena to a third party does not violate the rights of a defendant.”<sup>52</sup> While originally justifying the police subpoena of a suspect’s bank records, the third party doctrine has since become a serious impediment to Fourth Amendment restrictions on new surveillance technologies due to the essential role third parties play over the Internet. As a result, argues Stephen Henderson, the “reasonable expectation of privacy” test in its current form threatens to “render the Fourth Amendment a practical nullity.”<sup>53</sup> Whereas the Fourth Amendment requires a warrant for surveillance of personal paper mail, for example, the third party doctrine leaves e-mail without similar protection.<sup>54</sup> This impelled Congress to legislate protection for e-mail with the 1986 Stored Communications Act,<sup>55</sup> but

---

49. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 135 (2004).

50. *Id.* at 119.

51. 425 U.S. 435 (1976).

52. *Id.* at 443, 444.

53. Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 510 (2005).

54. *See Frequently Asked Questions*, U.S. POSTAL INSPECTION SERVICE, <https://postalinspectors.uspis.gov/contactUs/faq.aspx> (last visited Oct. 19, 2014) (“First-Class letters and parcels . . . cannot be opened without a search warrant.”).

55. 18 U.S.C. §§ 2701–2711 (2006).

advances in technology quickly rendered that law obsolete.<sup>56</sup> Likewise, Peter Swire warns that increasing use of the Internet, and thus third parties, to conduct phone calls may render the “expectation of privacy” test ineffective even for phone call wiretapping—the original subject of the *Katz* ruling.<sup>57</sup> In today’s era of “big data,” which Craig Mundie points out is characterized by the “widespread and perpetual collection and storage” of personal information by third parties<sup>58</sup> and in which individuals and businesses increasingly store information “in the cloud” rather than on their own devices, a traditional privacy paradigm based on secrecy is no longer relevant or useful. Several Supreme Court justices have acknowledged this flaw in *Katz* jurisprudence.<sup>59</sup>

### VIII. KATZ STAYS HOME

*Katz* will be mourned much less than one might have expected given the excitement with which its arrival was greeted. At the time, *Katz* was said to be a “revolution”<sup>60</sup> and a “watershed in [F]ourth [A]mendment jurisprudence,”<sup>61</sup> and consensus quickly emerged that it was a “landmark decision that dramatically changed Fourth Amendment law.”<sup>62</sup> This was, at least in part, because prior to *Katz* the boundary between that which was private (in the Fourth Amendment sense, requiring a warrant to be searched) and that which was not was largely based on the legal concept that one’s home

- 
56. Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004).
57. Peter P. Swire, *Katz Is Dead. Long Live Katz.*, 102 MICH. L. REV. 904, 910–12 (2004).
58. Craig Mundie, *Privacy Pragmatism: Focus on Data Use, Not Data Collection*, FOREIGN AFF., March/April 2014, at 28, 28.
59. See, e.g., *Smith v. Maryland*, 442 U.S. 735, 750 (1979) (Marshall, J., dissenting) (arguing that “unless a person is prepared to forgo . . . personal or professional necessity, he cannot help but accept the risk of surveillance [by third parties],” which is of less relevance to privacy than “the risks he should be forced to assume in a free and open society”); see also *United States v. Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (arguing that the third party doctrine is “ill suited to the digital age”).
60. James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 649 (1985); Richard G. Wilkins, *Defining the “Reasonable Expectation of Privacy”: An Emerging Tripartite Analysis*, 40 VAND. L. REV. 1077, 1087 (1987).
61. Amsterdam, *supra* note 5, at 382.
62. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 820 (2004).

was one's castle, while that which was out in public was fair game for the state. (This notion was explicated in the third party doctrine.) *Katz* was held to have redefined this boundary such that, in the words of the majority opinion of the Court, that which a person "seeks to preserve as private, even in an area accessible to the public," is protected by the Fourth Amendment, whereas that which "a person knowingly exposes to the public, even in his own home or office, is not."<sup>63</sup> Yet the assertion that "the Fourth Amendment protects people, not places" did not create the expected privacy bubble that accompanies a person wherever she or he went.<sup>64</sup> In an important qualification, Justice Harlan noted from the onset that "what protection [the Fourth Amendment] affords to those people . . . requires reference to a 'place.'"<sup>65</sup>

Most importantly, as *Katz* was used as a precedent in case after case that followed, time and time again the courts recognized a reasonable expectation of privacy when the intrusions concerned the home—but not when the person or their communications were in public spaces, in effect reintroducing the property-based definition of privacy through a back door! As Daniel Pesciotta points out, the Supreme Court used *Katz* to maintain "steadfast support of citizens' privacy rights in the most private of all places—the home."<sup>66</sup> In the *Katz* ruling itself, the argument that *Katz* had a reasonable expectation of privacy in a phone booth hinged on the fact that he "occupie[d]" the phone booth and "[shut] the door behind him."<sup>67</sup> According to Justice Harlan, this made the phone booth a "temporarily private place," raising an implicit comparison to the only permanently private place: the home.<sup>68</sup> In *United States v. Karo*,<sup>69</sup> the Court justified denying the use of a tracking device within a house on the "basic Fourth Amendment principle" that "private residences are places in which the individual normally expects privacy."<sup>70</sup>

Justice Scalia's majority opinion in *Kyllo v. United States*,<sup>71</sup> which denied the use of infrared technology to evaluate the contents of a house, made the case for a return to the home even more strongly.

---

63. *Katz v. United States*, 389 U.S. 347, 351–52 (1967).

64. *Id.* at 351.

65. *Id.* at 361 (Harlan, J., concurring).

66. Daniel T. Pesciotta, Note, *I'm Not Dead Yet: Katz, Jones, and the Fourth Amendment in the 21st Century*, 63 CASE W. RES. L. REV. 187, 243 (2012).

67. *Katz*, 389 U.S. at 352 (majority opinion).

68. *Id.* at 361 (Harlan, J., concurring).

69. 468 U.S. 705 (1984).

70. *Id.* at 714.

71. 533 U.S. 27 (2001).

Justice Scalia stated that the “right of a man to retreat into his own home and there be free from unreasonable governmental intrusion” forms “the very core”<sup>72</sup> of the Fourth Amendment, which “draws a firm line at the entrance of the house”<sup>73</sup> based on “roots deep in the common law” that reveal the “minimal expectation of privacy.”<sup>74</sup>

In the same post-*Katz* period, cases dealing with surveillance technology outside the home have rarely favored privacy interests. Such cases include *Smith v. Maryland*,<sup>75</sup> which held there was no “expectation of privacy” for lists of phone numbers dialed;<sup>76</sup> *United States v. Knotts*,<sup>77</sup> which allowed the use of a tracking device in public;<sup>78</sup> and *California v. Ciraolo*<sup>79</sup> and *Dow Chemical Co. v. United States*,<sup>80</sup> which allowed aerial surveillance of a backyard<sup>81</sup> and a chemical plant,<sup>82</sup> respectively.

Some legal scholars find some support for the transformative view of *Katz* in the Supreme Court’s 2012 ruling in *United States v. Jones*,<sup>83</sup> the first Fourth Amendment technology case in a decade.<sup>84</sup> They cite this case as revealing *Katz*’s potential to reconcile technology and privacy by protecting “a defendant’s Fourth Amendment rights in his public movements.”<sup>85</sup> However, the majority in *Jones* held that a GPS device surreptitiously attached to a suspect’s vehicle violated his privacy rights based on the pre-*Katz*<sup>86</sup> “property-based approach” of a “common-law trespassory test” rather than the “reasonable expectation of privacy” test.<sup>87</sup>

---

72. *Id.* at 31 (quoting *Silverman v. United States*, 365 U.S. 505, 511 (1961)).

73. *Id.* at 40 (quoting *Payton v. New York*, 445 U.S. 573, 590 (1980)).

74. *Id.* at 34.

75. 442 U.S. 735 (1979).

76. *Id.* at 742.

77. 460 U.S. 276 (1983).

78. *Id.* at 285.

79. 476 U.S. 207 (1986).

80. 476 U.S. 227 (1986).

81. *Ciraolo*, 476 U.S. at 214.

82. *Dow Chem. Co.*, 476 U.S. at 232.

83. 132 S. Ct. 945 (2012).

84. *E.g.*, Pesciotta, *supra* note 66, at 230 (noting that the Court took a “more than ten-year hiatus from deciding a Fourth Amendment case involving technology”).

85. *Id.* at 244.

86. *Id.* at 210 (citing *Jones*, 132 S. Ct. at 950–52).

87. *Id.*; Sherry F. Colb, *The Supreme Court Decides the GPS Case*, *United States v. Jones, and the Fourth Amendment Evolves: Part One in a*

In fact, a close reading of the *Jones* ruling reveals that the Court agreed on the drawbacks of the “reasonable expectations” test. Justice Alito’s concurrence, backed by three other justices, spends several paragraphs discussing *Katz*’s flaws, including its “circularity,” its subjectivity, and especially the erosion of privacy expectations in the face of technology.<sup>88</sup> Justice Sotomayor’s own concurrence goes even further, taking the opportunity to criticize the third-party doctrine as “ill suited to the digital age” despite the lack of third parties in the actual case at hand.<sup>89</sup> Justice Scalia’s majority opinion sidesteps these issues by resurrecting the property-based standard and treating the vehicle in question as akin to a home because trespassing, a term usually used for homes, and here applied to a person’s car, was involved.<sup>90</sup> Alito’s concurrence criticizes Scalia’s application of “18th-century tort law” as unsuited to “21st-century surveillance,” pointing out the ruling’s “[d]isharmony with a substantial body of existing case law,” emphasis on the “trivial” matter of a physical device rather than the central issue of privacy, and irrelevance to non-physically intrusive electronic surveillance.<sup>91</sup> Scalia responds to this criticism by warning that relying “exclusively” on *Katz* “eliminates rights that previously existed.”<sup>92</sup>

The issue stands out if one puts aside for a moment the language of legal discourse, going beyond “this court stated” vs. “this court ruled,” and examines it in layperson’s terms. Compare two situations: In the first, the government suspects that a person is illegally growing marijuana in his home, but the suspicion does not rise to the level that would convince a judge to grant a warrant. How much violation of privacy occurs if the government uses a thermal device to find out the temperature in that home’s den—and it turns out that the person was innocent, cooking nothing more than dinner? Or consider a police dog trained to detect bombs and contraband that approaches the home from a side most visitors do not. The Court has ruled that both cases are intrusions on the home and thus violate a reasonable expectation of privacy. Now, compare these to a situation in which cameras follow a person every place they go in public, all day and all night—to bars, clinics, Alcoholics Anonymous sessions, political meetings, rendezvous with a lover—and collect and analyze all this

---

*Two-Part Series of Columns*, JUSTIA (Feb. 28, 2012), <http://verdict.justia.com/2012/02/08/the-supreme-court-decides-the-gps-case-united-states-v-jones-and-the-fourth-amendment-evolves>.

88. *Jones*, 132 S. Ct. at 962 (Alito, J., concurring).

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

90. *Id.* at 949–50 (majority opinion).

91. *Id.* at 961 (Alito, J., concurring).

92. *Id.* at 953 (majority opinion).



information to make it available to the government. Such systems are not science fiction but rather are an increasing reality in major U.S. cities; notable examples include Persistent Security Systems<sup>93</sup> and Microsoft's Domain Awareness System.<sup>94</sup> Or consider the use of parabolic microphones to eavesdrop on private conversations in a public area such as a park. If one accepts the principle that some privacy should exist even in public areas, these modes of surveillance represent much broader, deeper, and more indiscriminate violations of privacy than the limited and situational intrusions of a drug-sniffing dog or an infrared scanner penetrating the home.

In short, *Katz* took the U.S. no more than, at best, a baby step toward privacy protection outside the home. It excessively privileges the home, while that which the U.S. needs is a doctrine of privacy that protects privacy in both realms against unreasonable search and seizure. A psychologist may argue that the legal community is holding on to *Katz* because it does not want to regress to the property-based, home-centered privacy doctrine—but in effect *Katz* does little to move the protection of privacy beyond the home's walls. The time has come to develop a cyber-age privacy doctrine that focuses on secondary use rather than on primary collection of personal information, a subject that deserves a separate treatment.<sup>95</sup>

- 
93. Craig Timberg, *High Above, an All-Seeing Eye Watches for Crime*, WASH. POST, Feb. 6, 2014, at A01 (stating that Persistent Security Systems uses airborne cameras to “track every vehicle and person across an area the size of a small city, for several hours at a time,” and explaining that [p]olice are supposed to begin looking at the pictures only after a crime has been reported”).
94. Press Release, N.Y.C., Mayor Bloomberg, Police Commissioner Kelly and Microsoft Unveil New, State-of-the-Art Law Enforcement Technology that Aggregates and Analyzes Existing Public Safety Data in Real Time to Provide a Comprehensive View of Potential Threats and Criminal Activity (Aug. 8, 2012). A joint effort of Microsoft and the New York Police Department “aggregates and analyzes existing public safety data streams” from cameras, license plate readers, radiation detectors, and law enforcement databases. *Id.* The technology helps police track suspects by providing arrest records, related 911 calls, local crime data, and vehicle locations. Material deemed to have “continuing law enforcement or public safety value or legal necessity” may be retained indefinitely; otherwise it is stored for up to five years. *Id.*; see also Martin Kaste, In “Domain Awareness,” Detractors See Another NSA, NPR (Feb. 21, 2014, 4:00 PM) <http://www.npr.org/blogs/alltechconsidered/2014/02/21/280749781/in-domain-awareness-detractors-see-another-nsa> (suggesting that expansion of the system to include additional cameras, facial recognition, cell phone and social media tracking is planned).
95. Amitai Etzioni, *A Cyber Age Privacy Doctrine: A Liberal Communitarian Approach*, 10 ISJLP 641 (2014).