Garbage Pails and Puppy Dog Tails: Is That What *Katz* is Made Of?

Aya Gruber[*]

This Article takes the opportunity of the fortieth anniversary of Katz v. U.S. *to assess whether the revolutionary case's potential to provide broad and flexible privacy protection to individuals has been realized. Answering this question in a circumspect way, the Article pinpoints the language in* Katz *that was its eventual undoing and demonstrates how the* Katz *test has been plagued by two principle problems that have often rendered it more harmful to than protective of privacy. The manipulation problem describes the tendency of conservative courts to define reasonable expectations of privacy as lower than the expectations society actually entertains. The normativity problem captures the idea that the* Katz *test allows reasonable expectations to be set by those who engage in normatively disfavored privacy defeating conduct. The Article then concentrates on two specific doctrines exemplary of these problems, the third party doctrine and the contraband exception, and discusses their ruinous effects on privacy in a technological era. The third party doctrine, which roughly holds that third party exposure defeats privacy interests, has severely hampered the ability of the* Katz *test to afford Fourth Amendment protection to intimate online communications. Likewise, the contraband exception, which holds that there is no legitimate expectation of privacy in illegal items, proves exceedingly dangerous to privacy as crime detection technology becomes increasingly refined. In the end, however, this Article does not advocate trashing the* Katz *test, but rather suggests methods of interpretation that remedy the manipulation and normativity problems.*

[*] Associate Professor of Law, Florida International University College of Law; Assistant Public Defender, Washington, D.C.; Assistant Federal Defender, S.D. Fla; J.D., Harvard Law School; B.A., UC Berkeley. I would like to thank all the participants in and organizers of the *Katz v. U.S.*: 40 Years Later Symposium, and especially Professor Jennifer Chacón of the UC Davis School of Law. I also praise the diligent editing of the UC Davis Law Review staff, and in particular Kristy Young.

TABLE OF CONTENTS

INTRODUCTION

There are two great temptations felt by scholars analyzing *Katz v. United States* and the "*Katz* test."[1] The first is to explore novel privacy issues by playing analogy "smackdown." For example, my Internet-provider-as-mail-carrier trumps your Internet-provider-as-bank-teller analogy. The second grand temptation is to reference *Katz* issues through the use of catchy double entendres. When criticizing the *Illinois v. Caballes* canine sniff decision, one is often inclined to say that *Katz* has "gone to the dogs."[2] There is also the critique that the *California v. Greenwood* garbage case "trashed" *Katz*.[3] One could even go so far as to say the pen register decision in *Smith v. Maryland* is "phony."[4] A perusal of the title of this Article surely reveals that I have already failed to resist one of these great temptations, although the rest of the paper is hopefully more than a game of choose-your-own-analogy. Indeed, *Katz* represents much more than a mere opportunity to engage in academic rumination and clever analogizing. On this fortieth anniversary of the revolutionary decision, it is important to consider *Katz*'s legacy over the years and determine whether, in an age of advanced technology, *Katz* proves to have nine lives.[5]

Katz was and is a revolution both as to the scope of individual privacy rights and constitutional interpretative methodology.[6] Until *Katz*, the U.S. Supreme Court tended toward a literal reading of the Fourth Amendment, limiting its protective ambit to "persons, houses, papers, and effects."[7] *Katz* not only broadened the operative applicability of the Fourth Amendment, it also served as an important departure from literalist constitutional interpretation. While literalist methodology survives in limited areas of criminal procedure, most

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

[2] 543 U.S. 405 (2005).

[3] 486 U.S. 35 (1988).

[4] 442 U.S. 735 (1979).

[5] I give Professor Chacón full credit for the "*Katz* has nine lives" expression.

[6] *See, e.g.*, Marc J. Blitz, *Video Surveillance and the Constitution of Public Space: Fitting the Fourth Amendment to a World that Tracks Image and Identity*, 82 TEX. L. REV. 1349, 1366-74 (2004) (discussing "*Katz* Revolution"); David A. Sklansky, *Back to the Future:* Kyllo, Katz, *and Common Law*, 72 MISS. L.J. 143, 153-54 (2002) (calling "striking" *Katz*'s rejection of historical approach to Fourth Amendment jurisprudence); Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call For Judicial Deference*, 74 FORDHAM L. REV. 747, 753 (2005) (characterizing *Katz* as part of "Warren Court's criminal procedure revolution").

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

notably the open fields doctrine,[8] it is now generally accepted that the Constitution protects "people, not places."[9]

Katz's liberation of the Fourth Amendment from literal constraints appears on the surface to be an unequivocal progressive victory, and conversely a conservative defeat, because one would expect the departure from textual limitations to broaden clearly the scope of the Fourth Amendment.[10] In its most civil libertarian light, *Katz* renders the "persons, houses, papers, and effects" provision a floor of protection the Court is obligated to exceed whenever a person exhibits a "reasonable expectation of privacy" in a place or thing.[11] Under such a reading, the *Katz* decision and test articulated in Justice John Marshall Harlan's concurrence has no potential to undo the Fourth Amendment's baseline protections.[12]

Unfortunately, while much of the language in *Katz* spoke of broadening privacy protections to account for technological advances, there are portions of the decision that planted the seeds of future jurisprudence subverting privacy.[13] During the last forty years, two significant judicial developments have cast doubt on the assumption that the *Katz* test could not possibly undermine the primary textual protections of the Fourth Amendment.[14] The first development, the third party doctrine, was established in business records decisions[15]

[8] *See* Oliver v. United States, 466 U.S. 170, 184 (1984).

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

[10] *See* Thomas K. Clancy, *A Vision of Search and Seizure Protection*, 34 MD. B.J. 11, 14 (2001) (noting that *Katz* decision had initial "liberal gloss"); Corinna Barrett Lain, *Countermajoritarian Hero or Zero? Rethinking the Warren Court's Role in the Criminal Procedure Revolution*, 152 U. PA. L. REV. 1361, 1430 (2004) (observing that at first blush *Katz* appears as bold liberal move countering conservatism of time).

[11] *See infra* Part I.B (discussing *Katz*'s liberal promise).

[12] *See* Morgan Cloud, *A Liberal House Divided: How the Warren Court Dismantled the Fourth Amendment*, 3 OHIO ST. J. CRIM. L. 33, 72 (2005) (suggesting that rigid standard would protect individuals more than malleable *Katz* test); Melvin Gutterman, *A Formulation of the Value and Means Models of the Fourth Amendment in the Age of Technologically Enhanced Surveillance*, 39 SYRACUSE L. REV. 647, 663 (1988) (asserting that *Katz* initially affirmed protective potential of Fourth Amendment); Susan N. Herman, *The USA Patriot Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 110 (2006) (asserting that *Katz* could have "provided an opportunity for the Court to apply Fourth Amendment protection to more than property rights").

[13] See *infra* Part I.C for discussion of *Katz*'s conservative potential.

[14] *See* Herman, *supra* note 12, at 125 (asserting that under current *Katz* interpretation "property rights are not even a floor").

[15] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 745 (1979) (holding that dialed telephone numbers are not protected); United States v. Miller, 425 U.S. 435, 443 (1976) (holding that bank records are not protected).

and garbage search cases like *Greenwood*;[16] and the second, the contraband exception, grew out of dog sniff cases like *Caballes*.[17] These doctrines twist the *Katz* test by denying Fourth Amendment safeguards in situations where even a conservative literal interpretation of the Fourth Amendment would likely secure protection.[18] Moreover, they are particularly troublesome in light of emergent crime detection technologies and increased access to private information by third parties via the Internet.

This Article explores how the third party and dog sniff cases run counter to the liberal promise of *Katz*. It analyzes the dangers of these doctrines as third parties become more essential for everyday communication and law enforcement technologies improve.[19] Part I of the Article discusses the historical context of *Katz* and examines both its liberal promise and conservative potential. Part II analyzes *Greenwood* and demonstrates how, given modern modes of communication, the case erodes privacy in the most intimate of contexts. Part III explains how the contraband exception in *Caballes* runs counter to *Katz*'s recognition of privacy zones and discusses its dangerous potential as crime detection technologies advance. Finally, Part IV suggests some ways to reconceptualize the *Katz* test to reinvigorate *Katz*'s liberal promise.

I. *KATZ*: A POTENTIAL REVOLUTION

A. The Preceding Literalist and Trespass Paradigms

Prior to the *Katz* regime, whether a search of a place or seizure of items implicated the Fourth Amendment turned on two questions: (1) whether the place searched or item seized was one cataloged in the text of the Fourth Amendment, and (2) whether the government

[16] California v. Greenwood, 486 U.S. 35 (1988).

[17] Illinois v. Caballes, 543 U.S. 405 (2005); *see also* United States v. Jacobsen, 466 U.S. 109, 123 (1984) (holding that testing of powder for presence of cocaine does not implicate Constitution); United States v. Place, 462 U.S. 696, 707 (1983) (finding that dog sniff of luggage is not search).

[18] *See* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 554 (1990) (stating that "in the two decades since *Katz* was decided, the Court has applied the standard to reduce rather than enhance fourth amendment protections").

[19] *See* Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 68 (2005) (arguing that as technologies improve, third parties will have increasing access to personal information).

sufficiently trespassed[20] on a protected interest.[21] Targets of investigative wiretapping were liable to suffer defeat on both prongs, given the Court's findings that conversations were not "papers or effects" and wiretapping did not involve physical trespass into a "house." In *Olmstead v. United States*,[22] for example, the Court held that the government's wiretapping of Olmstead's home telephone was not a constitutional event because it was not a seizure of his "papers or his tangible material effects or an actual physical invasion of his house 'or curtilage.'"[23] This strict literalist approach to the Fourth Amendment[24] spurred a passionate dissent from Justice Louis Brandeis, criticizing what he characterized as an archaic and limited reading of the Constitution. He chastised the majority for failing to recognize that "[t]he future is their care," and thus, the Court's "contemplation cannot be only of what has been but of what may be."[25]

After *Olmstead*, the Court clarified in *Silverman v. United States*[26] that when there is a physical trespass into a protected area, the government may not claim that no search occurred because police only "seized" a conversation.[27] In *Silverman*, police used a high

[20] I do not use trespass in the state property law sense, but rather to signify some physical entry into a protected area. In *Silverman*, for example, there was no violation of state trespass laws, but the Court found a "trespass" under the Fourth Amendment because the government had physically intruded on Silverman's protected area. Silverman v. United States, 365 U.S. 505, 512 (1961). Conversely, in open fields cases, courts often find trespass under state property law, but no constitutional trespass into a protected area. *See, e.g.*, United States v. Hatfield, 333 F.3d 1189, 1199 (10th Cir. 2003).

[21] *See* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 WAKE FOREST L. REV. 307, 316 (1998) (discussing pre-*Katz* approach limiting Fourth Amendment protection to tangible objection and physical invasions).

[22] 277 U.S. 438 (1928).

[23] *Id.* at 466.

[24] Justice Hugo Black's dissent in *Katz* reflects the literalist approach with a peculiar spin on the trespass-based analysis. He vehemently rejected that conversations are protected, advancing a strict textual approach. Katz v. United States, 389 U.S. 347, 365 (1967) (Black, J., dissenting). As for the idea that any invasion into a protected area is a search, Justice Black asserted that such physical trespasses are not Fourth Amendment violations but unreasonable intrusions entailing exclusion under the Court's "supervisory power." *Id.* at 369. He asserted that neither seizure of conversations nor physical trespass into a protected area implicates the Fourth Amendment, although the Court could police such physical intrusions on other grounds. *Id.* at 370.

[25] *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting).

[26] 365 U.S. 505 (1961).

[27] *Id.* at 509-10.

powered microphone to detect a conversation within the suspect's house.[28] The Court found that the microphone's placement abutting a duct outside of the house rendered the police action a physical invasion and thus a search implicating the Fourth Amendment.[29] The *Katz* majority opinion and Justice Harlan's concurrence characterized *Silverman* as overruling *Olmstead* because it rejected *Olmstead*'s principal "ground that conversations were not subject to the protection of the Fourth Amendment."[30] Alternatively, *Silverman* can be seen as prioritizing the trespass-based approach to the Fourth Amendment over the literalist principle that conversations are unprotected.[31] The Court continued to maintain that conversations themselves are not "tangible objects" worthy of constitutional protection.[32] However, it elevated and expanded the trespass premise by holding that any minor physical invasion into a protected area, even if to seize an unprotected thing, is a Fourth Amendment search.[33]

B. The Liberal Promise of Katz

The Supreme Court granted certiorari in *Katz* to determine whether the government's warrantless monitoring of conversations from a public phone booth violated the Fourth Amendment.[34] *Katz* showed an enormous amount of potential to expand individual rights because it definitively marked the departure from the long-accepted literalist

[28] *Id.* at 506.

[29] *Id.* at 509-12.

[30] Katz v. United States, 389 U.S. 347, 362 n.* (1967); *see* Cloud, *supra* note 12, at 65 n.119 (noting that *Silverman* "is viewed as the opinion overruling *Olmstead*'s holding that only tangible things, and not intangibles like conversations, could be seized").

[31] *See* Michael Adler, Note, *Cyberspace, General Searches, and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093, 1103 (1996) (asserting that physical intrusion was "decisive difference between *Olmstead* and *Silverman*").

[32] *See Silverman*, 365 U.S. at 509 ("Nor do the circumstances here make necessary a reexamination of the Court's previous decisions in this area.").

[33] *See id.* (finding that eavesdropping was executed "by means of an unauthorized physical penetration into the premises"). Justice Antonin Scalia in *Kyllo v. United States* characterized *Silverman* as recognizing the ultimate inviolate nature of the home, stating "In *Silverman* . . . we made clear that any physical invasion of the structure of the home, 'by even a fraction of an inch,' was too much." 533 U.S. 27, 37 (2001) (quoting *Silverman*, 365 U.S. at 512).

[34] *Katz*, 389 U.S. at 348-49. The petitioner had originally framed the principal issue in trespass terms, that is, "[w]hether a public telephone booth is a constitutionally protected area." *Id.* at 349.

concept that Fourth Amendment protections apply only to the enumerated items.[35] The Court rejected the argument that Fourth Amendment protections are confined only to papers and effects.[36] It thus recognized that protection against unwarranted government intrusion pertains not only to the physical contents of one's home or property, but also to the intangible contents of one's mind.[37] Moreover, the Court dismissed the idea that a place must be a house or curtilage in order to enjoy constitutional protection.[38] The Court held that the factor determinative of constitutional protection is whether the person expects the place or thing searched to be private,[39] stating that what a person "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[40] The clear import of this analysis is that privacy in things and places not listed within the language of the Fourth Amendment can nonetheless be protected.[41]

Less clear is whether the Court completely receded from the trespass-based analysis lurking in *Olmstead* and *Silverman*. The *Katz* opinion initially seems to reject the trespass paradigm, stating that "the correct solution of Fourth Amendment problems is not necessarily promoted by incantation of the phrase 'constitutionally protected area.'"[42] The Court accordingly refused to define the Fourth Amendment by reference to a list of protected areas, including homes, and a list of unprotected areas, including open fields.[43] However, the

[35] *See* James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 650 (1985) (noting that *Katz*'s "monumental theoretical achievement" was to define protection by reference to values underlying Fourth Amendment).

[36] *Katz*, 389 U.S. at 352-53.

[37] *Id.* at 353.

[38] *Id.* at 352.

[39] *Id.* at 351-52.

[40] *Id.* at 351, 359 ("Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures.").

[41] *See* Tomkovicz, *supra* note 35, at 650 (observing that *Katz* confirmed that "[a]ctivity would no longer be categorized as a search or nonsearch due to its purpose or physical qualities").

[42] *Katz*, 389 U.S. at 350. Many scholars take this language as an unequivocal rejection of the trespass approach. *See, e.g.*, Sklansky, *supra* note 6, at 152-53 (asserting that *Katz* "Court took the occasion [to] reject as obsolete the 'trespass' theory underlying the *Olmstead* decision").

[43] *Katz*, 389 U.S. at 351 & n.8 (describing parties' delineation of protected and unprotected areas and stating that any "effort to decide whether or not a given 'area,' viewed in abstract, is 'constitutionally protected' deflects attention from the problem presented by this case").

Court elsewhere engaged language indicating that it considered the phone booth a protected area, at least insofar as spoken conversations were concerned.[44] The Court stated of phone booths:

> One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world. To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication.[45]

Justice Harlan's concurrence also concentrated more on debunking the notion that conversations are not protected from electronic search than retreating from the "protected area" analysis.[46] Rather than deeming the place of search irrelevant, he broadened the category of constitutionally protected areas to include public phone booths.[47] He characterized the phone booth as a "temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[48] Moreover, prior to articulating the now-famed *Katz* test, Justice Harlan noted that the protection the Fourth Amendment affords will often be defined with reference to places.[49] The determination of whether a particular area is "constitutionally protected" in turn relies on whether the person exhibits an actual and reasonable expectation of privacy in the place or activity conducted therein.[50]

The majority and concurrence's treatment of the trespass issue nonetheless can be seen as liberal. The opinion broadened the category of protected places to include any location where a person can reasonably expect privacy, even if in public.[51] More significantly, the Court expanded the notion of trespass to include more than just

---

[44] *See* Sklansky, *supra* note 6, at 158 (questioning whether *Katz* would have reached different result if phone booth was not involved).

[45] *Katz*, 389 U.S. at 356.

[46] *See* Blitz, *supra* note 6, at 1369 ("Harlan's opinion did not so much abandon the doctrine of Constitutionally protected areas as update it . . . .").

[47] *Katz*, 389 U.S. at 360 (Harlan, J., concurring) (asserting that "an enclosed telephone booth is an area . . . a person has a Constitutionally protected reasonable expectation of privacy").

[48] *Id.* at 361.

[49] *Id.*

[50] *Id.* Harlan phrases the famed *Katz* test as follows: "[F]irst 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.'" *Id.*

[51] *Id.* at 351 (majority opinion).

physical invasions.[52] Justice Harlan, recognizing the phone booth as a protected area, asserted that the Fourth Amendment prohibits unwarranted "electronic as well as physical intrusion[s]" into that area.[53] This new broadened interpretation of trespass, although perhaps less revolutionary than a total rejection of the "protected area" analysis, has some very important ramifications. While in some aspect tied spatially to a "place," *Katz* can be interpreted as proposing that a person enjoys a roving "zone of privacy" wherever she may be, so long as she has concealed those things sought by the government from the prying eyes or ears of the general public.[54]

Thus, the spirit of *Katz* is a promise of freedom from unwarranted invasions of privacy in all areas we consider intimate.[55] Unfortunately, the *Katz* revolution was not unequivocally liberal.[56] There is language in the case that laid the groundwork for the eventual erosion of privacy rights. Looking back over the last forty years, one can now pinpoint the dicta in *Katz* and portions of the *Katz* test that eventually became its undoing as the Court swung to the right.[57]

C. The Seeds of Conservatism

The *Katz* decision contains two reactive ingredients which eventually exploded into a line of conservative cases providing less protection than a literal approach to the Fourth Amendment. First,

---

[52] *Id.* at 353.

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

[54] *Cf.* Rakas v. Illinois, 439 U.S. 128, 166 (1978) (White, J., dissenting) (asserting that *Katz* stands for proposition that people enjoy "zones of privacy" not defined merely by reference to property law). In a different context, the Court held, "there is a zone of privacy surrounding every individual." Cox Broad. Corp. v. Cohen, 420 U.S. 469, 487 (1975); *see also* Lee Tien, *Door, Envelopes, and Encryption: The Uncertain Role of Precautions in Fourth Amendment Law*, 54 DEPAUL L. REV. 873, 874 (2005) (asserting that *Katz* recognized "temporary zone of personal privacy").

[55] Professor Tracey Maclin asserts that *Katz* "loosened [the Fourth Amendment] from the ancient niceties of common-law property rules" and allowed for "thoroughly modern and realistic understandings of the privilege against unreasonable searches and seizures." Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 62 (2002).

[56] To further muddy the water, there is evidence that the Justices themselves never agreed on the true meaning of *Katz*. *See id.* at 91 (suggesting that Justices White and Harlan saw *Katz* very differently).

[57] One expert notes that "what ultimately emerged [from *Katz*] was an amendment that was privacy bound, rising or falling in both scope and protection based upon how the notion of privacy fared in the Court and within society as a whole." Scott E. Sundby, *"Everyman"'s Fourth Amendment: Privacy or Mutual Trust Between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1758 (1994).

the *Katz* test itself is fluid, vague, and liable to produce wildly varying results.[58] Second, certain language in the decision hinges privacy on an individual's precautionary behavior.[59] The combination of these two factors laid the groundwork for future doctrine defining reasonable expectation as risk assumption, a doctrine that has shown the potential to swallow the entirety of Fourth Amendment privacy protection.[60]

If one were to identify *Katz* with a particular judicial tactic, one could say it is really a case about moving from bright line rules to standards. The fixed categories of protected areas and things gave way to a test that invited the Court to determine the extent of Fourth Amendment protections more broadly on a case-by-case basis. The problem, however, is that the benefit of flexibility is often accompanied by the danger that the case-sensitive approach will be manipulated or manifest as arbitrary. Over the years, the *Katz* decision has been the subject of two principle civil libertarian criticisms: what I term the "manipulation problem" and the "normativity problem." The manipulation problem describes the tendency of conservative pragmatist courts to manipulate *Katz*'s requirements to defeat privacy claims in places or things society considers personal.[61] The normativity problem is the charge that *Katz* allows objectionable governmental or social practice to define the scope of the Fourth Amendment.[62]

Turning to the manipulation problem, critics assert that both the subjective expectation and reasonableness requirements of the *Katz* test are vulnerable to political manipulation.[63] Generally, subjective

[58] *See* Clancy, *supra* note 21, at 340 (observing that "a conservative Court has employed privacy analysis as a vehicle to restrict Fourth Amendment protections").

[59] *See* Katz v. United States, 389 U.S. 347, 352 (1967) (stating that Katz was "entitled" to assume privacy because, inter alia, he "shut the door" of phone booth).

[60] *See* Gutterman, *supra* note 12, at 665-66 (observing that subjective portion of test invited "future members of the Court [to] apply their own beliefs" as to reasonable precautions and expectations).

[61] *See* Clancy, *supra* note 21, at 330-40 (describing how *Katz* test's malleable nature has allowed conservative courts to constrict privacy rights); Gutterman, *supra* note 12, at 666 ("By placing the fourth amendment on such an indefinite and shifting footing, Justice Harlan laid the foundation for *Katz* to be used in the future to restrict the core of privacy embodied in the fourth amendment."); Katz, *supra* note 18, at 556 (asserting that *Katz* test "leaves room for broad swings of judicial interpretation and maneuvering").

[62] *See* Maclin, *supra* note 55, at 89 (noting that "because it lacks any type of principled norm, the expectations test . . . does not provide a substantive model or neutral principle that protects Fourth Amendment liberties").

[63] *See, e.g.*, Gutterman, *supra* note 12, at 665-66 (criticizing both Court's

beliefs are established through direct or circumstantial evidence that the individual entertained a certain thought.[64] In the Fourth Amendment context, there should be a near presumption of subjective expectation of privacy, given that every case involves illegal behavior, something people presumably seek to keep clandestine.[65] However, certain language in *Katz* allows courts to answer the subjective inquiry, not by discerning actual intent, but by assessing precautionary behavior. For example, Katz was "entitled" to Fourth Amendment protection because, among other things, he "shut[] the door behind him."[66] Later decisions have taken such language as an invitation to manipulate the inquiry to say that a person has no subjective expectation of privacy unless he takes precautions satisfactory to the Court.[67] This, however, has absolutely nothing to do with the point of the subjective inquiry, which is to determine whether the defendant actually did consider his actions private.[68]

One may respond that such a judicial mishap has no consequence because the second part of the *Katz* test requires the defendant's subjective expectations be reasonable. Thus, the Court would have to look at precautionary measures anyway to determine the reasonableness of the defendant's belief.[69] Reasonableness has many permutations and surely an extended discussion of this oft-analyzed

treatment of subjective and objective prongs).

[64] *See, e.g.*, Rawlings v. Kentucky, 448 U.S. 98, 105 (1980) (holding no Fourth Amendment protection given defendant's "frank admission . . . that he had no subjective expectation that [he] would remain free from governmental intrusion").

[65] Even without such a presumption, it is very likely that evidence will reveal the defendant, no matter how misguided, believed that what he did was private.

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

[67] *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) (finding no subjective expectation because people in general know that they convey telephone numbers to phone company).

[68] One can only make sense of the subjective test as a type of standing requirement; that is, a defendant should not be able to claim a privacy violation in an area he never expected to be private. Nonetheless, critics assert that because of the manipulation problem, the subjective requirement should be abandoned. *See, e.g.*, James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 344 (2002) (stating that subjective test "is superfluous or duplicative, at best. At worst, it has the potential to mislead lower courts into denying legitimate Fourth Amendment claims.").

[69] *See* Tomkovicz, *supra* note 35, at 655 (noting that defendant's precautionary behavior has become important part of reasonable expectation of privacy analysis). This runs counter to Justice Harlan's warning that "the burden of guarding privacy in a free society should not be on its citizens." United States v. White, 401 U.S. 745, 793 (1971) (Harlan, J., dissenting).

term is beyond the scope of this Article.[70] Generally, however, a belief is reasonable either when it is numerically typical or when it is a minority position that otherwise has some logical or moral validity. Thus, the most straightforward way for the Court to analyze reasonableness would be to determine whether the typical American would expect a certain action, place, or thing to be private.[71] Regarding precautions, there are some that render an expectation of privacy unreasonable when absent, and others that do not. For example, if one sets up an open shower on his front porch, it would be atypical to expect his shower activities to be private. On the other hand, a person who takes a shower in his home likely has not checked every possible crevice or window crack through which a voyeur could look. Yet, his failure to take such precautions does not render his expectation of privacy in his shower unreasonable because the average person does not take such precautions.[72]

After *Katz*, as *Greenwood* and related cases demonstrate, the Court twisted the reasonableness requirement, holding that an individual must assume the risk of government intrusion when she has not taken truly extraordinary and even impossible precautions.[73] Perhaps, then, this heightened precaution standard can be justified as a normative reading of the reasonableness requirement. In other words, society at large might fail to take such precautions, but such precautions are nonetheless preferable or morally required. The assumption of risk analysis then creates incentives to take socially beneficial precautions.[74] The problem with such an argument, as I demonstrate

[70] For a discussion of reasonableness in the context of the Fourth Amendment, see generally Thomas K. Clancy, *The Fourth Amendment's Concept of Reasonableness*, 2004 UTAH L. REV. 977.

[71] Indeed, the Court gives lip service to this idea, stating that reasonableness should be defined in terms of social expectations. *See* Rakas v. Illinois, 439 U.S. 128, 143 & n.12 (1978) (stating that reasonableness should be determined by "understandings that are recognized and permitted by society").

[72] *See* Tien, *supra* note 54, at 887 (observing that Court "has been deeply conflicted about how to handle the many types of precautions used in everyday life, and especially reluctant to recognize predominant social conventions").

[73] *See infra* notes 132-47 and accompanying text (discussing assumption of risk principles); *see also* Gutterman, *supra* note 12, at 666-69 (discussing Court's assumption of risk analysis); David Rudovsky, *The Impact of the War on Drugs on Procedural Fairness and Racial Equality*, 1994 U. CHI. LEGAL F. 237, 253-54 (observing that "[a]pplying notions of 'assumption of the risk' and 'knowing exposure' of information or conduct, the Court severely limited both the physical areas and personal conduct entitled to Fourth Amendment protection").

[74] Some law and economics scholars argue that there should be a disincentive for not protecting one's personal space from outside invasion because such invasions

in the next part, is that the risk analysis used to determine reasonableness by the Court in Fourth Amendment cases has absolutely nothing to do with whether the individual's public "exposure" is voluntary, morally wrong, or inefficient.[75] Consequently, "assumption of risk" is a linguistic subterfuge that paints the defendant's actions as voluntary or suboptimal when, in fact, there is no logical reason to shackle the defendant with risk disabilities, save for the basic desire to prioritize law enforcement over privacy.[76]

Another way the Court manipulates the objective test is to substitute the term "legitimate" for "reasonable." In cases like *Caballes*, the Court considers, not whether the areas searched are ones society typically holds private, but whether the thing eventually seized by the police is "legitimate," meaning lawful.[77] The Court's tendency to twist the reasonableness inquiry into a tool to undermine typical privacy expectations leads critics to disparage the *Katz* test as an invitation to political exploitation.[78] The test can deny privacy whenever "a bare majority of justices concludes that even a vigorously exercised subjective expectation of privacy is unreasonable." [79]

Even when the Court does base reasonable expectations on societal beliefs, it may produce less than satisfying results.[80] Although the Court is not manipulative, there is still a normativity problem because our collective privacy expectations are often formed in response to normatively disfavored behavior.[81] For example, the government can

create external costs. *See, e.g.*, Alon Harel, *Efficiency and Fairness in Criminal Law: The Case for a Criminal Law Principle of Comparative Fault*, 82 CAL. L. REV. 1181 *passim* (1994). The response, however, is not that the typical actor should be disincentivized as much as the deviant or voyeuristic actor should be punished. *See* Aya Gruber, *Pink Elephants in the Rape Trial: The Problem of Tort-Type Defenses in the Criminal Law of Rape*, 4 WM. & MARY J. WOMEN & L. 203, 243-45 (1997).

[75] *See infra* notes 132-40 and accompanying text (analyzing Court's use of assumption of risk in Fourth Amendment cases).

[76] Professor Melvin Gutterman asserts that, in fact, crime control was the explicit goal this manipulative move was intended to serve. Gutterman, *supra* note 12, at 665.

[77] *See infra* notes 215-23 and accompanying text (examining this judicial move).

[78] *See supra* notes 60-63.

[79] Cloud, *supra* note 12, at 72; *see also* Clancy, *supra* note 21, at 339 (noting that lack of textual ground for *Katz* test "leaves the fluid concept of privacy to the vagaries of shifting Court majorities").

[80] *See* Erik G. Luna, *Sovereignty and Suspicion*, 48 DUKE L.J. 787, 825-26 (1999) (stating that "Court has interpreted privacy to be a question of fact rather than a constitutional value").

[81] *See* Gutterman, *supra* note 12, at 731 ("By refusing to acknowledge normative expectations of privacy in the face of government expediency, the Court has inverted

implement overbearing policies that create lowered expectations of privacy.[82] Defining reasonableness thereafter with reference to collective expectation allows government gamesmanship to defeat basic Fourth Amendment protections.[83] Similarly, private deviants and snoops affect our typical expectations; and thus, defining reasonableness solely by collective beliefs allows the Fourth Amendment's parameters to be set by hackers and peeping toms.[84]

These examples illustrate the basic "is-ought" problem of the reasonable requirement. At some level the constitutional inquiry must concern not just what society actually believes is private, but what we ought to be able to regard as private, regardless of the ability of the government or others to penetrate our privacy barriers.[85] Soon after *Katz*, Justice Harlan recognized as much, observing in his *United States v. White* dissent, "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."[86]

In the next two sections, I demonstrate how the *Greenwood* and *Caballes* lines of cases have cultivated the seeds of conservatism in *Katz*. These two doctrines have directly undermined the liberal promise of *Katz*, manipulating the test to deny privacy in ways contrary to basic intuition. In this sense, they have rendered *Katz* more devolution than revolution.

---

the plain reading of the fourth amendment."); Tien, *supra* note 54, at 899 (arguing that privacy rights should be ordered around natural evolution of collective beliefs, as opposed to government-imposed lowered expectations).

[82] *See* Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 384 (1974) (noting that government could lower privacy expectations "by announcing half-hourly on television that . . . we were all forthwith being placed under comprehensive electronic surveillance").

[83] The *Smith* Court recognized as much, observing that a "normative" inquiry would be required if the government were to announce widespread searching. Smith v. Maryland, 442 U.S. 735, 741 (1979).

[84] *See* Sundby, *supra* note 57, at 1760 (observing that "because as governmental and nongovernmental intrusions on privacy expand, the scope of what one reasonably expects to be private correspondingly becomes truncated"); *see also infra* notes 181-83 and accompanying text (discussing hackers and Internet privacy).

[85] *See Smith*, 442 U.S. at 750 (Marshall, J., dissenting) ("By its terms, the constitutional prohibition of unreasonable searches and seizures assigns to the judiciary some prescriptive responsibility . . . ."); Gutterman, *supra* note 12, at 665 (criticizing *Katz* test for "fail[ing] to acknowledge that there are privacy rights to which the people are entitled"); Tomkovicz, *supra* note 35, at 685 (stating that judge's "task is to discern and impose norms").

[86] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

II. GARBAGE PAILS

The third party line of cases, according to many liberal scholars, has sounded the death knell of *Katz* as a liberal doctrine.[87] Indeed, *Greenwood* embodies both the manipulation and normativity problems with the *Katz* test. The case is exemplary of a broader strategy of watering down *Katz* through a jurisprudence of possibility, risk analysis, and third party exposure. This type of analysis has particularly disturbing implications in light of the modern prevalence of private electronic communication involving third party service providers.

A. Possibilities, Risks, and Third Parties

Greenwood held that garbage searches fall outside the purview of the Fourth Amendment because there is no reasonable expectation of privacy in trash left out for collection.[88] Initially, the Court appeared to concede that *Greenwood* may very well have retained an actual expectation of privacy in his trash, which was left outside in opaque bags.[89] As a consequence, the Court's analysis turns on the meaning of "reasonable expectation."[90] The Court came to the conclusion that *Greenwood*'s expectation of privacy was not reasonable by making three principal arguments: (1) Greenwood exposed the trash to the public;[91] (2) the handling of the trash by third party garbage collectors defeated its private nature;[92] and (3) the trash items were in "plain view."[93] The Court's plain view holding does not merit extended discussion, mainly because the Court seemed just to misapply the doctrine. As a consequence, *Greenwood* has not served as precedent for the claim that the contents of opaque bags are in plain view.[94]

---

[87] *See, e.g.*, Katz, *supra* note 18, at 564 (describing assumption of risk doctrine as "devourer" of *Katz*'s privacy notions); Maclin, *supra* note 55, at 79 (observing that "[e]xpectations theory and risk analysis replaced Katz as the defining methodology for measuring the Fourth Amendment's protection").

[88] California v. Greenwood, 486 U.S. 35, 37 (1988). It is important to note the Court considered only the case of trash located "outside the curtilage." *Id.* at 37-39.

[89] *Id.* at 39.

[90] *Id.* at 39-43.

[91] *Id.* at 40 ("Here, we conclude that respondents exposed their garbage to the public sufficiently to defeat their claim to Fourth Amendment protection.").

[92] *Id.* at 41 (holding that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979)).

[93] *Id.*

[94] *See* United States v. Hedrick, 922 F.2d 396, 399 (7th Cir. 1991) (noting that

Thus, more troubling are the *Greenwood* Court's two other arguments, as they create extremely dangerous doctrinal methodologies for interpreting reasonableness.

1. The First Manipulation: Possibility vs. Privacy

One of the Court's main arguments is that Greenwood had no privacy interest in trash he "exposed" to the public. The Court appeared to concede, however, that Greenwood did not subjectively believe that he had exposed his trash.[95] Perhaps, then, the Court mistakenly equated voluntariness and reasonableness. It is not so much that Greenwood believed his trash would be seen by the public, as he should have known it would be viewed when he voluntarily put it on the curb.[96] Yet this is only true if the public harbors the general belief that trash left for pick-up in an opaque bag will be seen by the general public, including potentially the government.[97] Indeed, the *Greenwood* Court attempted to make this very case, asserting that "[i]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public."[98] However, the Court's empirical support for its conclusions about "common knowledge" is thin at best, indicating that the Court's treatment of reasonableness is manipulative.

The Court cited a state case in which a dog "at the behest of no one" dragged trash from the defendant's back yard to a neighbor's yard.[99] That trash was eventually searched by the police, and the state court

Greenwood's holding does not mean that container contents, that are not in plain view, are searchable); *cf.* United States v. Hall, 47 F.3d 1091, 1096 (11th Cir. 1995) ("We do not read *Greenwood* as measuring the degree of exposure only through reference to that which is in plain view.").

[95] *Greenwood*, 486 U.S. at 39.

[96] *See* Katz, *supra* note 18, at 563 (stating that *Katz* never meant "every limited exposure [to] constitute a witting or unwitting renunciation of the fourth amendment protection").

[97] Professor Scott Sundby suggests that it is so obvious that we do not expect trash to be private that it was "silly" for the Court to grapple with the issue in such depth. Sundby, *supra* note 57, at 1792. He argues that the core problem with the *Greenwood* holding is that it creates a world in which "government officials regularly examine[] the contents of trash cans to maintain control over the citizenry." *Id.* On the other hand, if all that was at stake was merely unprivate "fruit rinds and coffee grinds," *id.*, then trash sifting would be an ineffective control mechanism.

[98] *Greenwood*, 486 U.S. at 53.

[99] *Id.* at 41 n.2 (quoting State v. Ronngren, 361 N.W.2d 224, 228 (N.D. 1985)).

upheld the search's validity.[100] From this, the Court concluded that the possibility of animal tampering renders the expectation of privacy in trash unreasonable.[101] The problem is the state court holding turned, not on the unprivate character of personal trash, but on the fact that a nonstate actor (in this case a dog) was the one who intruded on the privacy interest.[102] The Court did not explain why the possibility of dogs entering our yards does not destroy our yards' privacy while the possibility of them rummaging through our trash destroys its privacy. As Justice William Brennan pointed out in his *Greenwood* dissent, while it is permissible for police to inspect "a package whose 'integrity' a private carrier has *already* 'compromised,'" the trash at issue in *Greenwood* was searched at the direction of the government.[103]

The Court then discussed the case of a "[r]ich lady" who rifled through the town dump seeking proofs of purchase for refunds.[104] However, this empirical evidence, itself scant, supports a different proposition altogether — that society harbors no expectation of privacy in trash items already deposited into a public dump.[105] Granted, it may be unreasonable to believe that our trash will never become publicly exposed. Our privacy concerns, however, are not just about people viewing our trash, but about them viewing our trash, knowing it is *ours*. For this reason, we attempt to keep our trash anonymous until it is sufficiently amalgamated to prevent identification.[106] One scholar explains:

> The expectation that attends one's contributions to these waste streams is not secrecy but anonymity. A similar attitude accompanies our use of the postal and telephone systems: the names and addresses of correspondents and the numbers of those called are of necessity disclosed to the system's employees,

[100] *State v. Ronngren*, 361 N.W.2d 224, 228 (N.D. 1985).

[101] *Greenwood*, 486 U.S. at 40-41.

[102] *See Ronngren*, 361 N.W.2d at 228.

[103] *Greenwood*, 486 U.S. at 53 (Brennan, J., dissenting).

[104] *Id.* at 41 n.3 (majority opinion).

[105] *Id.* at 53 (Brennan, J., dissenting) (stating, "[H]ad police searching the city dump run across incriminating evidence that, despite commingling with the trash of others, still retained its identity as Greenwood's, we would have a different case").

[106] *See infra* notes 161-69 and accompanying text (discussing anonymity and privacy on Internet).

> but there exists an expectation that this information will be treated as part of an undifferentiated flow.[107]

The only actual example of private trash bag snooping to which the Court referred is the practice of celebrity "trash-picking" by tabloid journalists.[108] Again, however, this phenomenon is highly unlikely to make the average nonfamous person believe that his trash will be rummaged though by members of the general public.[109] The Court's examples demonstrate that instead of defining reasonableness in terms of society's actual beliefs about what is shielded from public viewing, the Court manipulated the reasonableness inquiry into a disturbing, dangerous, and unwarranted jurisprudence of possibility. It basically held that the remote possibility of disclosure renders unreasonable an individual's privacy expectations.[110] Indeed, the closest the Court came to doing any empirical analysis on views of the privacy of trash was its canvassing of other court decisions.[111]

Let us assume for a moment, however, that the actions of various snoops make the average person paranoid that someone is always rifling through his trash. Arguing that Greenwood's expectation is therefore unreasonable requires the Court to adopt the absurd position of allowing untrained dogs and sleazy journalists to define reasonableness.[112] In turn, the reasonably private person must be a super-paranoid individual who has walled in his house, speaks in code, buries the trash in the backyard, and keeps money under the mattress.[113] The Court therefore should consider whether, regardless

---

[107] John M. Junker, *The Structure of the Fourth Amendment: The Scope of the Protection*, 79 J. CRIM. L. & CRIMINOLOGY 1105, 1158-59 (1989).

[108] *Greenwood*, 486 U.S. at 41 n.4.

[109] *See* George C. Thomas, *Time Travel, Hovercrafts, and the Framers: James Madison Sees the Future and Rewrites the Fourth Amendment*, 80 NOTRE DAME L. REV. 1451, 1504 (2005) (noting that "if we fully expected sometimes to discover that our trash was strewn all over the street, no one would put garbage in plastic bags").

[110] *See Greenwood*, 486 U.S. at 54 (Brennan, J., dissenting) ("The mere possibility that unwelcome meddlers might open and rummage through the containers does not negate the expectation of privacy in their contents any more than the possibility of a burglary negates an expectation of privacy in the home.").

[111] *See id.* at 42-43 (citing cases).

[112] *See* Rudovsky, *supra* note 73, at 255 ("The fact that other people may steal, vandalize, or enter our property to take this material can hardly provide legitimate grounds for permitting the police to do the same.").

[113] One scholar jokes that under current Supreme Court law an "Accidental Tourist's Guide to Maintaining Privacy Against Government Surveillance" would give the following advice:

> To maintain privacy, one must not write any checks nor make any phone

of the prevalence of voyeurs, people ought to be able to regard their bagged trash as private.[114] The Court did undertake such a normative inquiry, but ended up setting forth legal analysis even more dangerous to privacy than its loose empirical analysis.

2. The Second Manipulation: Assumption of Risk & Third Parties

The portion of *Greenwood* most dangerous to civil rights is the Court's holding regarding third party exposure. The Court found Greenwood did not have a defensible privacy interest because he "placed [his] refuse at the curb for the express purpose of conveying it to a third party, the trash collector, who might himself have sorted through respondent's trash or permitted others, such as the police, to do so."[115] The Court relied principally on *Smith v. Maryland* for the proposition that voluntary exposure to third parties renders personal items nonprivate.[116] In *Smith*, the Court held that the use of a pen register to detect and store numbers dialed from a home telephone did not implicate the Fourth Amendment.[117]

The *Smith* Court began by speculating that society does not typically expect privacy in dialed telephone numbers because individuals know that the telephone company collects such numbers and can expose them to the world.[118] However, most people would probably consider the numbers they dial *not* to be general public information, whether or not they are aware that the telephone company collects numbers.[119] While clearly manipulating the empirical inquiry, *Smith* did grapple

> calls. It would be unwise to engage in conversation with any other person, or to walk, even on private property, outside one's house. . . . [I]deally, one would take the trash personally to the disposal site and bury it deep within. Finally, when buying items, carefully inspect them for any electronic tracking devices that may be attached.

Sundby, *supra* note 57, at 1789-90.

[114] *See supra* notes 60-62 (asserting *Katz* test should be normative).

[115] *Greenwood*, 486 U.S. at 40.

[116] Smith v. Maryland, 442 U.S. 735, 742-43 (1979).

[117] *Id.* at 745-46.

[118] *Id.* at 742 ("All telephone users realize that they must 'convey' phone numbers to the telephone company. . . ."); *see* Jose Felipe Anderson, *Reflections on Standing: Challenges to Searches and Seizures in a High Technology World*, 75 MISS. L.J. 1099, 1120 (2006) (calling Court's empirical conclusion "loose conjecture").

[119] *See* Thomas, *supra* note 109, at 1502 (drawing "distinction between 'exposing' phone numbers to the telephone company and putting my marijuana Christmas tree in front of my picture window and opening the curtains"). Indeed, popular culture is rife with examples of spouses calling paramours, giddy teenagers secretly dialing crushes and hanging up, and friends arranging surprise parties by telephone.

with the normativity problem.[120] The Court stated that a normative rather than subjective societal inquiry would be appropriate "if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry [and] individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects."[121]

So then what differentiates the phone company's practice of storing dialed numbers, at issue in *Smith*, from a hypothetical case in which the government announces that it will compel phone operators to monitor phone conversations at random? The Court hinted at an answer by stating "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications."[122] This is indeed a promising line of analysis, for it allows the Court to differentiate between kinds of information sought and determine the corresponding amounts of justification the government must possess before obtaining them.[123] In the computer context, while mass aggregate data or other relatively innocuous information might not enjoy full constitutional protection, information that conveys intimate personal details, communications content, or navigation predilections would enjoy protection, whether or not a third party Internet Service Provider ("ISP") had access.[124]

---

[120] *Smith*, 442 U.S. at 741; *see supra* notes 60-63 and accompanying text (discussing normativity problem).

[121] *Smith,* 442 U.S. at 741 n.5.

[122] *Id.*

[123] Unfortunately, in the modern era, the information that falls under *Smith*'s pen register holding may encompass far more than just telephone number information. *See infra* note 151 (discussing Internet pen registers and trap and trace devices). In 1994, Congress passed the Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994), which required telecommunications carriers to ensure that law enforcement would have the capability to intercept individual telephone calls and obtain certain "call-identifying information," including the location of antenna towers used in wireless telephone calls, signaling information from custom calling features, telephone numbers dialed after calls are connected, and three way calling information. *See* U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 453, 460 (D.C. Cir. 2000). The carriers sued, arguing that under *Smith,* the companies could only be forced to disclose telephone numbers. *Id.* at 459. The court responded, "*Smith*'s reason for finding no legitimate expectation of privacy in dialed telephone numbers . . . applies as well to much of the information provided by the challenged capabilities." *Id.*

[124] Under the framework set forth in the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, Title III, 82 Stat. 212 (codified as amended at 18 U.S.C. §§ 2510-2522 (2000 & Supp. II 2003)) [hereinafter Title III], and the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) [hereinafter ECPA],

Of course, even the content/noncontent distinction has problems. Justice Brennan warned that telephone numbers "are not without 'content'" and convey intimate information.[125] Nonetheless, an analysis of privacy that rests on the level of intimacy of the information sought is better than the analysis that survived from *Smith*.[126] Had *Smith* established a content test, the *Greenwood* Court would have had a difficult time finding a person's trash is without content.[127] Unfortunately, the content/noncontent analysis is not central to *Smith*, and the case is generally regarded as establishing a very rigid third party doctrine.[128] The Court ended up defining reasonable expectations, not empirically in terms of typical belief or normatively in terms of levels of intimacy, but by risk assumption.[129] The Court held that a person who exposes private information to a third party custodian must assume the risk that the third party will share it with the government.[130] As a result the government is permitted to obtain such information directly and contemporaneously.[131]

the question of content versus noncontent information is often a central issue to the validity of a search. *Compare* 18 U.S.C. § 3121 (2000 & Supp. I 2002) (allowing government to use trap and trace devices with only court order and without probable cause), *with* 18 U.S.C. §§ 2510-2522 (requiring "acquisition of the contents" of electronic communications to accord with wiretap warrant procedures). Nonetheless, judicial clarity in this area is very important. While the ECPA provides that the content of email transmissions may not be intercepted without a valid Title III warrant, short term stored emails (180 days or less) require a warrant, but not a wiretapping warrant, and long term stored emails only require a court order. 18 U.S.C.S. § 2703 (2007). In addition, under the statutory scheme, it is unclear whether email header information, click stream data, web commerce data, and the like should fall under the provisions regulating content or the provisions regarding trap and trace devices. *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 51, 70 (2004).

[125] *Smith*, 442 U.S. at 748 (Stewart, J., with whom Brennan, J., joined, dissenting).

[126] *See* Freiwald, *supra* note 124, at 40 (noting that *Smith* "substituted the fact-of-interceptibility test for a difficult normative judgment").

[127] *See* California v. Greenwood, 486 U.S. 35, 50-51 (1988) (Brennan, J., dissenting) ("It cannot be doubted that a sealed trash bag harbors telling evidence of the 'intimate activity associated with the 'sanctity of a man's home and the privacies of life," which the Fourth Amendment is designed to protect." (citations omitted)).

[128] *See id.* at 41 (majority opinion) (referencing *Smith* for unqualified proposition that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (quoting *Smith*, 442 U.S. at 743-44)).

[129] *Smith*, 442 U.S. at 743-44.

[130] *Id.* at 744.

[131] The Court blew off Smith's argument that the phone company would not keep a record of local calls from his phone, asserting, "We are not inclined to make a crazy quilt of the Fourth Amendment, especially in circumstances where (as here) the

Assumption of risk is a principal familiar from torts premised on the concept that consent prevents redress.[132] For this reason, one who is unaware of a risk cannot be said to assume it.[133] In addition, a plaintiff who is aware of a danger "does not assume the risk if the danger appear[s] to him to be so slight as to be negligible."[134] It goes without saying that neither Greenwood nor Smith consented to the government examining their effects or third party disclosure to the government. Moreover, though they may have been aware of the possibility of third party disclosure, they likely thought that the danger of exposure to the government or public was negligible.[135] To be sure, it is difficult to understand how the Court could have thought that Greenwood's consent was determinative given that, by statute, he was required to convey his trash to a third party.[136] As Justice William Douglas points out, "It is idle to speak of 'assuming' risks in context where, as a practical matter, individuals have no realistic alternative."[137]

Perhaps the Court believed Smith and Greenwood failed to take reasonable privacy precautions, adopting more of a contributory negligence rationale.[138] However, a person is only contributorily negligent when his action is unreasonable under community standards. It is not wrongful or unreasonable to use the telephone for communications or put out trash for collection, as opposed to using methods that do not require third party services. In fact, using the telephone to communicate and using city trash disposal services are necessary, socially acceptable, and even desirable.[139] The Court did

pattern of protection would be dictated by billing practices of a private corporation." *Id.* at 745.

[132] *See* RESTATEMENT (SECOND) OF TORTS § 496D cmt. b (1965) (stating that "the basis of assumption of risk is the plaintiff's consent to accept the risk").

[133] *Id.* § 496D (noting plaintiff must "know[] of the existence of the risk and appreciate . . . its unreasonable character").

[134] *Id.* § 496D cmt. b.

[135] *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (admitting that Greenwood likely believed his trash would not be exposed); *Smith*, 442 U.S. at 742 (establishing only that people "presumably have some awareness of one common [pen register] use: to aid in the identification of persons making annoying or obscene calls").

[136] *See Greenwood*, 486 U.S. at 54-55 (Brennan, J., dissenting) ("Greenwood can hardly be faulted for leaving trash on his curb when a county ordinance commanded him to do so." (citing ORANGE COUNTY CODE § 4-3-45(a) (1986))).

[137] *Smith*, 442 U.S. at 750 (Marshall, J., dissenting).

[138] *See* RESTATEMENT (SECOND) OF TORTS § 463 cmt. b ("Contributory negligence is conduct which involves an undue risk of harm to the person who sustains it.").

[139] *See Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (characterizing telephone as

not explain why an individual should suffer disabilities for doing things that it otherwise encourages people to do.[140]

Instead, the Court elucidated an amoral risk assumption theory that goes something like this: if there is some risk of third party disclosure to the government, no matter how unlikely and regardless of whether third party exposure was necessary or preferred, you have no privacy interest.[141] Even worse, the Court has made clear that this rigid third party analysis holds even when the third party has guaranteed confidence.[142] This doctrine quite obviously has potential to completely undermine Fourth Amendment privacy protection. Everyday, we expose private information, in differing limited capacities, to persons of trust and essential service people. Meter readers visit our backyards; cleaning people organize our underwear drawers;[143] mail carriers temporarily possess our letters;[144] and maintenance persons fix pipes in our sinks.[145] Under the third party doctrine, the possibility of disclosure from these parties renders all of our homes and belongings subject to governmental intrusion.[146]

"personal or professional necessity").

[140] *Id.* ("[W]hether privacy expectations are legitimate within the meaning of *Katz* depends not on the risks an individual can be presumed to accept when imparting information to third parties, but on the risks he should be forced to assume in a free and open society."); *see also* Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 400 (1997) ("[W]e only assume those risks of unregulated government intrusion that the courts tell us we have to assume.").

[141] *See* Gutterman, *supra* note 12, at 671-72 (noting that assumption of risk cannot "be rationalized in terms of *Katz*'s central theme: restraining government from intruding too easily into people's lives").

[142] *See* United States v. Miller, 425 U.S. 435, 443 (1976) (upholding third party doctrine where defendant revealed information "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed").

[143] *Cf.* Stoner v. California, 376 U.S. 483, 489 (1964) (finding reasonable expectation of privacy in hotel room despite access by cleaning personnel and others).

[144] *Cf.* United States v. Jacobsen, 466 U.S. 109, 114 (1984) (holding that "packages are in the general class of effects in which the public at large has a legitimate expectation of privacy"); *Ex parte* Jackson, 96 U.S. 727, 733 (1877) (finding reasonable expectation of privacy in sent mail).

[145] *Cf.* Chapman v. United States, 365 U.S. 610, 616-18 (1961) (holding landlord's ability to access rented house did not destroy tenant's reasonable expectation of privacy). *But see* United States v. Hinton, 222 F.3d 664, 675 (9th Cir. 2000) (finding no reasonable expectation of privacy in content of postal lockers maintained at post office); United States v. Osunegbu, 822 F.2d 472, 479 (5th Cir. 1987) (finding that defendant had no reasonable expectation of privacy in content of locked rental mailbox because rental manager had access to mail for purposes of sorting).

[146] *See* Stephen E. Henderson, *Nothing New Under the Sun? A Technologically*

Today, the only thing preventing the third party doctrine from totally destroying privacy is the near brightline protection the Court normatively affords to homes and tangible items.[147]

Although their conclusions about privacy rest on several grounds, *Greenwood* and *Smith* have become synonymous with a simplistic and broad version of the third party doctrine. They establish the principle that any disclosure to any third party, whether a fiduciary or temporary custodian, destroys an individual's privacy interest. Remember, however, "[i]n *Katz*, the phone company . . . no doubt had the technical ability to hear the contents of [*Katz*'s] call. That technical ability, however, was no impediment to the Court's conclusion that *Katz* had an expectation of privacy in the conversation."[148] The third party doctrine twists the *Katz* test into a mechanism that undermines privacy. In *Greenwood*, reasonableness is used to declare an individual's socially acceptable expectations regarding intimate objects constitutionally irrelevant.

B. The Third Party Doctrine in the Cyberworld

It is well-recognized that the third party doctrine has the potential to significantly impact privacy interests regarding a wide variety of information conveyed over the Internet or relevant to Internet subscription.[149] Because the Court has provided meager guidance in

Rational Doctrine of Fourth Amendment Search, 56 MERCER L. REV. 507, 546 (2005) (criticizing third party doctrine because "it treats privacy as an indivisible commodity — once information is given to any one party for any one purpose, it is treated as if it were given to every person for any possible purpose"); Andrew J. DeFilippis, Note, *Securing Informationships: Recognizing a Right to Privity in Fourth Amendment Jurisprudence*, 115 YALE L.J. 1086, 1108 (2006) (noting that third party doctrine "conceives of privacy as an on/off switch, whereby an individual's disclosure of information relegates his Fourth Amendment claims to the constitutional darkness").

[147] For a discussion of the bright line rule governing home searches, see *supra* note 33; *infra* note 322.

[148] Patricia Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1405 (2004) (citation omitted).

[149] *See* Bellia, *supra* note 148, at 1429 (suggesting that click stream might not be protected because of exposure on third party server); 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, 1211 (2004) (observing that even email content might not be protected under third party doctrine); Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1118 (2006) (noting privacy ramifications of third party doctrine in Internet arena); Solove, *supra* note 6, at 755 (suggesting that Court might find stored emails and ISP information unprotected under third party doctrine); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357,

the area, Congress has stepped in to regulate the interception and monitoring of Internet communications and activities through the Electronic Communications Privacy Act ("ECPA").[150] Yet the fact that Congress has, to some extent, tempered the problems caused by the third party doctrine should provide little solace to the concerned civil libertarian. Congress is perhaps not in the best position to police civil liberties, especially during times of moral panic over terrorism and pedophilia.[151] Moreover, statutes often provide little incentive for law enforcement compliance given their weak remedial mechanisms.[152] However, this is not an essay about institutional competence. Thus, whether or not Congress is willing to fulfill the legacy of *Katz* is beside the point.[153] This section looks at the implications of the third party doctrine in the modern world and shows how far courts have come from the *Katz* revolution.

1. Internet Subscriber Information

Internet subscriber information includes information that Internet account purchasers give to provider companies (ISPs) and certain information collected by ISPs, which the subscriber may be unaware it maintains. For billing purposes, Internet providers collect customers'

377 (asserting that because of third party doctrine, Fourth Amendment is often inapplicable in Internet context).

[150] *See supra* note 124 (discussing ECPA).

[151] *See* Will Thomas DeVries, *Protecting Privacy in the Digital Age*, 18 BERKELEY TECH. L.J. 283, 297-307 (2003) ("[L]egislatures are unlikely to impose many new limits on government misuse of personal information in the current atmosphere of heightened national security and fear."). Indeed, the provisions of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot Act") makes government monitoring of communications easier. Pub. L. No. 107-56, 115 Stat. 272 (Supp. 2001) [hereinafter Patriot Act]. *See, e.g.,* Patriot Act § 209 (treating voicemail like stored email rather than conversation); *id.* § 216 (treating email header information like phone numbers); *see also* Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 917-18 (2004) (suggesting that Congress is unlikely to be spurred on by novel privacy-defeating court decisions, given low judicial threshold for privacy protection).

[152] *See, e.g.*, 18 U.S.C. § 2518(10)(a), (c) (1994 & Supp. IV 1999) (codifying ECPA's explicit exemption of electronic communications from statutory remedy); *see* Freiwald, *supra* note 124, at 83 (noting lack of statutory suppression remedy in ECPA).

[153] For a thorough and spirited debate of this issue, compare Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (arguing in favor of statutory rather than constitutional regulation of surveillance involving modern technology), with Solove, *supra* note 6, at 747 (opposing Kerr's view).

names, addresses, telephone numbers, and credit card information.[154] In addition, ISPs keep records on subscribers' login and user names, passwords, and IP addresses, a number that uniquely identifies a computer for the purposes of server exchanges.[155]

Typically, the subscriber information issue arises when police observe an individual, identified by an anonymous username, engaging in illegal activity on the Internet, often involving child pornography or solicitation. The police then request information from the ISP to match the username to an actual computer, name, and address.[156] This request for information is often in the form of a subpoena or court order, but not always in the form of a warrant based on probable cause.[157] Of course, targets of such investigations argue that obtaining their subscriber information absent probable cause and a valid search warrant violates the Fourth Amendment.[158]

Lower federal courts and state courts interpreting the U.S. Constitution have analyzed this claim in two ways. Some courts hastily dismiss the claim that there is a reasonable expectation of privacy on the sole ground that a third party, the ISP, has access to the information.[159] Others are more attuned to the nature of the information provided, holding that there is no reasonable expectation of privacy because the information sought is noncontent information.[160] The first type of analysis is incredibly dangerous as it

---

[154] *See* United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000) (noting that "when Mr. Hambrick entered into an agreement to obtain Internet access from MindSpring, he knowingly revealed his name, address, credit card number, and telephone number").

[155] *See* United States v. Kennedy, 81 F. Supp. 2d 1103, 1106 n.3 (D. Kan. 2000) ("The IP, or Internet Protocol, address is unique to a specific computer.").

[156] *See, e.g.*, United States v. Sherr, 400 F. Supp. 2d 843, 846 (D. Md. 2005) (agents discovered child pornography had been sent to Carols459@aol.com and requested his identifying information from AOL); *Hambrick*, 55 F. Supp. 2d at 504-05 (defendant solicited agent posing as minor under username "blowuinva" and government obtained information from ISP MindSpring to identify "blowuinva").

[157] *See, e.g., Sherr*, 400 F. Supp. 2d at 846 (administrative summons); *Kennedy*, 81 F. Supp. 2d at 1107 (court order); *Hambrick*, 55 F. Supp. 2d at 506 (invalid warrant).

[158] *See, e.g.*, *Hambrick*, 55 F. Supp. 2d at 506 (defendant asserted reasonable expectation of privacy in his ISP information).

[159] *See, e.g.*, *id.* at 508-09 (holding that defendant was not entitled to expect his web surfing and username to be anonymous because MindSpring employees had access to information identifying him); *see also* State v. Reid, 914 A.2d 310, 313 (N.J. Super. Ct. App. Div. 2007) (asserting that cases finding ISP information unprotected "followed inexorably from Supreme Court precedent which 'consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties'" (quoting Smith v. Maryland, 442 U.S. 735, 743-44 (1979))).

[160] *See, e.g.*, *Sherr*, 400 F. Supp. 2d at 848 (finding no reasonable expectation of

opens the door to undermining the privacy of the content of electronic communications, click stream activity, stored documents, or any other items to which an ISP might have access. The second line of analysis, while less dangerous, greatly expands the third party doctrine to include information far more intimate than the phone numbers involved in *Smith*.

Turning to the latter approach first, these cases seem to follow the promising strain of analysis in *Smith* by distinguishing between content and noncontent information.[161] Under this approach, courts find that ISP information is not content related, and thus, like telephone numbers, may be obtained by the government.[162] Nonetheless, Justice Brennan criticized *Smith* on the ground that telephone numbers "easily could reveal the identities of the person and the places called, and thus reveal the most intimate details of a person's life."[163] While telephone number information, upon further investigation, might lead to the revelation of private and embarrassing facts, compromising the anonymity of an Internet user *immediately* reveals information about his associations and predilections.[164] In other words, ISP information is inherently content based because it instantly divulges to the government the websites the user has viewed, chats in which he has participated, and emails he has sent.[165]

As with garbage, the important privacy value is not necessarily the immunity of Internet activity from public viewing, but the protection of that activity from being linked with an identity.[166] Anonymity is at the heart of our expectations of privacy and potential for creativity on the web.[167] For this reason, the average person would likely be far

privacy in noncontent ISP information).

[161] *See* Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181-82 (D. Conn. 2005) (noting that courts have found Fourth Amendment privacy to depend on whether interception of electronic communication involves content); *Sherr*, 400 F. Supp. 2d at 848.

[162] *See Freedman*, 412 F. Supp. 2d at 181-82.

[163] *Smith*, 442 U.S. at 748 (Stewart, J., with whom Brennan, J., joins, dissenting).

[164] *See* Freiwald, *supra* note 124, at 48 ("In the context of traditional wiretapping, there is not much besides the contents of communications to be acquired. But in the online context, communication attributes convey rich information.").

[165] *Cf.* Konop v. Haw. Airlines, Inc., 236 F.3d 1035, 1044-46 (9th Cir. 2001) (holding that secure website information is "electronic communication" under ECPA).

[166] *See supra* text accompanying notes 106-07 (discussing value of anonymity).

[167] *See* Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 818 (1995) (asserting that Internet anonymity promotes political speech on web); Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 301 (2001) ("Privacy enables

more agitated over someone looking at his click stream or knowing his online identity than someone reading his phone records.[168] Courts, however, seem to virtually ignore the value of anonymity, holding in effect that because of ISP exposure, communicating in a chat room under a username is the same as shouting the conversation in a public square.[169] Nonetheless, at least the cases embracing the content/noncontent distinction preserve the possibility that the substance of Internet communications may be protected.

Unfortunately, another line of ISP cases adopts *Greenwood*'s strict third party doctrine. They hold subscriber information is unprotected on the sole ground that such information is "revealed" to a third party.[170] For example, in *United States v. Kennedy*, the Kansas district court, citing *Smith* and *Greenwood*, broadly observed that "[w]hen defendant entered into an agreement for Internet service, he knowingly revealed *all* information connected to the IP address 24.94.200.54"[171] and summarily concluded "[h]e cannot now claim to have a Fourth Amendment privacy interest."[172] The problem is that although some minority of Internet subscribers might be passively aware of the type of information exposed to an ISP employee, even those users certainly do not intend for ISP employees to reveal their usernames to the world or follow them on the web.[173] Moreover, the

anonymity and anonymity is privacy realized."); Sonia K. Katyal, *The New Surveillance*, 54 CASE W. RES. L. REV. 297, 315 (2003) ("Perceptions of anonymity in cyberspace have enabled a level of participation in public discourse unlike anything before. . . .").

[168] *Cf.* United States v. Allen, 53 M.J. 402, 409 (C.A.A.F. 2000) (observing that click stream information lies somewhere between (protected) content of emails and (unprotected) subscriber information).

[169] In *United States v. Hambrick*, the Court called the defendant "not a completely anonymous actor" because of ISP exposure even though the court recognized that "[i]t is true that an average member of the public could not easily determine the true identity of 'Blowuinva.'" 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

[170] *See* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001); United States v. McClure, No. 1L05-CR-140, 2006 WL 89859, at *1-2 (E.D. Tenn. Jan. 13, 2006); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); *In re* Property of Forgione, 908 A.2d 593, 607-08 (Conn. Super. Ct. 2006); Hause v. Commonwealth, 83 S.W.3d 1, 11-12 (Ky. Ct. App. 2001). This is true even when the ISP has specifically stated that it would not divulge personal information. *See, e.g.*, Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005) (finding no reasonable expectation of privacy despite AOL's nondisclosure policy).

[171] 81 F. Supp. 2d at 1110 (emphasis added).

[172] *Id.*

[173] *See* Katyal, *supra* note 167, at 350 (noting that these cases create "troubling

particular danger is that these cases pave the way for holding that content of private electronic communications is not protected because of ISP access.

2. Electronic Communications Content

There are a number of ways individuals communicate over the Internet. Some are public, for example, creating a public website,[174] posting a public bulletin,[175] or engaging in a public chat.[176] Many other modes of communication over the web are essentially private. Email, for example, is a written message typically intended for an individual recipient or group of recipients, and not for general public viewing. Emails are transmitted over the Internet, and saved emails may be stored on the Internet itself or remotely by an ISP.[177] ISP workers and system administrators have limited ability to access private emails with effort, much in the way that phone company employees could listen to conversations or mail carriers could read private mail.[178] Individuals also communicate privately over the Internet via instant message or private chat, in which communications are written in real time,[179] or by Internet telephone services like

contradiction" that individuals "expect anonymity, even when engaging in illicit activities that are open to private surveillance"). To the extent that people actually fear that ISPs monitor their click streams, it may be because of government manipulation. *See* Anne Broache, *Attorney General to Talk Data Retention with New Congress*, CNETNEWS.COM, Jan. 18, 2007, http://news.zdnet.com/2100-9588_22-6151325.html (noting that former Attorney General Gonzalez urged legislation to require data monitoring by ISPs).

[174] *Cf.* J.S. *ex rel.* H.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 425 (Pa. Commw. Ct. 2000) (finding no reasonable expectation of privacy in contents of public website).

[175] *Cf. Guest*, 255 F.3d at 333 (finding no reasonable expectation of privacy in messages posted on public Internet bulletin).

[176] *Cf.* United States v. Maxwell, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (finding no reasonable expectation of privacy in messages "sent to the public at large in the 'chat room'").

[177] *See* Freiwald, *supra* note 124, at 45-46 (explaining route email takes from sender server to recipient server).

[178] First, "random monitoring except for mechanical or service" is prohibited by statute. *See* 18 U.S.C. § 2511 (2000 & Supp. I 2002). Second, there are practical difficulties to reading email content. *See* Joseph Z. Fleming, *Ethical Issues Relating to Airline and Railroad Labor and Employment Law: Overview*, SL040 ALI-ABA 1091, 1187-88 (2006) ("Because the specific route taken by each email message through the labyrinth of phone lines and ISPs is random, it would be very difficult consistently to intercept more than a segment of a message by the same author.").

[179] One court found that although state privacy law is violated when agents surreptitiously record phone calls, an agent's surreptitious interception and storing of

"Skype."[180] Finally, individuals may move from a public communication forum, like a website, bulletin, or public chat room, to a private forum, such as email, instant message, or private chat room. It is common for individuals to engage in a general discussion in a public chat room, and then move to a private room for more intimate discussions.

These private communications are hardly different than phone conversations or letters.[181] Regarding instant messages and Internet telephone conversations, we no more expect that third parties are listening in, whether governmental- or ISP-employed, than we would expect third parties to listen in on our telephone or cell phone conversations. Likewise, we no more think that ISP administrators or web hackers access our personal emails than we believe that mail persons or snoops read our letters.[182] Nonetheless, when it comes to web communications, courts seem more than willing to make up a whole new set of rules intensifying the third party doctrine to new scope.[183]

Courts have expressed a tentative willingness to find no expectation of privacy in the content of emails and chat room exchanges because

an instant message is not violative. *See* State v. Lott, 879 A.2d 1167, 1172 (N.H. 2005).

[180] Unlike cordless phones in their infancy, Internet phone services are now encrypted and not easily intercepted. *See* David Alan Jordan, *Decrypting the Fourth Amendment: Warrantless NSA Surveillance and the Enhanced Expectation of Privacy Provided by Encrypted Voice over Internet Protocol*, 47 B.C. L. REV. 505, 530 (2006) (noting that "today's encrypted [Internet phone] conversations are practically indecipherable, even by the most sophisticated professionals"); *infra* text accompanying note 300.

[181] *See* Sklansky, *supra* note 6, at 199 (noting that cyberspace has been described to include zone we occupy when communicating over phone).

[182] *See supra* notes 166-68 and accompanying text (discussing anonymity on web). Perhaps one could argue that we do expect our private emails and instant messages to be read by hackers and system administrators. *See* Bellia, *supra* note 148, at 1386 (noting argument that "we are conditioned to presume the vulnerability of our electronic communications at various points on the Internet to hackers"). Not only is this disputable, but also our lowered expectations may be a product of propaganda "from companies seeking to promote network security products, by employers who announce monitoring policies to deter misuse of network access, and by service providers who seek to disclaim liability for security breaches." *Id.* at 1387.

[183] The Eighth Circuit has indicated broadly in dicta that email simply might not be protected by the Fourth Amendment at all. *See* United States v. Bach, 310 F.3d 1063, 1066 (8th Cir. 2002). One court went so far as to say that allowing a private individual to use your email account renders invalid any claim that the account is private. *See* State v. Kaufman, No. 32007-0-II, 2005 WL 2746676, at *3 (Wash. App. Oct. 25, 2005) ("Having voluntarily allowed a third person access to his Comcast account, Kaufman cannot now claim a privacy expectation.").

of ISP access, thus extending the third party doctrine well into the area of content.[184] At least one case, *United States v. Maxwell*, found email sent from a private AOL account protected by the Fourth Amendment, like postal mail.[185] Even that case, however, took pains to mention email always runs "the risk that an employee or other person with direct access to the network service will access the email, despite any company promises to the contrary."[186] In addition, the court specified that a message forwarded to several people might lose its protected character.[187] Other courts have indicated in dicta that, because of third party exposure, email content is of lesser protected status than mail or telephone content[188] or possibly not protected at all.[189] Such courts thus hold that the privacy of email depends, not on social expectation or whether content is at issue, but on the fact of third party access.[190]

To be fair, many of the cases dealing with the unwarranted seizure of email find no Fourth Amendment protection because the email originated from a work account openly monitored by the employer.[191]

---

[184] *See, e.g.*, *Bach*, 310 F.3d at 1066 (asserting that it is unclear that there is constitutional expectation of privacy in emails); McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015, at *4 (Tex. App. May 28, 1999) (asserting defendant's stored emails differed from tangible stored items because such emails were "first transmitted over the network and were at some point accessible by a third party").

[185] United States v. Maxwell, 45 M.J. 406 (C.A.A.F. 1996). Unfortunately, at least one lower court has noted that *Maxwell* "has little or no precedential value because the United States Court of Appeals for the Armed Forces decided the case." United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999).

[186] *Maxwell*, 45 M.J. at 418. The Court, however, concluded that "this is not the same as the police commanding an individual to intercept the message." *Id.*

[187] *Id.* This is akin to saying that the government may wiretap a conference call because it involves several people or that if a conversant allows other private citizens to listen to a conversation, then the government, without consent, can listen as well. In addition, the court made much of the fact that the emails were stored on a remote server rather than on the web itself. *Id.*

[188] *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (1997) (finding only "a limited reasonable expectation of privacy" in email messages and observing that "[w]hen an individual sends or mails letters, messages, or other information on the computer, that Fourth Amendment expectation of privacy diminishes incrementally").

[189] *Bach*, 310 F.3d at 1066.

[190] This is of particular concern because emails often go through different stages of exposure to and accessibility by third parties. *See* Freiwald, *supra* note 124, at 45-46.

[191] *See, e.g.*, United States v. Zeigler, 456 F.3d 1138, 1145-46 (9th Cir. 2006); Biby v. Bd. of Regents, 419 F.3d 845, 850-51 (8th Cir. 2005); United States v. Thorn, 375 F.3d 679, 683 (8th Cir. 2004), *cert. granted and judgment vacated on other grounds by* 543 U.S. 1112 (2005); United States v. Angevine, 281 F.3d 1130, 1133-35 (10th Cir.

Courts rule that that there is no reasonable expectation of privacy in a work email just as there is no reasonable expectation of privacy in a work locker, when the employer has a policy of random locker searches.[192] Yet even knowing that bosses and IT people read our work emails, we have to catch ourselves because one's instinct is that what she writes in the little box is private. Moreover, the practice of bosses reading private email seems no less iniquitous than bosses listening to phone conversations that originate from an office phone or reading mail left for postal pickup at the office.[193] It also bears noting that work email accounts often serve as individuals' primary private email accounts as well.

Even more disturbing, when dealing with web communications, some courts tend to mélange the third party doctrine from *Greenwood* and *Smith* with the consensual wiretap doctrine from *United States v. White*[194] and *Hoffa v. United States*.[195] *White* and *Hoffa* stand for the proposition that individuals possess no reasonable expectation of privacy against government agents posing as nonagent conversants and contemporaneously recording conversations.[196] It is fairly uncontroversial that when a private person violates a confidence by recording a conversation and transmitting it to the police, there is no constitutional problem because it is only private action.[197] The more complicated issue is whether there is a constitutional violation when

2002); Muick v. Glenayre Elecs., 280 F.3d 741, 743 (7th Cir. 2002); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000); *see also* United States v. Geter, No. NMCM 9901433, 2003 WL 21254249, at *3 (N-M. Ct. Crim. App. May 30, 2003) (holding that government employee has no reasonable expectation of privacy in government email account provided only for official use).

[192] This does not necessarily hold for similar searches in the absence of such an employer policy. *See, e.g.*, United States v. Slanina, 283 F.3d 670, 676-77 (5th Cir. 2002), *vacated on other grounds by* 537 U.S. 802 (2002), *appealed after remand* 359 F.3d 356 (5th Cir. 2004) (per curiam); Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001).

[193] *But see Zeigler*, 456 F.3d at 1145-46 ("Employer monitoring is largely an assumed practice.").

[194] 401 U.S. 745 (1971).

[195] 385 U.S. 293 (1966).

[196] *White*, 401 U.S. at 751 (holding that co-conversant's trustworthiness is something "the defendant necessarily risks"); *Hoffa*, 385 U.S. at 302 (holding that Fourth Amendment does not protect "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

[197] In many states, however, such action amounts to a criminal offense. *See, e.g.*, CAL. PENAL CODE § 632 (West 2007); Fla. Stat. Ann. § 934.03(3)(d) (West 2002); MD. CODE ANN., CTS. & JUD. PROC. § 10-402(C)(3) (West 2006); 18 PA. CONS. STAT. ANN. § 5703 (West 1988).

one converses with someone clandestinely acting as a state agent. The Court has held that it is unreasonable to expect our conversations to be exempt from such monitoring because we must assume the risk that our fellow conversants are wired undercover agents.[198] However, it seems that the majority of us, in fact, generally believe our co-conversants are not secret government agents.[199] Moreover, even if that expectation is somehow atypical, there is a normative argument that society members should be able to feel comfortable that in any given conversation they are not being literally and figuratively duped by government agents.[200] Consequently, the *White/Hoffa* doctrine itself can be seen as a departure from the spirit of *Katz*.

Nonetheless, the *White/Hoffa* doctrine is narrower than the third party doctrine in the sense that a person loses constitutional protection only when his fellow conversant actually *does* breach a confidence. Under the third party doctrine, an individual looses protection simply when there is a risk, no matter how minimal, that the third party *might* breach the confidence.[201] If conversants are treated like third parties under *Greenwood*, no conversation could ever be protected by the Constitution because the potential always exists that a fellow conversant *might* breach our confidences. Consequently, to mix *White/Hoffa* and *Greenwood* would patently undermine *Katz*'s holding that the content of conversations is protected.[202]

Unfortunately, in the Internet context, lower courts have done exactly this. When an individual chats directly with an agent privately on the Internet, courts could simply dispose of the issue by invoking

---

[198] *See White*, 401 U.S. at 751; *Hoffa*, 385 U.S. at 302.

[199] *See White*, 401 U.S. at 790 (Harlan, J., dissenting):

> [T]he expectation of the ordinary citizen . . . [is] that he may carry on his private discourse freely, openly, and spontaneously without measuring his every word against the connotations it might carry when instantaneously heard by others unknown to him and unfamiliar with his situation or analyzed in a cold, formal record played days, months, or years after the conversation.

[200] *Id.* at 785 (rejecting that "uncontrolled consensual surveillance in an electronic age is a tolerable technique of law enforcement"); *see also* Gutterman, *supra* note 12, at 670 ("In searching for 'assumption of risks,' *White* missed the mark. It overlooked the central issue, the significance of this type of electronic surveillance as a threat to our sense of security.").

[201] *See supra* notes 115-16, 128-31 and accompanying text (discussing third party doctrine in *Greenwood* and *Smith*).

[202] Professor Bellia notes, "*Katz*'s co-conspirator could have revealed the contents of the communication at any time to police. His mere ability to do so was not thought to eliminate *Katz*'s expectation of privacy." Bellia, *supra* note 148, at 1405.

White/Hoffa and asserting that one has no expectation of privacy vis-á-vis the behavior of a fellow conversant.[203] However, courts go further and argue broadly that there is no reasonable expectation of privacy in a chat room because fellow chatters have the potential to breach confidences. For example, in *United States v. Charbonneau*, a police agent became a member of a private chat room for surveillance purposes and, as a member, received an email addressed to all chat room participants containing illegal images.[204] Although the court recognized that communications directly to the agent are not protected under *Hoffa*,[205] it went on to hold broadly that the defendant "could not have a reasonable expectation of privacy in the chat rooms [such that] the email sent by Defendant to others in a 'chat room' is not afforded any semblance of privacy."[206]

Courts reason that private chat room conversations are not protected because fellow conversants are anonymous and have the potential to betray confidences.[207] However, if one were to meet someone on the Internet and then call her on the phone, such a conversation would not be un-private merely because the new friend has not revealed her "true" name. Nonetheless, these courts deem private chat rooms unprotected simply because there is a potential that an anonymous conversant may breach confidences. This paves the way for holding that private chat room or instant message conversations may be monitored by the police, even when none of the participants has consented to interception.

In the end, *Smith*, *Greenwood*, and their progeny far removed *Katz* from its civil libertarian roots. Instead of determining typical expectations or normative privacy values, these cases rely on a

---

[203] *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184 (D. Ohio 1997) (holding that "a sender of email runs the risk that he is sending the message to an undercover agent").

[204] *Id.* at 1179-80.

[205] *Id.* at 1184.

[206] *Id.* at 1185.

[207] *See, e.g.*, State v. Turner, 805 N.E.2d 124, 132 (Ohio Ct. App. 2004) (stating that "when parties make contact in a chat room, a private box opens up so that they can have a conversation only with each other (instant messaging) [but] that still did not give Turner an expectation of privacy, since he was chatting with a stranger, not a known acquaintance"); State v. Moller, No. 2001-CA-99, 2002 WL 628634, at *5 (Ohio Ct. App. Apr. 19, 2002) (asserting that "individuals possess no reasonable expectation of privacy in statements made to an unknown individual over the Internet"); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001) (finding no Fourth Amendment protection because "[w]hen Appellant engaged in chat-room conversations, he did not know to whom he was speaking").

capricious and unjustified analysis of risk assumption. The damaging potential of the third party doctrine can be seen in Internet cases, where very minimal and limited third party exposure was the dispositive factor in denying protection in a vast array of intimate communications. Notwithstanding society's actual expectations of web privacy, courts tend to treat web communications as less private than letters or phone calls, perhaps because of an instinct that third parties are more essential to Internet communication or an overblown belief in the prevalence of hackers.[208] The neo-*Greenwood* legal regime tells us, not only should we expect others to be reading personal emails, but also we ought to live in a world where curious ISP employees, hackers, snoops, and the government can access our private thoughts.

III. PUPPY DOG TAILS

Although *Illinois v. Caballes* is not as fundamentally damaging to the *Katz* regime as *Greenwood* and related cases, it still illuminates how manipulative the Court can be in order to serve crime control goals. The *Caballes* Court considered whether police can employ a narcotics dog to sniff a car for drugs after a routine traffic stop to issue a traffic violation without probable cause or reasonable articulable suspicion.[209] Because of the many permutations of the case, some do not regard *Caballes* as requiring application of the *Katz* test.[210] Indeed, the Court introduced a seizure analysis, noting that the dog sniff did not extend the *Terry* stop beyond the time it took for the officer to issue the ticket.[211] It is true that the Court might have attempted to resolve the

[208] *See* Freiwald, *supra* note 124, at 11 nn.6-7 (citing studies revealing that we engage in intimate communication on web without taking precautions like encryption); Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1646 (1999) ("Those who make comments in 'chat rooms' or 'list servs,' or who simply visit Web sites, are . . . likely to have . . . mistaken beliefs regarding the specific level of disclosure of personal data involved in their activities."); 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, 737 (1993) (conducting study and finding that people consider computer searches highly intrusive).

[209] Illinois v. Caballes, 543 U.S. 405, 407 (2005).

[210] *Cf. Caballes*, 543 U.S. at 421 (Ginsburg, J., dissenting) (criticizing Court's decision because of intrusive nature of dog sniff from seizure standpoint).

[211] *Id.* at 408 (majority opinion) (noting that trial court found "the duration of the stop in this case was entirely justified by the traffic offense and the ordinary inquiries incident to such a stop"). A *Terry* stop is a brief stop, like a traffic stop, which is less intrusive than an arrest and justified by reasonable articulable suspicion rather than

issue under a *Terry* analysis, holding, similar to *Pennsylvania v. Mimms*,[212] that a dog sniff is one in the "bundle of abilities" police retain by virtue of making a traffic stop. This, however, would have been difficult because a drug dog sniff, unlike removing the driver from a car, as in *Mimms*, is not a necessary safety precaution.[213] Consequently, the Court had to strain for a justification of the canine search beyond the general go-to justification of officer safety used in most traffic stop cases.[214] It did so by holding that the sniff was not a search because there is no "legitimate" expectation of privacy in contraband.[215] As a result, the Court's principal resolution of the dog sniff issue is an interpretation of the *Katz* test that creates the potential to erode privacy in the most intimate places given increasingly refined technology.

A. The Manipulation: Reasonableness as External Legitimacy

The issue before the *Caballes* Court was whether the dog sniff itself was a search within the meaning of the Constitution, requiring independent justification. Under the *Katz* regime, the Court should have resolved the question by determining whether Caballes had an actual and reasonable belief that the contents of his car were private, or, more specifically, immune from a dog sniff.[216] The Court did not address Caballes's subjective belief, but one could fairly assume that he did not expect a dog to sniff his car when he was pulled over for speeding. As to the reasonableness prong, the Court did not determine whether society at large considers automobiles to be impervious to such intrusion or decide whether we ought to be so secure. Rather, the Court broadly held that a dog sniff is sui generis because it is "likely to reveal only the presence of contraband" and "any interest in possessing contraband cannot be deemed 'legitimate.'"[217] This brand of Fourth Amendment logic can be traced to an influential 1983 law review article by Professor Arnold Loewy,

probable cause. *See* Terry v. Ohio, 392 U.S. 1, 10 (1968).

[212] 434 U.S. 106, 111 (1977) (holding that police officers without any basis could order driver out of car after routine traffic stop).

[213] *Id.* at 110 (finding interest in officer safety "both legitimate and weighty").

[214] *See id.*; Maryland v. Wilson, 519 U.S. 408, 414 (1997) (applying *Mimms* rule to passengers); Michigan v. Long, 463 U.S. 1032, 1048 (1983) (finding that reasonable belief of danger during traffic stop justifies search of passenger compartment).

[215] *Caballes*, 543 U.S. at 408-09.

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

[217] *Caballes*, 543 U.S. at 408-09.

which opined, "[O]f course [a criminal] would like to keep to himself the evidence of his crime. But his claim is not a powerful one."[218]

The manipulation ploy was to divert the inquiry from the reasonableness of the privacy expectation to the "legitimacy" of the thing sought by police.[219] Yet today it is an unassailable tenet of criminal procedure that "[a] search prosecuted in violation of the Constitution is not made lawful by what it brings to light."[220] As Justice Ruth Bader Ginsburg pointed out in her *Caballes* dissent, "The Court has never removed police action from Fourth Amendment control on the ground that the action is well calculated to apprehend the guilty."[221] The *Caballes* majority thus answered the wrong question — it analyzed whether Caballes had the right to possess contraband rather than whether every driver has the right to be free from dogs sniffs.[222] As one commentator notes, "Focusing on the police technique as a means to gather limited information about

[218] Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1245-46 (1983); *see also* Sherry F. Colb, *Innocence, Privacy, and Targeting Fourth Amendment Jurisprudence*, 96 COLUM. L. REV. 1456, 1477 (1996) (hypothesizing that existence of magnetic field which prevented police for searching innocent spaces would render "the lack of probable cause or justification for a search . . . largely irrelevant").

[219] *See* George M. Dery III, *Who Let the Dogs Out? The Supreme Court Did in* Illinois v. Caballes *by Placing Absolute Faith in Canine Sniffs*, 58 RUTGERS L. REV. 377, 390 (2006) (asserting that *Caballes* added "a new qualification for legitimacy" to *Katz* test where legitimacy meant "legality"); David A. Harris, *Superman's X-Ray Vision and the Fourth Amendment: The New Gun Detection Technology*, 69 TEMP. L. REV. 1, 38 (1996) (calling legitimacy test "judicial sleight of hand"). Professor Phyllis T. Bookspan traced the move from "reasonableness" to "legitimacy" to *Rawlings*, a standing case in which Justice William Rehnquist denied standing to the defendant, not because she had no socially cognizable expectation of privacy, but because she was not "legitimately" on the premises. Phyllis T. Bookspan, *Reworking the Warrant Requirement: Resuscitating the Fourth Amendment*, 44 VAND. L. REV. 473, 497 (1991). She characterized this judicial move as an example of Rehnquist "adeptly employ[ing] language to mold the law." *Id.* at 498 n.124.

[220] Byars v. United States, 273 U.S. 28, 29 (1927).

[221] *Caballes*, 543 U.S. at 422 (Ginsburg, J., concurring) (citing United States v. Karo, 468 U.S. 705 (1984)); *see also* Minnesota v. Carter, 525 U.S. 83, 110 (1998) (Ginsburg, J., dissenting) ("Fourth Amendment protection, reserved for the innocent only, would have little force in regulating police behavior toward either the innocent or the guilty.").

[222] *See* Gutterman, *supra* note 12, at 710 (asserting that this analysis misses "the *Katz* mark" because although police technique "may disclose only the presence or absence of limited information, it still remains as a method to disclose the contents of private property in a private, enclosed space").

contraband deflects attention away from the critical question: Is uncontrolled dog sniffing the type of intrusion we should tolerate?"[223]

Caballes's manipulation of the reasonableness prong is a departure from the "zone of privacy" analysis accepted both in *Katz* and previous cases.[224] Justice Brennan criticized this doctrinal shift, stating, "In determining whether a reasonable expectation of privacy has been violated, we have always looked to the context in which an item is concealed, not to the identity of the concealed item."[225] Even before *Katz*, *Silverman* held that the fact that conversations were exempt from the Fourth Amendment's umbrella did not preclude a finding that the police's actions were nonetheless a search.[226] *Silverman* made clear that any minor invasion into a protected area, even if to seize an unprotected thing, is a search within the meaning of the Fourth Amendment. One might respond that no such trespass occurred because the dogs did not physically invade defendant's automobile. *Katz*, and later *Kyllo v. United States*, however, confirm that privacy spaces can be invaded by nonphysical means.[227] Indeed, "[a] dog adds a new and previously unobtainable dimension to human perception. The use of dogs, therefore, represents a greater intrusion into an individual's privacy. Such use implicates concerns that are at least as sensitive as those implicated by the use of certain electronic detection devices."[228]

Caballes thus runs directly counter to *Katz*'s liberal proposition that any invasion into an area in which a person has a reasonable expectation of privacy is a search within the meaning of the Constitution. It seeks to subject the *Katz* rule to a caveat that the Fourth Amendment does not apply if the search is narrowly tailored

---

[223] *Id.* at 711.

[224] *See supra* notes 42-50 and accompanying text (asserting that *Katz* did not fully depart from spatial view of privacy).

[225] United States v. Jacobsen, 466 U.S. 109, 138-39 (1984) (Brennan, J., dissenting).

[226] *See supra* notes 32-33 and accompanying text (discussing spatial view of privacy in *Katz*).

[227] *See supra* notes 52-54 and accompanying text; *see also* Gutterman, *supra* note 12, at 709 ("The Court has always framed its analyses in terms of privacy expectations that normally attend the location of the item."). Vestiges of the physical invasion requirement have survived in part because of judicial confusion over the terms "intrusion." *See* Ric Simmons, *From* Katz *to* Kyllo*: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 HASTINGS L.J. 1303, 1319 (2002) (noting that "the tendency of courts to use the term 'intrusive' to apply to both physical invasiveness and degree of prying into private affairs helps to explain why the former has survived so tenaciously as a factor in the Katz test").

[228] United States v. Place, 462 U.S. 696, 719-20 (1983) (Brennan, J., concurring).

only to recover contraband. However, in *Katz* itself, the police were extremely self-conscious, seeking only to monitor conversations involving criminal activity.[229] In this sense, one could argue that the wiretap at issue, like a sniffer dog, was "generally likely to reveal only" incriminating statements, which are "illegitimate."[230] *Katz* vehemently rejected this very line of analysis. In language completely ignored by *Caballes*, the *Katz* majority declared, "[T]his Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end."[231]

Perhaps *Caballes* can be justified as the Court's attempt to assert normatively that dog sniffs do not compromise privacy. The argument is that even if society expects their cars to be exempt from the minimal intrusion of dog sniffs, such a belief is unreasonable because dog sniffs only uncover contraband and are not intrusive. This is, however, still a problematic judicial move. First, it gives the Court the ability to elevate its own normative privacy-restricting views over the views of a majority of ordinary citizens.[232] Second, it is not necessarily true that the average (innocent) person has no reason to fear a loss of privacy from a dog sniff.

The Court must assume that it is unreasonable for one to expect to be exempt from suspicionless searches that only turn up contraband. The argument that those with nothing to hide should not be concerned about civil rights is a common theme among crime control enthusiasts, but it has been long since debunked by scholars and rejected by Fourth Amendment jurisprudence.[233] It is well established that every

---

[229] Katz v. United States, 389 U.S. 347, 356 (1967) ("It is apparent that the agents in this case acted with restraint . . . .").

[230] Illinois v. Caballes, 543 U.S. 405, 409 (2005) (quoting Brief for the Respondent at 17, Illinois v. Caballes, 543 U.S. 405 (2005) (No. 03-923)).

[231] *Katz*, 389 U.S. at 357-58.

[232] *See infra* text accompanying notes 316-19 (arguing that Court should face high hurdle when elevating its privacy-restricting normative judgments over society's views).

[233] *See supra* notes 220-21 and accompanying text. The author of the *Caballes* opinion, Justice John Paul Stevens, recognized elsewhere:

> [T]hose who have found — by reason of prejudice or misfortune — that encounters with the police may become adversarial or unpleasant without good cause will have grounds for worrying at any stop designed to elicit signs of suspicious behavior. Being stopped by the police is distressing even when it should not be terrifying, and what begins mildly may by happenstance turn severe.

heightened level of police citizen interaction is fraught with risk, even if the citizen is innocent.[234] A sniffer dog, for example, could cause an investigee to react in a manner the police officer deems threatening, leading to the citizen's arrest, injury, or even death. The fact that a dog search could only turn up contraband likely provides little solace to the innocent person who wants to feel secure that such a situation will never happen to her. Even without considering such a dire turn of events, innocent people likely harbor an undifferentiated aversion to government dogs nosing their private spaces. The Court is basically saying that all these people are unreasonable because the only logical reason for any discomfort would be fear of contraband discovery.[235]

Moreover, in order to maintain even facial validity of its normative argument, the Court must be secure in its conclusion that a sniffer dog can only detect contraband. If a sniff search uncovers any evidence of legal activity, then the Court's assertion, that our beliefs about freedom from dog sniffs are unreasonable because innocents have nothing to worry about, unambiguously fails. Justice David Souter points out in the dissent that the infallibility of a dog sniff is a "legal fiction" because the empirical evidence reveals that dogs might very well indicate false positives.[236] The majority summarily dismisses this point, asserting that "an erroneous alert, in and of itself, [does not] reveal[] any legitimate private information."[237] It is true that dog barking is not a human conversation, but it is only uninformative if

Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 465 (1990) (Stevens, J., dissenting).

[234] My former colleague Robert Wilkins, a brilliant African American attorney, and a wonderful, smart, soft-spoken person, in what is now a fairly known case in legal circles, was innocently driving home from his grandfather's funeral with his family when stopped by a police officer and given a search request. Because, among other things, it was the middle of the night, raining, and his family was involved, he declined to consent to the search, to which the officer replied, "If you have nothing to hide, then what is the problem?" The family was detained on the road while a canine unit was called. When the dog finally arrived, Wilkins and his family were pulled out of the car and made to wait in the rain while the dog sniffed around the car. Other events transpired, and a lawsuit was filed and eventually settled favorably to Wilkins and his family. *See* Complaint at 3, Wilkins v. Md. State Police, Civil No. MJG-93-468 (D. Md. 1993), *cited in* Angela J. Davis, *Race, Cops, and Traffic Stops*, 51 U. MIAMI L. REV. 425, 440 n. 97 (1997); Settlement Agreement, Wilkins v. Md. State Police, Civil No. MJG-93-468 (D. Md. 1993), *cited in* Davis, *supra*, at 440 n.99. For a more in-depth discussion of this story, see *id.* at 438-42. Clearly, the damage suffered by the Wilkins family had absolutely nothing to do with the discovery of contraband.

[235] *But see infra* notes 241-42 and accompanying text (illustrating intrusiveness of canine searches).

[236] Illinois v. Caballes, 543 U.S. 405, 411 (2005) (Souter, J., dissenting).

[237] *Id.* at 409 (majority opinion).

viewed in a vacuum. "[I]n practice, the government's use of a trained narcotics dog functions as a limited search to reveal undisclosed facts about private enclosures, to be used to justify a further and complete search of the enclosed area."[238] If fallible, this limited search actually reveals information about noncontraband items that the police will undoubtedly perceive with their own senses.[239] The dog sniff is really no different than the thermal imaging device used in *Kyllo*, which disclosed limited information, not immediately interpretable as an observation, but potentially leading to a privacy-invading inspection. The Court found the use of such a device to be a search.[240]

The *Caballes* Court's argument that dog sniffs are not intrusive is likewise unconvincing. If "intrusive" means physically invading or intimidating,[241] the Court's conclusion that a dog sniff is not intimidating defies common sense. One recent article's hypothetical underscores the menacing nature of this investigative technique:

> Imagine that you are a pedestrian standing on a busy street corner in broad daylight, or a motorist sitting in your car waiting for the light to change, or simply sitting in your parked car. Suddenly, you notice a police officer approaching you with a large black police dog on a tight leash with a muzzle around its jaws. Without uttering a word of warning or explanation . . . the police officer then conducts what is referred to as a "sniff-around," by walking the dog around your person or your car, while the dog sniffs you or your car. Suddenly, the dog stops by your side, its nose close to your leg or your car door and begins pawing at you . . . . On the basis of this alert, the police officer then orders you to surrender your bags or to exit your car and submit to a search. This is not a request; it is a directive that you may not refuse.[242]

---

[238] *Id.* at 413 (Souter, J., dissenting).

[239] That is not, however, the way people feel, with good reason. Some argue that the correct solution to this problem is to prevent courts from equating a positive dog sniff with probable cause for the larger search. *See, e.g.*, Richard E. Myers II, *Detector Dogs and Probable Cause*, 14 GEO. MASON L. REV. 1, 8 (2006). Unfortunately, even this solution falls short of *Katz*'s promise. First, this does not necessarily solve the false positive problem. Moreover, there are still problems with calling our beliefs that we are immune from dog sniffs unreasonable, even if they are assumed to be 100% accurate.

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

[241] Thus, the Court focused on the fact that "the dog sniff was performed on the exterior of respondent's car while he was lawfully seized." *Caballes*, 543 U.S. at 409.

[242] Cecil J. Hunt II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable*

Of course, not every dog sniff will be so intimidating. However, the Court does not differentiate between types of canine sniffs, deeming some intrusive and others benign. Instead, the Court makes a blanket statement that dog sniff's are not searches.

B. Caballes *and New Technologies*

The import of the *Caballes* ruling is that the more investigative techniques are tailored to detect only contraband, the less members of the public, both innocent and guilty alike, can expect to be shielded from their intrusions.[243] Back in 1984, Justice Brennan forewarned that such analysis would prove Orwellian in an age of technology, stating that "if a device were developed that could detect, from the outside of a building, the presence of cocaine inside, there would be no Constitutional obstacle to the police cruising through a residential neighborhood and using the device to identify all homes in which the drug is present."[244] Today, the government has the capability of using and further refining contraband detecting machines.[245] If *Caballes* stands for the broad proposition that there is no search when only contraband is detected, then the government is free to deploy such devices in each and every one of our houses on the ground that if we are innocent, we have nothing to hide.[246] Big Brother could be in all our lives, with the caveat that he only transmit evidence of illegal activity to the government.

Expectations of Privacy, 56 CASE W. RES. L. REV. 285, 285-86 (2005).

[243] Almost 20 years ago, one scholar forewarned of the effects of the Court's dog sniff holding in *United States v. Place*, 462 U.S. 696 (1983): "Brave new worlds in which all passersby are scanned for drugs and police cruising through residential neighborhoods probe all homes with futuristic devices that disclose only whether the offending substance is present come quickly to mind." Junker, *supra* note 107, at 1140.

[244] United States v. Jacobsen, 466 U.S. 109, 138 (1984) (Brennan, J., dissenting).

[245] *See* Steven G. Brandl, *Reflections on the Criminal Justice System After September 11, 2001: Back to the Future: The Implications of September 11, 2001 on Law Enforcement Practice and Policy*, 1 OHIO ST. J. CRIM. L. 133, 148 (2003) (stating that "[i]t is likely that the discovery and adoption of technology for crime detection and investigation purposes will continue to progress at an accelerated 'information age' pace").

[246] There would be no problem with a machine that could scan our papers for evidence of crime, something that would be abhorrent to the Framers and early Court. *See* Boyd v. United States, 116 U.S. 616, 630 (1886) (condemning use of compulsory process to seize papers as "invasion of his indefeasible right of personal security, personal liberty, and private property").

This debate is not merely academic. Every day, crime detection technology advances. Hand-held devices that identify the presence of weapons under clothing are becoming more accurate.[247] Computers now have the capability to cull our Internet communications and transmit to the police only the portions that indicate illegality.[248] Facial recognition technologies are already in use,[249] and "sniffer chips" can detect trace amounts of illegal substances.[250] Under *Caballes*, all these devices could be employed on the sole bases of police hunches, whims, prejudices, or anything at all, because they are beyond the purview of the Fourth Amendment.

Consider the hypotheticals of a camera placed in the home that only transmits images of illegal activities to the police and a device attached to our computers that scans only for illegal files. Some might argue that the use of such devices does not implicate privacy. Professor Orin Kerr, for example, asserts that "a search of data stored on a hard drive occurs when that data, or information about that data, is exposed to human observation."[251] To him, the lynchpin of a violation of privacy is the revelation of information to the human senses of the police. Professor Richard Salgado, combining this notion of privacy with the ruling in *Caballes*, contends the employment of a computer hash program that inspects electronic communications for illegal activity and transmits only information of illegality to the police is not a search under the Fourth Amendment.[252]

What Kerr and Salgado discount is the idea that data-amassing machines, even when collecting "blind," are virtual manifestations of invasive police power, inseparable from human governmental conduct. For this reason, the contention that no search occurs until there is human perception runs counter to typical beliefs about

[247] *See* Laura B. Riley, Comment, *Concealed Weapon Detectors and the Fourth Amendment: The Constitutionality of Remote Sense-Enhanced Searches*, 45 UCLA L. REV. 281, 289-91 (1997) (discussing gun detection technology).

[248] *See* Brandl, *supra* note 245, at 149 (discussing computer programs able to search vast datasets for specific keywords).

[249] *See* Bridget Mallon, Comment, *"Every Breath You Take, Every Move You Make, I'll Be Watching You": The Use of Facial Recognition Technology*, 48 VILL. L. REV. 955, 957-62 (2003) (discussing facial recognition technology).

[250] Brandl, *supra* note 245, at 148 (discussing biometric technologies that can detect trace amounts of illegal substances).

[251] Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 548 (2005).

[252] Richard P. Salgado, *Fourth Amendment Search and the Power of the Hash*, 119 HARV. L. REV. 38, 38 (2005) (stating that "the use of hashing to find only files that constitute contraband does not constitute a Fourth Amendment search").

privacy.[253] Indeed, Kerr admits that "[t]he idea that the government could freely generate copies of our hard drives and indefinitely retain them in government storage seems too Orwellian — and downright creepy — to be embraced as a Fourth Amendment rule."[254] Similarly Salgado states that "there would be something very creepy about an expansive and unrestrained search through media . . . ."[255] I would like to imbue with content our feelings of unease (or "creepiness") at government intrusion geared toward contraband detection.

The *Caballes* Court puts a normative stamp of approval on a world in which police dogs sniff us at will, computers constantly inspect our communications, facial recognition machines scan our features, and contraband detection machines are directed at our homes, cars, and bodies.[256] If, as the Supreme Court believes, none of these actions impinge on legitimate privacy, why does this world appear so unabashedly draconian?

In addition to our awareness of the increased risks associated with police interactions in general, discussed above, we fear such devices because we do not believe in the infallibility of the techniques or incorruptibility of government actors.[257] Even knowing that certain techniques are highly accurate, we might nonetheless think that this one time the technique will fail or a corrupt police person will use the technology in an unfair way.[258] The *Caballes* Court might respond that this is a misplaced concern because the vast majority of the time nothing would go wrong. However, our beliefs about privacy do not necessarily hinge on statistical probabilities. To us, the consequences of a slip up or unethical officer are so dire that the very use of the enabling technique causes us to be insecure in our persons, houses, papers, and effects.[259] Consequently, the assumption that privacy is

[253] *See* United States v. Jacobsen, 466 U.S. 109, 137-38 (1984) (Brennan, J., dissenting) (asserting Orwellian nature of such actions). *But see* Simmons, *supra* note 227, at 1357 (arguing that this "instinctive reaction to such techniques seems misplaced").

[254] Kerr, *supra* note 251, at 560.

[255] Salgado, *supra* note 252, at 38.

[256] *See* Jonathan Zittrain, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83 (2005) (objecting to Kerr's analysis on ground that it permits sweeping governmental action without concurring requirement of judicial oversight).

[257] Indeed, in the cyberworld, this belief is compounded by definitional vagueness regarding illegal web activities. *See* Adler, *supra* note 31, at 1117.

[258] *See id.* at 1112 (asserting that *any* search "that eliminates an individual's control over the boundaries to her most private realms would likely be perceived as a threatening exercise of coercive power").

[259] Justice Harlan has urged that the principle question courts must answer is "the

not implicated by a contraband search not only assumes the infallibility of the detection technology, but the good intentions of those who use it.[260]

Second, even accepting the absolute infallibility of the technique and the ultimate good faith of individual officers, the use of a contraband detection device is still likely to be seen as an invasion of privacy because of our proprietary notions of privacy. When we think of a thing or an area as private, we believe that we control the destiny of that thing or area.[261] We entertain a proprietary notion that the government may not dictate how and when our zones of privacy are monitored, even if such monitoring can reveal only contraband.[262] For example, my proprietary notion of my home dictates that I and I alone determine what may go on in that home.[263] Consequently, everything that happens in my house, even that which is (gulp) illegal, is immune from unwarranted government observation.[264] I may not have the right to commit a crime, but I do have the right to keep criminal evidence in my home a secret.[265] The government may not invade my

likely extent of its impact on the individual's sense of security . . . ." United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

[260] *Katz* made clear, however, that proffered good faith does not adequately substitute for the Fourth Amendment. *See supra* note 231 and accompanying text; *see also* Olmstead v. United States, 277 U.S. 438, 479 (1928) (Brandeis, J., dissenting) ("The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.").

[261] *See* Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2005), *available at* http://www.harvardlawreview.org/forum/issues/119/dec05/ohm.shtml (asserting that private property right includes ability to dispose of property, to erase it from existence at will, and thus copying and preserving data files, even without human perusal, infringes privacy).

[262] *See* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) (defining privacy as "*control* we have over information about ourselves").

[263] *See* Clancy, *supra* note 21, at 368-69 ("The proper question is whether the papers or personal property are mine, whether the house is mine, whether the body is mine? If the answer is yes, then one has the right to exclude the government from searching or seizing.").

[264] I gulp because one would be quick to counter that "[i]f a person has no legitimate interest in concealing wrongdoing, he should also have no legitimate interest in withholding information about whether or not there was any wrongdoing in the first place." *The Supreme Court, 2004 Term — Leading Cases*, 119 HARV. L. REV. 179, 188 (2005). However, it is incorrect to assume that one's desire to be immune from all government surveillance, even surveillance that can only detect illegal activity, is no more than the bare desire to conceal criminal activity. If it were so simple, one could not account for the fact that innocent persons, who have never committed crimes in their lives, do not want to be subjected to such surveillance.

[265] *See* Terry v. Ohio, 392 U.S. 1, 9 (1968) ("No right is held more sacred, or is more carefully guarded, by the common law, than the right of every individual to the

home in the search of contraband, because it would negate an important aspect of what it means for that home to be my private space.[266] *Silverman* put it bluntly:

> A man can still control a small part of his environment, his house; he can retreat thence from outsiders, secure in the knowledge that they cannot get at him without disobeying the Constitution. That is still a sizable hunk of liberty — worth protecting from encroachment. A sane, decent, civilized society must provide some such oasis, some shelter from public scrutiny, some insulated enclosure, some enclave, some inviolate place which is a man's castle.[267]

IV. CALLING IN THE DOGS — SUGGESTIONS FOR THE FUTURE

Because of the many nuances of the *Katz* test, and the various doctrinal and philosophical difficulties in implementing it,[268] some have called for its wholesale rejection and replacement.[269] My project

possession and control of his own person, free from all restraint . . . ." (quoting Union Pac. R. Co. v. Botsford, 141 U.S. 250, 251 (1891))); Froomkin, *supra* note 167, at 838-40 (asserting that essential ingredient of privacy is ability to keep one's secrets).

[266] In a similar vein, Professor Michael Froomkin describes "informational privacy" as "the ability to control the acquisition or release of information about oneself" and as "a good in itself." A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463, 1467 (2000).

[267] Silverman v. United States, 365 U.S. 505, 512 n.4 (1961) (quoting United States v. On Lee, 193 F.2d 306, 315-16 (2d Cir. 1951) (Frank, J., dissenting), *aff'd*, 343 U.S. 747 (1952)). Thus, even "blind" technology searches infringe on our private spaces and may, in turn, lead to the chilling of the creative possibilities in those spaces. *See supra* note 167 and accompanying text (discussing privacy and creativity); *see also* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 447 (1980) (discussing that privacy is essential for "learning, writing and all forms of creativity").

[268] *See, e.g.*, Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 26 (2002); Sklansky, *supra* note 6, at 158 ("The [*Katz*] inquiry has proved distressingly indeterminate, and many observers, on and off the Court, have thought it circular.").

[269] *See, e.g.*, Henderson, *supra* note 146, at 562-63 (suggesting that Court "jettison" *Katz* test and return to text); Herman, *supra* note 12, at 125 (suggesting that *Katz* framework be replaced with test modeled on procedural due process); Swire, *supra* note 151, at 924-32 (declaring death of *Katz* and proposing test under which new police surveillance techniques are presumptively unreasonable unless carried out pursuant to particularized rules); *see* Luna, *supra* note 80, at 788 ("Academics of all stripes agree that search and seizure law is a 'mess' and have offered their own fix-it guides for the Fourth Amendment."); *cf.* Christopher Slobogin, *The World Without a Fourth Amendment*, 39 UCLA L. REV. 1, 3 (1991) (theorizing search and seizure law from ground up without "dogma" of existing case law).

is more modest because I believe that with a rearrangement of priorities, the Court can fulfill the revolutionary promise of *Katz*. I suggest that *Katz*'s problems might be mitigated by a two-step process of empirical determination of typical belief followed by a normative determination of the parameters of privacy.[270] First, the Court should ask whether an expectation is typical.[271] If it is, then it is not for the Court to say that such an expectation is nonetheless unreasonable. Second, if the expectation is not typical, the Court should make its own judgment whether one ought to be able to expect privacy in that area. It is likely that a strict adherence to a primary empirical and secondary normative analysis would necessitate the elimination of the third party doctrine and rejection of *Caballes*' contraband exception.[272]

A. Tempering the Manipulation Problem

There is no question *Katz*'s "reasonableness" requirement has its problems. As Professor Erik Luna explains, "The Fourth Amendment reasonableness test contains the vice of degenerative self-definition, with each unimpeded intrusion providing a new baseline against which all subsequent modes of government surveillance will be measured."[273] Given the obvious problems with the *Katz* test over the past forty years, some scholars have advocated reverting to the practice of defining the Fourth Amendment in terms of bright line rules.[274] However, *Katz*'s very fundamental flaw also embodies its most glorious promise for liberation. Reasonableness is the mechanism through which the Fourth Amendment can be a fluid protector of rights, rather than an outmoded relic tethered to no-longer-sufficient categories.[275] For this reason, the re-importation of bright line rules as

[270] *See infra* notes 277-82, 320-23 and accompanying text (laying out this process).

[271] S*ee generally* Slobogin & Schumacher, *supra* note 208 (discussing methodologies for quantifying typical social expectations of privacy).

[272] Many have suggested that the Court reject the third party and dog sniff lines of cases. *See* Bellia, *supra* note 148, at 1411-12 (asserting that third party cases be read to deny Fourth Amendment protection only when third party has access to information *and* there is separate determination that person retains no reasonable expectation of privacy); Sundby, *supra* note 57, at 1777 (arguing that citizen-government trust, not assumption of risk, should be central Fourth Amendment inquiry).

[273] Luna, *supra* note 80, at 794-95.

[274] *See* Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 268-301 (1993) (asserting that reasonableness standard has utterly failed and instead suggesting rules-based model); Kerr, *supra* note 251, at 533-34.

[275] *See supra* note 25 and accompanying text (noting Justice Brandeis's critique of

a substitute for a meaningful reasonableness analysis is ultimately unsatisfying. To revive the literal categories as some constraint when the Court gets *Katz*'s reasonableness requirement wrong is merely to revive *Olmstead*, leaving vast arenas of intimate conduct subject to monitoring.[276]

To ensure that courts do not manipulate the *Katz* reasonableness inquiry, reasonableness should be defined in terms of typical social expectations.[277] Simply, the Court should not be able to declare a subjective expectation of privacy unreasonable if it is one that is generally entertained by society. Formulating a detailed proposal for discerning typical social expectation[278] or recommending a particular scientific method[279] is unfortunately beyond the scope of this Article. I am arguing, however, that the Court should, at a basic level, integrate some empirical analysis regarding society's beliefs into its determination of reasonable expectation of privacy.[280] The Court is intimately familiar with the different methodologies for determining social expectations on a wide variety of matters, and it has various techniques for divining the feeling of relevant communities regarding specific social issues.[281] In addition to preventing manipulation, a

Olmstead's archaic nature).

[276] This problem is illustrated by the lower level status that many courts ascribe to people's cyberspaces. They tend to look at the Internet as a quintessentially nonprivate area, regardless of the fact that many people consider their computer activities incredibly private. *See supra* notes 181-83 and accompanying text.

[277] *See supra* notes 63-68 and accompanying text (discussing manipulation problem).

[278] Sundby suggests bypassing the empirical inquiry all together and only engaging in a normative determination of what police actions compromise citizen-government trust. Sundby, *supra* note 57, at 1777.

[279] Professors Slobogin and Schumacher have suggested an empirical methodology for canvassing social expectations regarding privacy. Slobogin & Schumacher, *supra* note 208, at 728.

[280] William Heffernan suggests privacy be found first "[w]hen it appears that conventional sources of vulnerability are at stake . . . [unless] an insider has affirmatively indicated her willingness to disclose them" or "when privacy cues are employed as signals for objects or information that do not normally generate a sense of vulnerability." William C. Heffernan, *Fourth Amendment Privacy Interests*, 92 J. CRIM. L. & CRIMINOLOGY 1, 67 (2002). Another (admittedly imperfect) methodology would be for the Justices to simply look at their own life experiences. *See* Cloud, *supra* note 268, at 31-32 (asserting that from personal perspective, Justices would be hard pressed to argue that they do not expect their backyards to be free from aerial surveillance).

[281] *See, e.g.*, Roper v. Simmons, 543 U.S. 551, 561, 605 (2005) (determining "evolving standards of human decency" through national consensus evidence and the court's own judgment); Miller v. California, 413 U.S. 15, 24 (1973) (defining

focus on typical social expectations will have the ancillary benefit of ensuring that the Court does not focus on law enforcement expediency as part of its determination of whether the police action is a search.[282]

It is quite apparent that the Court has not adopted a typicality approach to reasonable expectation. Instead, it has characterized privacy expectations as per se unreasonable because of remote possibilities of exposure,[283] assumption of risk,[284] illegality of the sought item,[285] or lack of physical intrusion.[286] There is some promising analysis in *Kyllo* equating reasonableness with typicality in a limited sense.[287] Rather than making the claim that Kyllo "voluntarily" exposed his house's temperature to the public or that the possibility of people sensing heat from his house destroyed any expectation of privacy, the Court held that using technology to detect "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."[288]

While better than a jurisprudence of possibility or risk assumption, this analysis still falls short. First, the Court's "functional equivalent of trespass" test may work in the context of thermal imaging of a home, but will likely prove unworkable for other types of technological searches.[289] More importantly if, as Justice Antonin Scalia has stated, "the Fourth Amendment is about privacy . . . not solitude,"[290] the question is not so much whether a particular

obscenity in part as "whether the average person, applying contemporary community standards would find that the work, taken as a whole, appeals to the prurient interest" (quoting Roth v. United States, 354 U.S. 476, 489 (1957))).

[282] *See* Tracey Maclin, *The Central Meaning of the Fourth Amendment*, 35 WM. & MARY L. REV. 197, 238 (1993) (describing Court's tendency to restrict reach of Fourth Amendment on crime control grounds).

[283] *See supra* Part II.A.1.

[284] *See supra* Part II.A.2.

[285] *See supra* Part III.A.

[286] *See* Cloud, *supra* note 274, at 252 (observing that, despite *Katz*'s ruling that Fourth Amendment protects people not places, Court has held that "different expectations attach to different physical locations").

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

[288] *Id.* (citation omitted).

[289] This is likely a result intended by the originalist author of the opinion, as he openly sought only to preserve "that degree of privacy against government that existed when the Fourth Amendment was adopted." *Id.* at 34.

[290] O'Connor v. Ortega, 480 U.S. 709, 730 (1987) (Scalia, J., concurring).

technology is in public use, but rather whether the public generally uses it in the manner the police seek to use it,[291] or indeed, whether it ought to be used in such a manner.[292] Certainly, a multitude of privacy-defeating tools are in public use: tools to pick locks, scale fences, amplify sounds, and see into crevices. Just because they have the potential to be used in privacy-defeating ways does not mean that we no longer have privacy expectations whenever they are used.[293]

A true typicality analysis, independent of the Court's assumptions about precautionary behavior or protected areas, would do much to restore the promise of *Katz*. It would necessitate the rejection of the assumption of risk analysis in *Greenwood* and *Smith*, although, depending on what our typical expectations are, perhaps not their conclusions.[294] Such a line of analysis would prove more protective of privacy rights in an increasingly digital world. Courts would not be able to summarily dismiss privacy claims in ISP information and electronic communication content on the sole ground that such information is "exposed" to a third party.[295] Rather, courts would have to discern how the average person feels about net privacy.

In addition, a typicality analysis would necessitate a rejection of the *Caballes* rule that contraband detection is sui generis.[296] *Caballes* did

---

[291] *See* Sklansky, *supra* note 6, at 208 (suggesting that "'general public use' in *Kyllo* should be read to mean widespread and lawful use of a device to see or hear the same things the government seeks to see or hear").

[292] *See* Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1425 (2002) (doubting "conclusion that societal mores concerning privacy are not transgressed by suspicionless surveillance of the home interior carried out with devices that are in general public use").

[293] *See Kyllo*, 533 U.S. at 47 (Stevens, J., dissenting) (asserting that *Kyllo*'s "general public use" criterion is "somewhat perverse because it seems likely that the threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available"); Thomas K. Clancy, *What Is a "Search" Within the Meaning of the Fourth Amendment?*, 70 ALB. L. REV. 1, 49 (2006) ("Once the bright-line rule of *Kyllo*'s 'otherwise-imperceptibility' test without its limitation on general public use is breached, the Court's options of either freezing the development of technological devices in some ad hoc manner or permitting unlimited use of very intrusive devices as they become readily available are not particularly satisfactory.").

[294] For example, the Court could not rule, as it did in *Greenwood*, that there is no expectation of privacy in trash merely because it has been conveyed to a third party. *See supra* Part II.A.2. It could, however, find that society typically believes trash is not private.

[295] At the very least, if unwilling to abandon the third party doctrine, courts should get it right and not mix the rule from *Greenwood* and *Smith* with the rule from *Hoffa* and *White*. *See supra* notes 194-202 and accompanying text.

[296] It is likely that we believe the use of such devices in, for example, the airport is

not attempt to discern society's expectations regarding dog sniffs because of its myopic focus on the fact of Caballes's guilt. Because the Court was so concerned with the reasons why the guilty fear dog sniffs, it gave no thought to the reasons why the average person might fear that same action.[297] This faulty analysis is spurred on by scholarship intent on drawing a dividing line between the expectations of the innocent and guilty for Fourth Amendment purposes.[298] Arguing that privacy should be innocent-focused misses the important fact that, in the absence of particularized suspicion, every target of investigation is an innocent. The Court has long held that the issue of whether a certain area is private is conceptually distinct from whether the law enforcement tactic at issue is beneficial to society.[299]

There is an interesting moment in history that illustrates the different impacts an assumption of risk approach and a typicality approach have on new technology cases. In the early 1990s, cordless phone technology was fairly new, and certain cordless phone conversations were picked up inadvertently by neighbors listening to the AM radio or deliberately by police using low tech interception devices.[300] Some courts, adhering to a *Greenwood*-type analysis, held that the possibility of radio interception, whether known or not to the cordless phone user, created a risk, which the user had to assume, that any cordless phone call would be intercepted by the police.[301] The Fourth Circuit went so far as to argue that people using landlines who called cordless phone users had no reasonable expectation of privacy

less intrusive than their use in our homes because we exercise some choice to use the airport and we do not carry out daily intimate activities in the airport. Alternatively, some may find the use of a sniffer dog during an on-the-street encounter more intrusive than the use of a hand-held device because of the intimidating nature of a dog. All these assertions, however, are just mere speculation as the *Caballes* Court did not address such issues. *See supra* notes 241-43 and accompanying text.

[297] *See* Tracey Maclin, *Justice Thurgood Marshall: Taking the Fourth Amendment Seriously*, 77 CORNELL L. REV. 723, 745 (1992) (suggesting that Court would come to right decisions about privacy if they were not always thinking about fact that person claiming right is criminal).

[298] *See* Colb, *supra* note 218, at 1482; Loewy, *supra* note 218, at 1229.

[299] *See supra* notes 220-23 and accompanying text.

[300] *See, e.g.*, United States v. McNulty (*In re* Askin), 47 F.3d 100, 101 (4th Cir. 1995) (interception by police using radio scanner); United States v. Smith, 978 F.2d 171 (5th Cir. 1992) (neighbor picked up calls on AM radio).

[301] *See* Price v. Turner, 260 F.3d 1144, 1148-49 (9th Cir. 2001); McKamey v. Roach, 55 F.3d 1236, 1237 (6th Cir. 1995); *McNulty*, 47 F.3d at 105; Tyler v. Berodt, 877 F.2d 705, 706 (8th Cir. 1989); United States v. Carr, 805 F. Supp. 1266, 1271 (E.D.N.C. 1992). In *United States v. Smith*, 978 F.2d 171, 173 n.1 (5th Cir. 1992), the Court specifically noted the availability of cordless phone scanners to the general public.

in the content of the conversations.[302] Like courts in the Internet context, the Fourth Circuit dangerously mixed the *White/Hoffa* rule with the third party rule:

> The common characteristic of the government informant and the cordless phone user is that they are both unreliable recipients of the communicated information: one because he repeats the conversation to law enforcement officers and the other because he broadcasts the conversation over radio waves to all within range who wish to overhear. It is this general risk of unreliability of which *White* and *Hoffa* warn, not the specific risk that the listener is an informant *per se*.[303]

Frighteningly, the Fourth Circuit established a rule by which content of any conversation is fair game, unless the defendant takes some unspecified measures to ensure the "reliability" of fellow conversants and call carriers.[304]

Compare this approach with the Fifth Circuit's analysis of the issue:

> Courts should bear in mind that the issue is not whether it is conceivable that someone could eavesdrop on a conversation but whether it is reasonable to expect privacy. No matter how technologically advanced cordless communication becomes, some people will always find a way to eavesdrop on their neighbors. However, "[t]he fact that [Listening] Toms abound does not license the government to follow suit."[305]

The court went on to note:

> The same holds true for land-based telephone lines. The equipment needed to tap a regular telephone line can be purchased for less than $25 at Radio Shack (considerably less that the cost of a Bearcat scanner) . . . . The fact that some individuals eavesdrop on regular telephone conversations does not mean that no one has a reasonable expectation of privacy for ordinary phone calls.[306]

---

[302] *McNulty*, 47 F.3d at 105.

[303] *Id.* (citations omitted).

[304] *See supra* notes 194-207 and accompanying text (criticizing this analysis); *cf.* Kerr, *supra* note 153, at 830 (asserting that courts finding no protection for cordless phones embraced trespass theory and were moved by absence of physical phone line tampering).

[305] *Smith*, 978 F.2d at 179-80 (citations omitted).

[306] *Id.* at 180 n.10. The Court nonetheless ultimately resolved the issue in favor of

This analysis gives a fairer meaning to the concept of reasonable expectation and reasonable caution because it does not define reasonableness by possibility or risk.[307] Unfortunately, at the time, most courts held that wireless conversations were not protected by the Fourth Amendment. It was not until Congress stepped in to regulate police behavior in that area that people began to enjoy privacy in wireless communications.[308] Professor David Sklansky thus sums up the cordless phone case era as a "sobering" reminder "that constitutional protections for the confidentiality of telephone conversation might be extinguished by a widespread risk of private surveillance made possible by new technology."[309]

B. Dealing with the Normativity Problem

Because social expectations can be manipulated by normatively objectionable means,[310] answering the empirical question is only the first step in determining whether there ought to be protection under the Fourth Amendment. The Court must make a normative judgment about what society is entitled to hold as private, regardless of prevailing social thought. However, the Court's ability and obligation to resort to reliance on its own judgment should be secondary to the empirical evaluation.

Conservative justices, notably Justice Scalia, are extremely wary of tests in which the Court exercises its "own judgment" to determine the constitutionality of a government action.[311] Conservatives tend to argue that this puts the Court in place of a super-legislature, creating law, and abusing its position in the delicate balance of governmental powers.[312] The conservative mantra is that the Court should not

---

the government. *Id.* at 181.

[307] *Cf.* cases cited *supra* note 301.

[308] Congress did not step in until 1994. *See* Communications Assistance for Law Enforcement Act § 202, Pub. L. No. 103-414, 108 Stat. 4279, 4290-91 (1994) (codified at 18 U.S.C. §§ 2510-2511 (2000 & Supp. III 2003)).

[309] Sklansky, *supra* note 6, at 202-03.

[310] *See supra* notes 82-84 and accompanying text (discussing government gamesmanship and voyeuristic behavior as manipulators of social expectation).

[311] *See* Roper v. Simmons, 543 U.S. 551, 608 (2005) (Scalia, J., dissenting) (characterizing majority's evolving standards of decency test as Court "proclaim[ing] itself sole arbiter of our Nation's moral standards").

[312] On the one hand, were the Court always to defer to the legislature, there could simply be no constitutional law. On the other hand, an interventionist Court is open to charges of being elitist and antidemocratic. This is known as the "countermajoritarian difficulty." *See* ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH: THE SUPREME COURT AT THE BAR OF POLITICS 16-17 (1962). To temper this

elevate its own judgment about issues like privacy or death penalty over the views of the American public.[313] It is therefore ironic indeed that the conservative portion of the Court was quickest to substitute its own beliefs for society's beliefs regarding privacy. It was the conservative swing of the Court that led reasonableness to be defined by risk assumption and possibility, rather than majoritarianism.[314]

A conservative might respond that the Court was correct to reject social definitions of privacy, because such social expectations are normatively objectionable.[315] I assert, however, that the resort to a normative judgment should be made only after finding that society does not expect privacy in the disputed area. The Constitution is

difficulty, conservatives argue that the only nonpolitical, neutral check on the judicial power, other than majoritarianism, is text and Framers' intent. *See* Richard S. Kay, *Adherence to the Original Intentions in Constitutional Adjudication: Three Objections and Responses*, 82 NW. U. L. REV. 226, 230-34 (1988) (describing originalist position). However, the idea that "pure" textual interpretation and nonrevisionist constitutional history exist such that their presumptive use in constitutional interpretation produces "neutral" results, is hotly disputed. *See* Paul Brest, *The Misconceived Quest for Original Understanding*, 60 B.U. L. REV. 204, 221 (1980) (asserting that when person engages in originalism "she is in a fantasy world more of her own than of the adopters' making").

[313] Calling progressive policies antidemocratic and progressives elitist is a favorite tactic of conservatives opposed to minority rights. Shane B. Kelbley, Note, *Reason Without Borders: How Transnational Values Cannot Be Contained*, 28 FORDHAM INT'L L.J. 1595, 1632 (2005) (observing that conservatives argued against perceived "gay rights" opinion in *Lawrence* by asserting that "activist judges" were imposing personal beliefs on American population); *see also* Aya Gruber, *Navigating Diverse Identities: Building Coalitions Through Redistribution of Academic Capital — An Exercise in Praxis*, 35 SETON HALL L. REV. 1201, 1209 (2005) (discussing "the co-opting of minority status by privileged members of society").

[314] *See supra* note 61 and accompanying text.

[315] Indeed, some argue for a presumption of no protection that cannot even be overcome by the typicality analysis. For example, Professor Kerr asserts that, regardless of social beliefs about privacy, the only time an expectation of privacy is "legitimate" is when it finds a source outside of the Fourth Amendment. *See* Orin S. Kerr, *The Fourth Amendment in Cyberspace: Can Encryption Create a "Reasonable Expectation of Privacy?"*, 33 CONN. L. REV. 503, 511-13 (2001). In essence this renders the Fourth Amendment completely impotent as a source of privacy rights. It becomes a mere procedural mechanism (possibly duplicative and unnecessary) for ensuring that state actors do not infringe upon already well-established rights. Kerr characterized his proposal as a civil libertarian theory, asserting that "by linking Fourth Amendment protection to the presence of extraconstitutional rights, the rights-based conception ensures that the government cannot use its mere ability to invade privacy as a basis for eradicating Fourth Amendment protection." *Id.* at 512-13. While it is true that bright line baseline controls can serve as a check on a Court bent on utter eradication of the Fourth Amendment, that observation only readily supports the conclusion that bright line rules should be set as a floor of constitutional protection.

counter-majoritarian in a very specific way — it permits the Court to supersede majoritarian sentiments when they conflict with fundamental individual rights.[316] Thus, the Court ought to be very circumspect about using the Bill of Rights as a tool to augment police power contrary to the wishes of the majority.[317] It follows that there should be a very high threshold test the Court must satisfy before it can prioritize its rights-restricting views over the public's rights-favoring expectations. Perhaps in the most compelling circumstances this threshold could be met,[318] but it certainly was not met in *Greenwood* or *Caballes*.[319]

It is a different story all together when the Court makes an initial determination that society typically believes that a certain area is not private. In this case, the Court has an obligation to determine whether, regardless of the prevailing beliefs, society ought to be able to regard the area as private. This is such an important inquiry because ever-improving technological abilities allow both the government and private individuals to bypass our typically erected privacy barriers.[320] The difficulty is determining the right normative formula for deciding which areas should be private, despite society's view that they are not clandestine because of technologically enhanced snooping. One suggestion is for the Court to examine critically the reasons why there is a prevailing view that the area is not private. If no privacy is expected only because of systematic government invasion or the voyeuristic behavior of particularly ambitious deviants, then the Court should hold that an expectation of privacy in that area

[316] *See supra* note 312 (discussing counter-majoritarian difficulty). *See generally* RONALD M. DWORKIN, A MATTER OF PRINCIPLE 57-60, 88, 110-11 (1985) (asserting that Constitution is meant to protect individuals from majorities).

[317] In addition, arguably the *Katz* Court never intended to allow the Court to impose rights restricting views on the populace. *See* discussion *supra* Part I.B.

[318] For example, in truly exigent situations where the very existence of the nation is at stake, the Court could declare persons' beliefs that that they are immune from certain investigative techniques normatively unreasonable. *See* Katz v. United States, 389 U.S. 347, 358 n.23 (1967) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case."). Such a proposition, however, would likely be very controversial.

[319] Although the Court masks assumption of the risk as a moral judgment in the third party cases, it is simply a rhetorical contrivance that cannot serve as a basis for ignoring majoritarian views. *See supra* text accompanying notes 73-76.

[320] See, for example, the technology discussed in *supra* notes 247-50 and accompanying text. Consequently, society might harbor a belief that an area is not private, while simultaneously believing that it should be private.

is nonetheless reasonable.[321] Alternatively, the Court might turn back to the literal list in the Constitution as a baseline of protection, under which no civilized society can fall.[322] In addition, the Court could develop the distinction between content and noncontent information, enabling courts to find that the content of communication is protected even in fora like the web, where advancing technology or popular fears of hacking, might engender a belief that online communications are not private.[323]

CONCLUSION

In the last forty years, the Supreme Court has, literally and figuratively, trashed *Katz*. The Court has allowed crime control concerns to guide it in a manipulative reading of the reasonableness prong. This has resulted in a body of law in which privacy means solitude and the police may engage in intrusive actions in the most intimate of areas — actions that might not have been permitted under a literalist reading of the Fourth Amendment. The situation has become so dire that even civil libertarians have proposed going back to a rules-based regime, reminiscent of *Olmstead*.

The Court's third party and contraband exceptions prove extremely dangerous in an increasingly technological world. As more and more communication is carried out through electronic media, third parties, or at least their virtual manifestations, have the capability of scanning all our communications. As crime detection techniques improve, every citizen is potentially subject to random contraband or criminality checks. Without even talking about other problematic aspects of the Court's post-*Katz* jurisprudence, like standing and plain view, the third party and contraband cases alone produce a very bleak view for the future. They create an America in which the scope of the

[321] Again, it is difficult to declare the precise formula for determining when this is the case. One way might be to look at what state laws prohibit. If state laws prohibit certain privacy-defeating behaviors, and those behaviors are what have destroyed the societal expectation of privacy, then the government nonetheless must treat the area as private.

[322] The analysis here would look similar to that in *Kyllo*, with one important difference: the analysis is not a substitute for the typicality inquiry, it is only used to restore privacy when the court finds lowered social expectations regarding a traditionally intimate area. Kyllo v. United States, 533 U.S. 27, 34 (2001) (drawing bright line of privacy protection at home).

[323] Of course, then there will be issues over what is content and what is noncontent. *See supra* note 125 and accompanying text.

government's surveillance and data gathering on its own citizens makes former FBI director J. Edgar Hoover's files look like child's play.

Despite all of its problems, I am not prepared to say that *Katz* has gone to the dogs. I believe the *Katz* test can be a good one with some modifications. With a little effort, the *Katz* revolution can still be realized. The Court must be willing to rethink the doctrines that have systematically undermined our privacy. If we look at Justice Harlan's test as a work in progress, we can see that he soon added the normativity requirement in his *White* dissent.[324] In an increasingly digital world, nature no longer gives us appropriate tools to construct our own privacy barriers. It is thus more important than ever that the Court construct legal fortifications to protect our privacy and withstand arbitrary government invasions.

[324] United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).