Journal of Business & Technology Law

Volume 12 | Issue 1 Article 2

A Grand Compromise for the Fourth Amendment

Carrie Leonetti

CARRIE LEONETTI*

A Grand Compromise for the Fourth Amendment

I. INTRODUCTION

When one thinks of trespass, one tends to think of the nineteenth-century doctrine involving unauthorized incursions onto the real property of another. As Harold Demsetz has pointed out, however, "the emergence of new property rights takes place in response to the desires of the interacting persons for adjustment to new benefit-cost possibilities."[1]

Section II of this Article describes the problems with the Supreme Court's current test for determining when Government conduct has violated the Fourth Amendment to the United States Constitution[2]: the "reasonable expectation of privacy" test from Justice Harlan's concurring opinion in *Katz v. United States*.[3] It argues that courts apply the *Katz* test through a lens of implied consent and assumption of risk that leads to absurd results, particularly when it comes to high-tech surveillance.

Section III argues that the Supreme Court should overrule *Katz* and replace its expectation-of-privacy test with one that relies on a new, broader conception of property that includes informational and intellectual, as well as traditional real and personal, property. Section IV concludes that a new doctrine of Fourth Amendment property could serve as a unifying principle to rationalize and expand the Amendment's privacy protections.

* Associate Professor, Center for Cyber Security & Privacy, University of Oregon School of Law.

1. Harold Demsetz, *Toward a Theory of Property Rights*, 57 AM. ECON. REV. 347, 350 (1967).

2. U.S. CONST. amend. IV. The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Id.

3. 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (dictating that the proper focus of any inquiry into the existence of a search—the trigger point for any Fourth Amendment protection—is the reasonableness of the expectations of privacy of the individuals affected by the Government's invasions).

II. THE PROBLEMS

A. The Problem with Katz

The modern test for determining the scope of the protections of the Fourth Amendment, established in Justice Harlan's concurring opinion in *Katz v. United States*, has been roundly criticized from all sides of the ideological spectrum.[4] One common critique revolves around the test's subjective, malleable, and circular nature.[5] Proving these critics' point, disagreements among the Justices rarely center

4. *See, e.g.*, Craig M. Bradley, *Two Models of the Fourth Amendment*, 83 MICH. L. REV. 1468, 1468–72 (1985) (describing the Fourth Amendment as "the Supreme Court's tarbaby: a mass of contradictions and obscurities"); Morgan Cloud, *Pragmatism, Positivism, and Principles in Fourth Amendment Theory*, 41 UCLA L. REV. 199, 268–301 (1993) (arguing that the *Katz* reasonableness standard is a failure and proposing a rules-based model instead); Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 20–36 (2002) (concluding that *Katz* has failed in its original purpose of using the Fourth Amendment to regulate high-tech surveillance); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 35–40 (2004) (describing *Katz*'s intended protection of privacy from electronic surveillance "anemic" and complaining that courts are uncomfortable making the test's normative judgment); Susan N. Herman, *The USA Patriot Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67, 125 (2006) (suggesting that the *Katz* framework should be replaced with a test derived from procedural due process); Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-First Century*, 65 IND. L.J. 549, 554 (1990) ("The *Katz* standard has been twisted to allow the government access to many intimate details about our lives . . . ."); Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L. Q. 1013, 1015 (2001) ("[*K*]*yllo* shows that a majority of the Court … doubt[s] … the usefulness of the *Katz* test."); Brian J. Serr, *Great Expectations of Privacy: A New Model for Fourth Amendment Protection*, 73 MINN. L. REV. 583, 587 (1989) ("[T]he entire course of recent Supreme Court fourth amendment precedent, which has narrowed significantly the scope of individual activities that are protected constitutionally, is misguided and inconsistent with the spirit of the fourth amendment."); Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 924–32 (2004) (proposing courts' replace the *Katz* test with a test under which new police surveillance techniques would be presumptively unreasonable unless they were carried out pursuant to particularized rules); Lloyd L. Weinreb, *Generalities of the Fourth Amendment*, 42 U. CHI. L. REV. 47, 49–50 (1974) (describing Fourth Amendment law as "a body of doctrine that is unstable and unconvincing").

5. *See, e.g.*, Minnesota v. Carter, 525 U.S. 83, 91, 97 (1998) (Scalia, J., concurring) (describing the Court's reasonableness analysis under *Katz* as "fuzzy," "notoriously unhelpful," and "self-indulgent"); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60 (2001) ("Harlan's test was applauded as a victory for privacy, but it soon became clear that it was entirely circular."); Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 60–61 (2001) ("Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable."); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 383–86 (1974) (complaining that *Katz*'s reasonable-expectation-of-privacy test was circular); Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *is Made of?*, 41 U.C. DAVIS L. REV. 781 (2008) (arguing that the *Katz* test has been more harmful to privacy than protective of it because it is easily manipulable by conservative courts in way that allows them to define societal expectations of privacy as lower than they actually are); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Myth of Caution*, 102 MICH. L. REV. 801, 822 (2004) ("[The] vague language [of the *Katz* test] can support a narrow or broad reading equally well."); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1343–62 (2002) (describing how *Katz*'s failure to provide clear guidance

on whether the *Katz* test should apply, but rather involve the judges in the majority and dissent applying the test to the same set of facts while reaching different conclusions.[6] Recently, the Court has begun to show fractures over whether *Katz* provides a dispositive answer to Fourth Amendment questions.[7]

In practical application, courts applying the *Katz* test tend to embrace loose norms of implied consent and assumption of risk, even though they rarely label them as such.[8] The typical reasoning dictates that, if an individual does not take sufficient precautions with his/her private information, then s/he has voluntarily consented to, or at least assumed, the risk that it will be viewed or seized and cannot reasonably expect otherwise.[9] At the extreme, the failure to take sufficient precautions can even

about the boundaries of constitutionally protected privacy has permitted lower courts to manipulate the test to reach any result); Christopher Slobogin, *Technologically-Assisted Physical Surveillance: The American Bar Association's Tentative Draft Standards*, 10 HARV. J.L. & TECH. 383, 401 (1997) [hereinafter "Slobogin, *Draft Standards*"] (contending that many of the factors that courts consider in deciding whether Government conduct infringes upon a reasonable expectation of privacy "are of dubious value").

6. *Compare, e.g.*, United States v. Kyllo, 533 U.S. 27, 34 (2001) (holding that thermal imaging of the heat signature of a home invaded the occupants' reasonable expectation of privacy), *with id.* at 43–44 (Stevens, J., dissenting) (arguing that any such subjective expectation of privacy was objectively unreasonable).

7. *See* United States v. Jones, 132 S. Ct. 945, 950 (2012) ("Jones's Fourth Amendment rights do not rise or fall with the *Katz* formulation.").

8. *See infra* note 9 (listing cases with varying indicia suggesting an amporphous, undefined, implied consent or assumption of risk standard from the courts).

9. *See Katz*, 389 U.S. at 351 (noting that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection"); United States v Maynard, 615 F.3d 544, 558 (D.C. Cir. 2010) (explaining that determining "whether an expectation of privacy is reasonable depends in large part upon whether that expectation relates to information that has been 'exposed to the public'"); *see, e.g.*, California v. Hodari D., 499 U.S. 621, 628–29 (1991) (concluding that Hodari had relinquished any reasonable expectation of privacy regarding a rock of cocaine that he tossed away while fleeing a police officer because he had "abandoned" it, and therefore lost the right to challenge any subsequent chemical testing of the rock); Nat'l Treas. Emp.'s Union v. Von Raab, 489 U.S. 656, 663–64 (1989) (upholding the warrantless drug testing of high-level Customs Service employees because they impliedly consented to the testing when they sought promotions); Florida v. Riley, 488 U.S. 445, 449–51 (1989) (finding that Riley had assumed the risk that his backyard would be surveilled by a helicopter flying at a "legal" altitude); California v. Greenwood, 486 U.S. 35, 40–41 (1988) (holding that Greenwood's Fourth Amendment protection did not extend to the garbage that he had placed at the curb for collection because he had assumed the risk that people might go through it); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (holding that Ciraolo's failure to shield his backyard marijuana garden from public view in navigable airspace diminished the reasonableness of any expectation of privacy that he may have had in his yard); United States v. Carpenter, 819 F.3d 880, 888 (6th Cir. 2016) ("[A]ny cellphone user who has seen her phone's signal strength fluctuate must know that, when she places or receives a call, her phone 'exposes' its location to the nearest cell tower and thus to the company that operates the tower."); United States v. Davis, 785 F.3d 498, 512 n.12 (11th Cir. 2015) (en banc) ("Cell phone users voluntarily convey cell tower location information to telephone companies in the course of making and receiving calls on their cell phones."); United States v. Jones, 406 Fed. Appx. 953, 954–55 (6th Cir. 2011) (finding that Jones had assumed the risk that the police would search his jacket by leaving it in the back of a bar); United States v. Forrester, 512 F.3d 500, 509–10 (9th Cir. 2008) (holding that the IP addresses that Forrester visited were not protected by the Fourth Amendment because he knowingly shared them with his internet service provider); United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet

provider is not protected by the Fourth Amendment's privacy expectation."); United States v. Liu, 180 F.3d 957, 961–62 (9th Cir. 1999) (finding that Liu had assumed the risk of the seizure and search of his suitcase when he left it on a train after he nervously fled an agent's request to see his ticket); United States v. Landry, 154 F.3d 897, 899 (8th Cir. 1998) (finding that Landry had assumed the risk of the seizure of his paper bag containing crack cocaine when he left it in a dumpster while he used a nearby pay phone); United States v. Washington, 12 F.3d 1128, 1132 (D.C. Cir. 1994) (finding that Washington had abandoned his overturned vehicle and its contents in an alley when he fled the scene after a high-speed chase and that the Fourth Amendment did not require the police to obtain a warrant to search a plastic bag, containing drugs, that was in plain view inside); United States v. Rem, 984 F.2d 806, 814 (7th Cir. 1993) (finding that Rem had assumed the risk of the seizure and search of his suitcase containing cocaine because he had abandoned it by leaving it on the train when he deboarded and denied that he had been on the train when asked by agents); United States v. Wilder, 951 F.2d 1283, 1286 (D.C. Cir. 1991) (finding that Wilder assumed the risk that the police would seize and search his paper bag containing crack cocaine when he left it on the steps of a public building and began to walk away after noticing the police watching him); United States v. Eubanks, 876 F.2d 1514, 1516 (11th Cir. 1989) (finding that Eubanks had assumed the risk that his fingerprints and trace amounts of cocaine would be lifted from a piece of paper when he "abandoned" the paper by dropping it on the ground); United States v. Osunegbu, 822 F.2d 472, 479 (5th Cir. 1987) (finding that Osunegbu had no reasonable expectation of privacy in the contents of his locked rental mailbox because the rental manager had access to them when sorting the mail); United States v. Brown, 473 F.2d 952, 954 (5th Cir. 1973) (holding that Brown assumed the risk that the police would search a suitcase containing the proceeds of a bank robbery when he abandoned it in an open field); People v. Roybal, 966 P.2d 521, 536–37 (Cal. 1998) (finding that Roybal had assumed the risk that the police would seize and search the contents of a plastic bag that he abandoned by placing it on a peripheral cinder-block wall that separated his mother's backyard from her neighbors'); People v. Gallego, 117 Cal. Rptr. 3d 907, 912 (Cal. Ct. App. 2010) ("[The] cigarette butt, like the trash bags in *Greenwood*, was left in a place 'particularly suited for public inspection.' Defendant thus abandoned the cigarette butt in a public place, and therefore had no reasonable expectation of privacy concerning the DNA testing of it to identify him as a suspect . . . . "); Commonwealth v. Bly, 862 N.E.2d 341, 356–57 (Mass. 2007) (finding that, by leaving his water bottle and cigarette butts behind in a police interrogation room, Bly had abandoned the DNA that they contained and assumed the risk that the police would analyze it); State v. Buckman, 613 N.W.2d 463, 474 (Neb. 2000) (holding that Buckman lacked a reasonable expectation of privacy in the DNA on two cigarettes that he smoked and left behind at the police station after his arrest because he assumed the risk that they would be seized); People v. Brown, 828 N.Y.S.2d 550, 551 (N.Y. App. Div. 2007) (holding that Brown lacked a reasonable expectation of privacy in a bandage soaked in his blood because he voluntarily gave it to emergency medical personnel when they exchanged it for a clean one); People v. LaGuerre, 815 N.Y.S.2d 211, 213 (N.Y. App. Div. 2006) (holding that LaGuerre lacked a reasonable expectation of privacy in his DNA sample extracted from chewed gum when he voluntarily gave it to undercover police officers pretending to conduct a soda taste test for the purpose of surreptitiously obtaining his DNA); State v. Belcher, 759 P.2d 1096, 1097 (Or. 1988) (finding that Belcher assumed the risk that the police would seize and inspect the contents of his backpack when he left it behind in the parking lot of a tavern fleeing the scene of a fight that the police had come to investigate); *see also* Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 624, 627 (1989) (holding that railroad employees had a diminished expectation of privacy in the subjection of their bodily fluids to drug and alcohol testing because they voluntarily entered a heavily regulated field of employment); South Dakota v. Opperman, 428 U.S. 364, 367–68 (1976) (holding that drivers have reduced expectations of privacy in their vehicles because of their pervasive statutory regulation); Dimeo v. Griffin, 943 F.2d 679, 682, 685 (7th Cir. 1991) (upholding the random suspicion-less drug testing of jockeys because they voluntarily entered a profession that requires frequent medical examinations). *But cf. In re* Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government, 620 F.3d 304, 317 (3d Cir. 2010) ("A cell phone customer has not 'voluntarily' shared his location information with a cellular provider in any meaningful way . . . . [I]t is unlikely that cell phone customers are aware that their cell phone providers *collect*

be deemed to have deprived the individual of a subjective expectation of privacy.[10] A canonical expression of these norms can be found in the Supreme Court's opinion in *California v. Greenwood*,[11] in which the majority reasoned:

> *It 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 . . . . Moreover, respondents placed their 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.*[12]

The result of this assumption-of-risk norm is a jurisprudence of blame, in which individuals can forfeit their constitutional privacy rights without knowingly, intelligently, and voluntarily doing so, by failing to take steps to avoid even very small risks. For example, in *United States v. White*[13] and *United States v. Hoffa*,[14] the Supreme Court held that individuals had no reasonable expectation of privacy in their conversations with undercover Government agents because they had assumed the risk that the person to whom they were speaking could be an untrustworthy confidant.[15] In *United States v. Miller*,[16] the Court held that Miller had no reasonable expectation of privacy in his private bank records because he had revealed them to a third party (his bank) and, therefore, had assumed the risk that the bank would in

and store historical location information."). *See generally* RESTATEMENT (SECOND) OF TORTS § 496D cmt. b (AM. LAW INST. 1965) ("The basis of assumption of risk is the plaintiff's consent to accept the risk . . . .").

10. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 281–82 (1983) (characterizing driving on public streets as a voluntary conveyance of Knott's route of travel to any interested onlooker, even one using a radio beeper to track him).

11. 486 U.S. 35 (1988).

12. *Id.* at 40.

13. 401 U.S. 745 (1971).

14. 385 U.S. 293 (1966).

15. *See White*, 401 U.S. at 751 (holding that "the defendant necessarily risks" that a person with whom they have a conversation would breach their confidence); *Hoffa*, 385 U.S. at 302 (holding that the Fourth Amendment did not protect Hoffa's "misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

16. 425 U.S. 435 (1976) (holding that, when Miller voluntarily relinquished checks and deposit slips that he had prepared to a bank, he relinquished any "protected Fourth Amendment interest" in them, so that the Government did not need a warrant issued on probable cause in order to obtain them from the bank).

turn reveal them to the Government.[17] In *Smith v. Maryland*,[18] the Court refused to recognize a reasonable expectation of privacy in the numbers dialed from or to a telephone, reasoning that, by voluntarily conveying numerical information to the telephone company, customers had assumed the risk that the phone company would share that information with the police.[19]

B. The High-Tech Problem

The latitude that courts have in deciding whether individual expectations of privacy are "reasonable" is inherent in the *Katz* test, and it has resulted largely in the evisceration of many of the Fourth Amendment's protections. The application of this presumption of assumption of risk, particularly in high-tech settings, has engendered increasingly ludicrous results: courts are consistently finding expectations of privacy—that most Americans take for granted as being constitutionally protected—to be unreasonable, and therefore not afforded Fourth Amendment protection.[20] Courts have extended *White* and *Hoffa* into the context of

17. *Id.* at 443 ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

18. 442 U.S. 735 (1979) (permitting the warrantless collection of Smith's telephone-usage details because it did not involve surveillance of the contents of his phone calls and he knowingly revealed the usage metadata to the phone company for billing purposes).

19. *Id.* at 742–44 (rejecting the claim that people have a reasonable expectation of privacy in the telephone numbers that they dial because they reveal them to the telephone company when placing and receiving calls).

20. *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."); Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 11 nn.6–7 (2004) (citing studies that show that Americans engage in private Internet communications without taking precautions like encryption); Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L. J. 213, 272–85 (2002) (demonstrating that Americans have an expectation of privacy to be free from unconstrained public video surveillance); 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, 732 (1993) ("[S]ome of the Court's conclusions [about whether particular expectations of privacy are reasonable] may be well off the mark."); *see, e.g.*, United States v. Forest, 355 F.3d 942, 951 (6th Cir. 2004) (holding, based on *Knotts*, that Forest had no legitimate expectation of privacy that precluded DEA agents from using his cell phone location information to track his location on public highways); see *also* United States v. Jones, 31 F.3d 1304, 1309 (4th Cir. 1994) (holding, based on *Knotts,* that Jones had no reasonable expectation of privacy that prevented postal inspectors' from using an electronic tracking device to monitor the contents of his van); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005) (finding no reasonable expectation of privacy in AOL's subscriber information even though AOL had an explicit nondisclosure policy for such information); *cf. Smith*, 442 U.S. at 750 (Marhsall, J., dissenting) ("It is idle to speak of 'assuming' risks in context where, as a practical matter, individuals have no realistic alternative.") (internal citation omitted); Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING

certain Internet communications[21] and chat rooms,[22] *Smith* to Internet activity revealed by a consumer to an Internet service provider ("ISP"),[23] and *Greenwood* into the context of cordless telephone conversations.[24] As Justice Marshall, dissenting in *Smith*, pointed out: "[U]nless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[25] Similarly, Justice Sotomayor has more recently noted that the *Smith* metadata doctrine is "ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[26]

For example, in *United States v. Graham*,[27] the United States Court of Appeals for the Fourth Circuit recently held that the Government's warrantless acquisition of cell service location information from Graham's cellular provider did not violate the

BUS. L. 27, 54 (2000) (noting that "any consent to system usage that might be implied from connection to the Internet surely does not include 'hacker' intrusion"); Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. REV. 1047, 1055 n.30 (2005) ("Real world property is marked by low monitoring and exclusion costs - trespassers are easily identified, and self-help exclusion (like fencing around a plot of land) is comparatively cheap. Intellectual property suffers from high monitoring costs, and self-help is not an option."); Kerr, *supra* note 5, at 809 (noting that "a 'reasonable expectation of privacy' is not the same as the privacy that a reasonable person would expect"); Slobogin, *Draft Standards*, *supra* note 5, at 400 ("[W]e only assume those risks of unregulated government intrusion that the courts tell us we have to assume."). *See generally* Eric Lichtblau, *Police Are Using Phone Tracking as a Routine Tool*, N.Y. TIMES (Mar. 31, 2012) (describing the routine police use of cell-location tracking and suggesting that it raises constitutional concerns), http://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html; Somini Sengupta, *The New Pay Phone and What It Knows About You*, N.Y. TIMES (Apr. 30, 2012) (discussing consumers' unwillingness to share their phone numbers with businesses and suggesting that Americans are uneasy with the idea that their phones divulge personal information), http://bits.blogs.nytimes.com/2012/04/30/the-new-pay-phone-and-what-it-knows-about-you/?_r=0.

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

22. *See Charbonneau*, 979 F. Supp. at 1185 (holding that Charbonneau "could not have a reasonable expectation of privacy in the chat rooms" and that "the email sent by Defendant to others in a 'chat room' is not afforded any semblance of privacy"); State v. Turner, 805 N.E.2d 124, 132 (Ohio Ct. App. 2004) ("[W]hen parties make contact in a chat room, a private box opens up so that they can have a conversation only with each other; that still did not give Turner an expectation of privacy, since he was chatting with a stranger, not a known acquaintance."); Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001) (holding that Proetto did not have a reasonable expectation of privacy in his chat-room conversations because "he did not know to whom he was speaking").

23. *See* Guest v. Leis, 225 F.3d 325, 335–36 (6th Cir. 2001) (holding that a consumer had no reasonable expectation of privacy in non-content Internet information disclosed to an ISP).

24. *See, e.g.*, United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992).

25. *See Smith,* 442 U.S. at 750 (Marshall, J., dissenting) (arguing that it was "idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative").

26. *Jones*, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

27. 824 F.3d 421 (4th Cir. 2016).

Fourth Amendment because he had "voluntarily" conveyed the information to his provider and "assumed the risk" that the provider would disclose it to the Government.[28] In reaching that holding, the court reasoned:

> *To be sure, some cell phone users may not recognize, in the moment, that they are "conveying" CSLI to their service provider. But the Supreme Court's use of the word "voluntarily" in* Smith *and* Miller *does not require contemporaneous recognition of every detail an individual conveys to a third party.*[29]

The court also relied on "the myriad of federal cases that permit the government to acquire third-party records, even when individuals do not 'actively choose to share' the information contained in those records."[30] The court reached this conclusion while recognizing the absurdity of the logical extension of *Miller* and *Smith* that was employed:

> *[A]ll routing information "records" some form of potentially sensitive activity when aggregated over time. For example, a pen register records every call a person makes and allows the government to know precisely when he is at home and who he is calling and credit card records track a consumer's purchases, including the location of the stores where he made them. . . .*
>
> *. . . .*
>
> *Technology has enabled cell phone companies . . . to collect a vast amount of information about their customers. The quantity of data at issue in this case – seven months' worth of cell phone records, spanning nearly 30,000 calls and texts for each defendant – unquestionably implicates weighty privacy interests. . . .*
>
> *. . . .*
>
> *. . . Third parties can even retain their records about us after our relationships with them end; it is their prerogative, and many business-related reasons exist for doing so. This is true even when, in the aggregate, these records reveal sensitive information similar to what could be revealed by direct surveillance. . . .*
>
> *Here, Defendants voluntarily disclosed all the CSLI at issue to Sprint/Nextel. And the very act of disclosure negated any reasonable expectation of privacy, regardless of how frequently that disclosure occurred or how long the third party maintained records of the disclosures. . . .*

28. *See id.* at 427.

29. *Id.* at 430 (internal citation omitted).

30. *Id.* at 431.

> *We recognize the appeal – if we were writing on a clean slate – in holding that individuals always have a reasonable expectation of privacy in large quantities of location information, even if they have shared that information with a phone company. But the third-party doctrine does not afford us that option. Intrinsic to the doctrine is an assumption that the quantity of information an individual shares with a third party does not affect whether that individual has a reasonable expectation of privacy. . . .*
>
> *. . . .*
>
> *. . . Indeed, although the Court formulated the third- party doctrine as an articulation of the reasonable-expectation- of-privacy inquiry, it increasingly feels like an exception. A per se rule that it is unreasonable to expect privacy in information voluntarily disclosed to third parties seems unmoored from current understandings of privacy.*[31]

In fact, despite the public uproar surrounding Edward Snowden's revelations about the infamous joint "Prism" program of the National Security Agency and Federal Bureau of Investigation, as I have previously written, the program likely passes constitutional muster under the Court's current jurisprudence.[32] A recently declassified opinion from the Foreign Intelligence Surveillance Court held that the bulk metadata collection that the program employed did not violate the Fourth Amendment because it was "squarely controlled" by *Smith*.[33]

One result of this assumption-of-risk norm has been the escalating cat-and-mouse game between the Government and high-tech consumers; the latter of whom seek technological guarantees of anonymity and encryption while the Government seeks tools to break through these protections, with the Fourth Amendment sometimes being the reward that courts bestow upon the victor.[34] The battle between the F.B.I. and Apple over Apple's proprietary encryption technology, which recently ended in an anticlimactic stalemate, is one high-profile example of how the gap in the Supreme

31. *Id.* at 434–37 (citations omitted).

32. *See* Carrie Leonetti, *Bigfoot: Data Mining, the Digital Footprint, and the Constitutionalization of Inconvenience*, 15 J. HIGH TECH. L. 260 (2015) [hereinafter "Leonetti, *Data Mining*"].

33. *In re* F.B.I. for an Order Requiring Prod. of Tangible Things from [Redacted by Court], No. BR 13-109, 2013 WL 5741573, at 2 (FISA Ct. Aug. 29, 2013). *See generally* Conor Friedersdorf, *Admit It, Rep. Sensenbrenner: You Were Wrong About the Patriot Act*, ATLANTIC (June 7, 2013) (explaining that the author of the Patriot Act believes NSA is using overbroad interpretation and threatening Americans' constitutional rights).

34. *See* Natalie Wolchover, *The Tricky Encryption That Could Stump Quantum Computers*, WIRED (Sept. 19, 2015), http://www.wired.com/2015/09/tricky-encryption-stump-quantum-computers/; Danny Yadron, *Google Allo: New Messaging App is Latest to Fight FBI over Encryption*, THE GUARDIAN (May 18, 2016), https://www.theguardian.com/technology/2016/may/18/google-allo-messaging-app-encryption-apple-fbi; *see, e.g.*, United States v. Smith, 978 F.2d 171, 180 (5th Cir. 1992) ("Although we express no opinion as to what features or circumstances would be necessary to give rise to a reasonable expectation of privacy, it should be obvious that as technological advances make cordless communications more private at some point such communication will be entitled to Fourth Amendment protection.").

Court's jurisprudence has left the solutions in the hands of programmers rather than justices.[35]

The Supreme Court's inconsistent, and sometimes illogical, understanding of the reasonableness (or unreasonableness) of particular expectations[36] is one of the reasons that some state supreme courts have rejected the Court's assumption-of-risk reasoning in interpreting their respective state constitutions. For example, in *State v. Hempele*,[37] the New Jersey Supreme Court, in declining to follow *Greenwood* in interpreting its state constitution, reasoned that, because people retain subjective privacy interests in their garbage even after placing it out for collection, the court's "abandonment" analysis was unpersuasive.[38]

I have previously argued that the geographical curtilage factors delineated in *United States v. Dunn*[39] were developed to apply primarily to rural dwellings and that this narrow application leaves urban and suburban dwellers without significant protection of their privacy or property.[40] I have also suggested that the Court's current Fourth Amendment jurisprudence is insufficient to address large scale Government data mining, particularly as it applies to Government seizure of consumers' commercial data,[41] the collection and analysis of biological evidence,[42] and "dragnet" searches, which are often justified as consensual encounters with, or third party disclosures to, the police.[43] This Article attempts to synchronize those critiques and solve the problems that they identify in one uniform stroke.

35. *See* Matt Burgess, *Apple Scores Major Win in FBI iPhone Standoff*, WIRED, (Mar. 1, 2016), http://www.wired.co.uk/article/apple-wins-fbi-iphone-new-york.

36. *See, e.g.*, United States v. Graham, 824 F.3d 421, 429 n.8 (4th Cir. 2016) (explaining that the third-party doctrine of *Miller* and *Smith* applied even to "highly private" information).

37. 576 A.2d 793 (N.J. 1990).

38. *See id.* at 808–10; *see also* State v. Joyce, 639 A.2d 1007, 1016–17 (Conn. 1994) (rejecting the State's argument that Joyce had assumed the risk that the police would seize and search his clothing when he left it by the side of the road after an emergency medical technician removed it before transporting him to the hospital for treatment); State v. Westover, 666 A.2d 1344, 1348–49 (N.H. 1995) (rejecting the State's argument that Westover had assumed the risk that the police would seize and search his sweatshirt, which contained marijuana, when he tossed it aside before entering a store). S*ee generally* State v. Earls, 70 A.3d 630, 641–42 (N.J. 2013) (explaining that New Jersey had "departed" from *Smith* and *Miller* and would not recognize the third-party doctrine).

39. 480 U.S. 294 (1987).

40. *See generally* Carrie Leonetti, *Open Fields in the Inner City: Application of the Curtilage Doctrine to Urban and Suburban Areas*, 15 GEO. MASON U. CIV. RTS. L.J. 297 (2005) [hereinafter "Leonetti, *Curtilage*"] (arguing that the factors in *Dunn* arose in, and apply primarily to, rural dwellings, thereby leaving large areas of the population without similar protections).

41. *See generally* Leonetti, *Data Mining*, *supra* note 32, at 265–70.

42. *See* Carrie Leonetti, *Code 9: Digital Data as a Fourth-Amendment Analogue for "Abandoned" DNA,* 17 COLUMBIA SCI. & TECH. L. REV. 1, 3 (2015) [hereinafter "Leonetti, *Code 9*"].

43. *See generally* Carrie Leonetti, *Motive & Suspicion:* Florida v. Jardines *and the Constitutional Right to Protection from Suspicionless Dragnet Investigations*, OHIO ST. J. CRIM. L. (forthcoming Fall 2016) [hereinafter "Leonetti, *Dragnet*"].

III. THE PROPOSED SOLUTION

The Supreme Court should overrule *Katz* and replace its expectation-of-privacy test with one that once again relies on property, and even tort, concepts like trespass,[44] nuisance,[45] theft, misappropriation, and conversion.[46] Applying these property law concepts more broadly than the pre-*Katz* trespass doctrine did would recognize that the Fourth Amendment does, in fact, protect "places" and not just reasonable people.[47] The idea of "property" can and does evolve over time. The property recognized under the test that this Article proposes should be defined with respect to the legal rights and interests that an individual challenging a Government search or

44. *See, e.g.*, Oystead v. Shed, 13 Mass. 520, 523–24 (Mass. 1816) (holding that a sheriff committed a trespass when he broke into a dwelling house to arrest a boarder who was staying inside); *cf.* Minnesota v. Olson, 495 U.S. 91, 96–97 (1990) (ruling that an authorized overnight guest had a reasonable expectation of privacy in his host's apartment because it was his temporary residence); Rakas v. Illinois, 439 U.S. 128, 143 n.12 (1978) (noting that a burglar does not have a reasonable expectation of privacy in a home into which s/he has broken and entered without permission); Chapman v. United States, 365 U.S. 610, 616 (1961) (deciding that the Fourth Amendment protected an apartment tenant, and not just the owner of the unit, against an unreasonable search of the dwelling); Amezquita v. Colon, 518 F.2d 8, 12 (1st Cir. 1975) (establishing that squatters on government land did not have a reasonable expectation of privacy in the homes that they had erected there because they had "no legal right to occupy the land").

45. *Cf.* 4 William Blackstone, Commentaries on the Laws of England in Four Books, 168 (1902) ("Eavesdroppers . . . are a common nuisance . . . ."); Adam Mossoff, *Spam—Oy, What a Nuisance!*, 19 Berkeley Tech. L.J. 625, 629 (2004) ("spam is a 'growing nuisance'").

46. *Cf.* Thyroff v. Nationwide Mut. Ins. Co., 864 N.E.2d 1272, 1278 (N.Y. 2007) (finding that the common-law cause of action of conversion applied to electronically stored records and data); Sporn v. M.C.A. Records, 448 N.E.2d 1324, 1327 (N.Y. 1983) (holding that a cause of action for conversion could exist over infringement of an intangible property right to a musical performance because the master recording that was misappropriated was a tangible item of property capable of being physically taken).

47. *Cf.* United States v. Karo, 468 U.S. 705, 714–15 (1984) (distinguishing *Knotts* and holding that the monitoring of a beeper in a private residence, whose location was not open to visual surveillance, violated the Fourth Amendment rights of those who had a cognizable privacy interest in the residence); Joshua A.T. Fairfield, *Virtual Property*, 85 B.U. L. Rev. 1047, 1050 (2005) (defining an emerging form of virtual property that is distinct from intellectual property); Alfred C. Yen, *Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace*, 17 Berkeley Tech. L.J. 1207, 1210 (2002) ("Of the many metaphors that have been applied to the Internet, the most prominent and influential has been the imagination of the Internet as a separate, new physical space known as 'cyberspace,' and its comparison to America's Western Frontier."). *Compare* Oliver v. United States, 466 U.S. 170, 183 (1984) ("The existence of a property right is but one element in determining whether expectations of privacy are legitimate."), *and Rakas*, 439 U.S. at 143 (admonishing that "arcane distinctions developed in property . . . ought not to control" the Fourth Amendment reasonableness inquiry), *and* Jones v. United States, 362 U.S. 257, 260–67 (1960) (rejecting arcane, traditional property-law distinctions in lieu of a broader understanding of property rights), *with* Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that wiretapping was not a "search" or "seizure" under the Fourth Amendment because "[t]here was no entry of the houses or offices of the defendants" to effectuate it).S*ee generally* Thomas K. Clancy, *What Does the Fourth Amendment Protect: Property, Privacy, or Security?*, 33 Wake Forest L. Rev. 307, 316 (1998) (discussing the way that pre-*Katz* Fourth Amendment doctrine protected against only tangible, physical invasions); Samuel Warren and Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 193–96 (1890) (discussing how the right to privacy evolved from its origins in the "right to life" to a broader "right to be let alone").

seizure has in relationship to the thing searched or seized.[48] This new property-based Fourth Amendment test should include intellectual and informational, as well as traditional categories of real and (tangible and intangible) personal[49] property.[50] It should prohibit not just warrantless physical intrusions, but technological intrusions, recognizing high-tech versions of trespass, nuisance, and conversion.[51] In short, it should apply to any area – geographic, online, or biological – in which an individual has a legally recognized interest into which the Government has intruded.[52] In doing

48. *Cf.* Ruckelshaus v. Monsanto Co., 467 U.S. 986, 1016 (1984) (holding that trade secrets were property such that the Government's public disclosure of them constituted a taking).

49. *Cf.* Soldal v. Cook Cty., 506 U.S. 56, 69 (1992) (holding that a seizure of property occurred whenever there was some meaningful Government interference with an individual's interest in it); Arizona v. Hicks, 480 U.S. 321, 325 (1987) (holding that moving Hicks's stereo read a barcode was a search for Fourth Amendment purposes because doing so "exposed to view concealed [property]"); United States v. Jacobsen, 466 U.S. 109, 113 (1984) (explaining that the collection of physical evidence constitutes a "seizure" for Fourth Amendment purposes when it causes a meaningful interference with an individual's possessory interests in the property collected).

50. *Cf.* Riley v. California, 134 S. Ct. 2473, 2488–89 (2014) (analogizing the contents of "modern cell phones: to personal property like "a cigarette pack, a wallet, or a purse"); Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419 (1982) (holding that New York statute authorizes a cable company to position "crossover" cables on the outside walls and roof of an apartment building without the building owner's consent constituted a "taking" of the landlord's private property under the Fifth Amendment because the cables were permanently physically occupying the building); Maureen A. O'Rourke, *Common Law and Statutory Restrictions on Access: Contract, Trespass, and the Computer Fraud and Abuse Act,* 2002 U. ILL. J.L. TECH. & POL'Y 295 (2002); Margaret J. Radin, *Property and Personhood,* 34 STAN. L. REV. 957, 958 (1982) (arguing that personal connection and self-conception justify the recognition of a property interest); Moonho Song & Carrie Leonetti, *The Protection of Digital Information and Prevention of its Unauthorized Access and Use in Criminal Law,* 28 JOHN MARSHALL J. OF COMPUTER & INFO. L. 523 (2011) (advocating the protection of the unauthorized access of intellectual property through criminal larceny laws).

51. For example, it would include sub-navigable airspace, likely requiring the Court to overturn California v. Ciraolo, 476 U.S. 207 (1986). *See* United States v. Causby, 328 U.S. 256 (1946); McCarran Int'l Airport v. Sisolak, 137 P.3d 1110 (Nev. 2006).

52. *See* Rakas v. Illinois, 439 U.S. 128, 143–44 n.12 ("One of the main rights attaching to property is the right to exclude others . . . .") (citation omitted); Denise M. Howell, *California High Court Complicates Control of Unwanted E-mails,* LEGAL BACKGROUNDER, Oct. 31, 2003, at 1 (recognizing that the tort doctrine of trespass to chattels "has become more concerned with intrusion than theft, like the analogous real property trespass" and "provides redress for conduct that does not dispossess an owner of property, but instead involves unauthorized interference with or use"); Thomas W. Merrill, *Property and the Right to Exclude,* 77 NEB. L. REV. 730, 730 (1998) (noting that the essence of a property right is the right to exclude others); *see also* Silverman v. United States, 365 U.S. 505, 512 (1961) (finding that the police had committed a Fourth Amendment "trespass" into a protected area with a high-powered microphone even though no trespass had occurred under state property law); *cf.* City of Ontario v. Quon, 560 U.S. 746, 760–65 (2010) (holding that a city police department's warrantless review of an officer's text messages was reasonable and did not violate the Fourth Amendment in part because the department owned the electronic device on which the text messages were stored); United States v. Dorais, 241 F.3d 1124, 1128 (9th Cir. 2001) ("[A] defendant has no reasonable expectation of privacy in a hotel room when the rental period has expired and the hotel has taken affirmative steps to repossess the room."); United States v. Baker, 221 F.3d 438, 442–43 (3d. Cir. 2000) (holding that Baker had a reasonable expectation of privacy in a car that he was driving with the owner's permission); United States v. Wellons, 32 F.3d 117, 119 (4th Cir. 1994)

so, it should abandon the assumption-of-risk talisman that it has read into the *Katz* test.[53]

A new property test for privacy would allow the Court to eliminate the problematic third-party doctrine of *Miller*, contents/metadata distinction of *Smith*, and the antiquated curtilage/open fields distinction of *Hester v. United States*,[54] *Oliver v. United States*,[55] and *Dunn*, some of which Justice Sotomayor recently called upon the Court to consider in *Jones:*

> *[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. . . . People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries and medications they purchase to online retailers. . . . I, for one,*

(holding that whether the driver of a rental car had a reasonable expectation of privacy therein turned on whether his/her name was on the rental contract as an authorized driver); United States v. Poulsen 41 F.3d 1330, 1337 (9th Cir. 1994) (holding that the reasonableness of Poulson's expectation of privacy in a rented foot locker turned on whether he had a right to exclude others from accessing it under state property law); United States v. Lyons, 992 F.2d 1029, 1031 (10th Cir. 1993) ("Because expectations of privacy derive in part from the right to exclude others from the property in question, lawful possession is an important consideration in determining whether a defendant had a legitimate expectation of privacy in the area searched, i.e. the hard disks."); United States v. Botelho, 360 F. Supp. 620, 624 (D. Haw. 1973) (holding that whether a tenant retained Fourth Amendment rights in a rented apartment depended on whether he had a right to occupy the premises under state property law); Chapa v. State, 729 S.W.2d 723, 728–29 (Tex. Crim. App. 1987) (en banc) (ruling that taxi passengers had a sufficiently reasonable expectation of privacy in the area under the front seat of a taxi to contest its warrantless search based on municipal ordinances in several Texas cities that gave taxi passengers the right to exclude others from the taxis in which they were riding).

53. By arguing in favor of a return to a property-based test, I do not mean to suggest that I agree with the prevailing approach that courts take to applying the *Katz* test, particularly where new investigative technologies are concerned. On the contrary, I have previously argued in favor of a different understanding of the right to privacy within the existing *Katz* framework. *See* Leonetti, *Code 9, supra* note 42 (arguing that the Court should engage in a separate expectation-of-privacy analysis for the genetic material collected from within biological evidence, analogizing DNA profiles to the contents of other containers); Leonetti, *Curtilage, supra* note 40 (arguing that the Court should take into consideration the time, place, and manner of police intrusions onto private property in determining whether they interfere with a resident's reasonable expectation of privacy); Leonetti, *Data Mining, supra* note 32 (arguing that the Court should find a reasonable expectation of privacy in the aggregate collection and searching of individuals' personal and consumer data for law enforcement purposes); Leonetti, *Dragnets, supra* note 43 (arguing that the Court should recognize that suspicionless "dragnet" investigations infringe on their target's reasonable expectation of privacy). Instead, this proposal attempts to cure the common complaints about the *Katz* test without requiring a new consensus about its application, which seems increasingly hopeless.

54. *See generally* 265 U.S. 57 (1924) (holding that the Fourth Amendment's protections did not extend to private property that constituted "open fields" beyond the curtilage of the home).

55. Oliver v. United States, 466 U.S. 170, 181 (1984) (holding that agents had not conducted a "search," for Fourth Amendment purposes, of the "open fields" beyond the curtilage of Oliver's home because he had no expectation of privacy in them).

> *doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year.*[56]

Although Justice Sotomayor joined the majority in the property rights holding of *Jones,* she made clear that she would have preferred the Court to have found that the GPS tracking was a search under *Katz* irrelevant of the placement of the device having occurred on Jones' private property.[57] Nonetheless, a robust property-based test for the Fourth Amendment would accomplish the same objectives.

The Court has begun to move its jurisprudence in a direction that makes it more amenable to this property-based shift towards increased privacy protection.[58] For example, in *Jones*, the Court held that the Government's installation of a GPS device and subsequent tracking of Jones's movements constituted a search because the police had physically invaded Jones's private property in order to plant the device "for the purpose of obtaining information."[59]

In *Florida v. Jardines*,[60] the Court relied, in part, on the law of trespass to invalidate the warrantless use of a drug-sniffing dog on Jardines' front porch.[61] In *Jardines*, which involved a physical trespass onto Jardines' property, the Court specifically rejected the assumption-of-risk and implicit consent reasoning evident in many of its earlier opinions, finding that the typical social invitation extended by the front walkway was related to the intent of the visitor and was not a blanket assumption of the risk of any person's entry.[62] The Court reasoned:

> *An invitation to engage in canine forensic investigation assuredly does not inhere in the very act of hanging a knocker. To find a visitor knocking on the door is routine (even if sometimes unwelcome); to spot that same visitor exploring the front path with a metal detector, or marching his bloodhound*

56. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring).

57. *See id.* at 954 (Sotomayor, J., concurring).

58. *Cf.* Kerr, *supra* note 5, at 809 ("Fourth Amendment doctrine has remained heavily tied to real property concepts. In most contexts, whether an expectation of privacy is deemed reasonable can be answered by whether it is backed by . . . a 'loose' version of real property law.").

59. *Jones,* 132 S. Ct. at 949.

60. 133 S. Ct. 1409, 1413 (2013) (holding that the use of a police canine to detect the presence of narcotics from the porch of Jardines's residence was an invasion of the curtilage of his home and therefore a search under the Fourth Amendment). In *Jardines,* the police responded to a tip that Jardines was growing marijuana in his home by bringing a trained drug-sniffing dog onto his porch to attempt to detect the odor of marijuana from inside the house. *See id.* When the dog "alerted" to the presence of drugs inside Jardines's home, the police obtained a search warrant for the premises, using the results of the warrantless dog sniff as a vital component of the probable cause for its issuance. *See id.*

61. *See id*. at 1414 (discussing the Court's reliance on trespass theory to invalidate the dog sniff at issue).

62. *Id.* at 1414-16.

> *into the garden before saying hello and asking permission, would inspire most of us to—well, call the police . . . [W]hether the officer's conduct was an objectively reasonable search . . . depends upon whether the officers had an implied license to enter the porch, which in turn depends upon the purpose for which they entered.*[63]

The Court concluded with the rather extraordinary statement that it "need not decide whether the officers' investigation of Jardines' home violated his expectation of privacy under *Katz*" because their physical intrusion "on Jardines' property to gather evidence [wa]s enough to establish that a search occurred."[64]

The central, albeit nonexhaustive, definition of property that this Article proposes is one that would focus on the existence of a right to exclude others (including, of course, the Government).[65] Under this robust property-based test, residents would have protection not only in their homes, their curtilage, and their tangible personal property for which they took steps deemed by courts to be sufficient to protect their expectations of privacy in them, but also in all of their real, personal, and intellectual property.[66] These property protections would come not just from the common law of property, but from statutorily vested rights to exclude, as well.[67] Apartment dwellers,

63. *Id.* at 1416 (footnote omitted).

64. *Id.* at 1417. The Court ultimately reached its conclusion on trespass, rather than expectation-of-privacy grounds, but its finding of trespass (on a front walkway) was based on the motive of the drug investigators. *See id.*

65. *See* Hodel v. Irving, 481 U.S. 704, 716 (1987) (explaining that the right to exclude others is essential to the concept of property); *cf.* Loretto v. Teleprompter Manhattan C.A.T.V. Corp., 458 U.S. 419, 426 (1982) (holding that a state statute that required landlords to allow cable-television installation on their premises for a nominal fee was a taking because the required cable equipment constituted a "permanent physical occupation" of their property); Kaiser Aetna v. United States, 444 U.S. 164 (1979) (holding that a Government order that the owners of private marina grant access to the boating public was a taking because the owners had an expectation of privacy in the marina and the order infringed on their right to exclude others).

66. *Cf.* Charles Fried, *Privacy,* 77 YALE L.J. 475, 482 (1968) (defining privacy as the "control we have over information about ourselves"). *But see* United States v. Locke, 471 U.S. 84, 105–06 (1985) (holding that a federal statute that voided unpatented mining claims when the claim holder failed to make timely annual filings was not a taking because the claim holders could have avoided the default with a minimal burden by complying with the Government's reasonable filing regulations).

67. *See* Clancy, *supra* note 47, 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."); *see, e.g.*, Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701, *et seq.* (2002) (prohibiting the unauthorized access to electronic communications in private storage facilities); Video Privacy Protection Act, 18 U.S.C. § 2710 (1988) (prohibiting the unauthorized access and disclosure of consumer video-rental information); Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030 (1986) (criminalizing unauthorized access to any computer "used in interstate or foreign commerce or communication"); Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.) (prohibiting the unauthorized interception of stored email and other Internet-based communications); Cable Communications Privacy Act, 47 U.S.C. § 551 (1984) (prohibiting the unauthorized access and disclosure of much consumer cable communications information);

therefore, would have Fourth Amendment protection from searches not only inside their individual units, but also in the common areas of the apartment property. This includes all of the areas in which the police would be trespassing if they entered without legal authorization: hallways, bike lockers, courtyards, and entryways.[68] Phone records, bank records,[69] commercial consumer data, the contents of cell phones and other electronic devices, a hacked or fraudulently accessed Facebook page, even the genetic profile from shed DNA[70]: these could all be protected as private "property,"[71] for the invasion of which the police would need a warrant issued on

Right to Financial Privacy Act, 12 U.S.C. §§ 3401-22 (1978) (prohibiting the unauthorized access and disclosure of bank records in response to *Miller*); ALASKA STAT. § 18.13.010-100 (2015) (requiring written consent from individuals before their DNA can be collected, analyzed, or retained or the results of the analysis can be disclosed); CAL. BUS. & PROF. CODE § 17529 (2016) (prohibiting unsolicited commercial email); CAL. PENAL CODE § 632 (criminalizing the surreptitious electronic recording of conversations) (1994); COLO. REV. STAT. § 10-3-1104.7(1)(a) (2013) ("[g]enetic information is the unique property of the individual to whom the information pertains"); FLA. STAT. § 760.40 (2010) (criminalizing DNA theft); FLA. STAT. § 934.03(3)(d) (2010) (criminalizing the surreptitious electronic recording of conversations); MD. CODE, CTS. & JUD. PROC. § 10-402(C)(3) (2016) (criminalizing the surreptitious electronic recording of conversations without the consent of both parties); 18 PA. CONS. STAT. § 5703 (2002) (criminalizing the surreptitious electronic recording of conversations); *cf.* Michael J. Madison, *Rights of Access and the Shape of the Internet,* 44 B.C. L. REV. 433, 434–45 (2003) (discussing "Internet-as-place" metaphor and concluding that, for legislators, "a rule of 'exclusion-from-computer' naturally assumes a rule of 'exclusion- from-information'").

68. *Cf.* Donovan v. Lone Steer, Inc., 464 U.S. 408 (1984) (holding that the Fourth Amendment did not apply to a fire inspector's inspection of a hotel lobby because the proprietor lacked a reasonable expectation of privacy in an area that was open to the public).

69. *Cf.* Phillips v. Wash. Legal Found., 524 U.S. 156 (1998) (holding that the short-term interest that clients earned on their legal retainers was property for takings purposes).

70. *Cf.* Moore v. Regents of the Univ. of Cal., 793 P.2d 479 (Cal. 1990) (addressing an individual's claim that genetic material was personal property).

71. *See, e.g.,* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–84 (1st Cir. 2001) (holding that Explorica's use of a software program to extract tour codes and prices from the website of a tour company violated § 1030(a)(4) of the CFAA); AOL, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 896–99 (N.D. Iowa 2001) (holding that an AOL member's harvesting of the addresses of other AOL members for the purpose of sending unsolicited bulk commercial e-mails was a trespass and violated § 1030(a)(2)(C) of the CFAA); AOL, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1277, 1279–80 (N.D. Iowa 2000) (recognizing a trespass based on National Health Care's sending of bulk e-mail through AOL's servers); eBay v. Bidder's Edge, 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (enjoining Bidder's Edge from using an automated program that aggregated data from eBay's auction web site based on a theory of trespass); CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (holding that Cyber Promotion's unauthorized spamming of CompuServe's system with bulk emails constituted a trespass to private property); *see also* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 396–97, 404 (2d Cir. 2004) (affirming the district court's preliminary injunction against Verio's use of automated software to extract information about new domain-name registrants from a public database for solicitation purposes). *But see* Intel Corp. v. Hamidi, 71 P.3d 296, 299–300 (Cal. 2003) (declining to find an action in tort for trespass to chattels based on Hamidi's hostile mass emailing of Intel's employees via its servers because the servers were not physically damaged).

probable cause (or circumstances amounting to an exception to the warrant requirement).[72]

The threshold test for the Fourth Amendment would be whether the subject of an investigatory intrusion has a property-like interest recognized by the law – a law expressly creating it, existing rules and understandings, and/or background principles of property law.[73] Because the existence of Fourth Amendment protection would depend upon recognition of the area intruded in a legal source independent of the Fourth Amendment, this new test would empower Congress and state legislators to "create" zones of Fourth Amendment protection by enacting statutory property protections for areas and items upon which they wanted to confer special protection.[74]

Of course, there are tradeoffs to restricting the Government's investigatory tools, but this new-property protection would not be all encompassing or prevent all forms of Government investigation. Courts would still be able to develop limited exceptions to a property-based rule, as they have in other property law contexts, some of which overlap substantially with existing Fourth Amendment exceptions.

Copyright law has a doctrine of fair use, which can provide an affirmative defense to infringement when the alleged infringer can demonstrate that its use of copyrighted material should be protected.[75] The fair-use defense to copyright

72. *Cf.* A. Michael Froomkin, *The Death of Privacy?*, 52 STAN. L. REV. 1461, 1463, 1467 (2000) (describing "informational privacy" as "the ability to control the acquisition or release of information about oneself"); Paul Ohm, *The Fourth Amendment Right to Delete*, 119 HARV. L. REV. F. 10 (2005) (arguing that private property rights include a legally cognizable right to dispose of property, which includes the deletion of electronic files, and concluding that the unauthorized copying and preserving of an individual's data files infringes on that right).

73. Takings law has an analogous predicate, since the Takings Clause is only implicated when the Governments takes "property" that has been recognized as such. *See* United States v. Willow River Power Co., 324 U.S. 499, 502 (1945); Colvin Cattle Co., Inc. v. United States, 468 F.3d 803, 806 (Fed. Cir. 2006). *See generally* Robert Meltz, *Takings Law Today: A Primer for the Perplexed,* 34 ECOLOGY L.Q. 307, 317–18 (2007).

74. *See* United States v. Jones, 132 S. Ct. 945, 964 (Alito, J., concurring) ("A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."); United States v. Graham, 824 F.3d 421, 438 (Wilkinson, J., concurring) ("For good reason, developing constitutional meaning has always been a collaborative enterprise among the three departments of government."). For example, Congress passed the ECPA to prevent the "unauthorized interception of electronic communications" and "update and clarify Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies." S. REP. NO. 99-541, at 1 (1986). Violation of these federal statutes is of limited importance in criminal prosecutions because suppression of evidence is rarely required for a violation of the ECPA amendments to the Wiretap Act and is explicitly precluded by the SCA, which authorizes solely civil remedies for its violation. *See* Leonetti, *Code 9, supra* note 42, at 25 n.79; *cf.* Dow Chem. Co. v. United States, 476 U.S. 227, 232 (1986) (rejecting Dow's claim that trade-secrets statutes, which protected the privacy of its facility, were relevant to determining the constitutionality of the Government's warrantless aerial surveillance of two of its power plants in a chemical-manufacturing facility).

75. *See* Harper & Row Publishers, Inc. v. Nation Enter., 471 U.S. 539 (1985) (recognizing an affirmative defense of fair use in a lawsuit involving an article that revealed portions of President Ford's memoirs before they were released); Chi. Bd. of Educ. v. Substance, Inc., 354 F.3d 624, 629 (7th Cir. 2003) (explaining that a copier bore the burden to demonstrate fair use).

infringement is analogous to the consent defense in real property law.[76] Fourth Amendment doctrine could develop a similar excuse for intrusions into new property, of which the Government could avail itself if it could overcome a presumption of protection and prove, for example, that the property owner consented to the intrusion.

Necessity has long been recognized as a defense to actions that would otherwise constitute trespass and related torts.[77] The traditional necessity defense allowed private actors to violate the property rights of others (even criminally) when human life was at stake.[78] Courts could develop an analogous doctrine of reasonableness and flexibility for necessary Government intrusions into this newly constitutionalized property when the intrusion is the lesser of evils.

In another exception to the sanctity of private property, the Government has the power of eminent domain to condemn private property for public use when doing so benefits the greater good and just compensation is paid to the owner.[79] The

76. *See* Ned Snow, *The Forgotten Right of Fair Use*, 62 CASE W. RES. L. REV. 135, 160 (2011); *see, e.g.*, Envtl. Processing Sys. v. F.P.L. Farming, Ltd., 457 S.W.3d 414 (Tex. 2015) (holding that lack of consent was an element of a claim for trespass).

77. *See generally* United States v. Bailey, 444 U.S. 394, 410 (1980) (describing the necessity defense); United States v. Schoon, 971 F.2d 193, 195 (9th Cir. 2001) (addressing a "systematic reason for the complete absence of" necessity defenese in federal caselaw). Necessity is often, but mistakenly, confused with duress, which would not likely constitute a "defense" to an invasion of property by the Government. *See Bailey,* 444 U.S. at 410 (explaining the difference between necessity and duress).

78. *See* MODEL PENAL CODE § 3.02 (codifying the principle of necessity as a justification for otherwise criminal conduct); WAYNE R. LAFAVE, CRIM. LAW, § 5.4, at 476–77 (3d ed. 2000); Edward B. Arnolds & Norman M. Garland, *The Defense of Necessity in Criminal Law: The Right to Choose the Lesser Evil*, 65 J. CRIM. L. & CRIMINOLOGY 289, 291–93 (1974).

79. *See* U.S. CONST., amend. V ("[N]or shall private property be taken for public use, without just compensation."); *see, e.g.*, Keystone Bituminous Coal Ass'n v. DeBenedictis, 480 U.S. 470, 488, 492 (1987); United States v. Central Eureka Mining Co., 357 U.S. 155, 168–69 (1958) (holding that a Government shutdown of Central Eureka's gold mines was not a taking for constitutional purposes because it was justified by wartime rationing); Block v. Hirsh, 256 U.S. 135, 157 (1920) (holding that wartime rent controls was not a taking for constitutional purposes in part because of the emergency nature of wartime); Phillip Morris, Inc. v. Reilly, 312 F.3d 24 (1st Cir. 2002) (en banc). This is not, however, intended as an invitation for the Court to return to its current broad reasonableness "balancing." *See, e.g.*, Nat'l Treasury Emp. Union v. Von Raab, 489 U.S. 656, 679 (1989) (upholding the warrantless drug testing of all high-level Customs Service employees because of the balance of interests involved); Skinner v. Ry. Labor Execs. Ass'n, 489 U.S. 602, 633–34 (1989) (concluding that it did not violate the Fourth Amendment rights of railroad employees for their private employers to conduct warrantless urinalysis of their blood alcohol concentration after all accidents at the Government's behest without a warrant because of the balance of relevant interests involved); Griffin v. Wisc., 483 U.S. 868, 880 (1987) (upholding as reasonable the warrantless search of Griffin's home by his probation officer who had reasonable suspicion, but not probable cause, to believe that he had violated the terms of his probation based on the balance of interests involved); O'Connor v. Ortega, 480 U.S. 709, 729 (1987) (remanding the case to be analyzed under the balancing test when an employee's office was searched under reasonable suspicion, but without probable cause or a warrant); New Jersey v. T.L.O., 469 U.S. 325, 347–48 (1985) (upholding as reasonable the warrantless search of a student's purse on reasonable suspicion, in the absence of probable cause, based on a balancing of the interests

constitutional prohibition against the Government's powers of eminent domain includes an exception when the owner of the encroached property consents to the encroachment.[80] It also includes exceptions for "highly regulated fields,"[81] abandoned property,[82] and "actual necessity," the latter of which overlaps substantially with the "hot pursuit"[83] and "burning building"[84] varieties of the current exigent-circumstances exception to the warrant requirement. The limitations on the Government's takings power overlap substantially with substantive due process limitations on governmental conduct.[85] In this way, this new property proposal

involved); Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (permitting a stop and protective frisk of a suspect for weapons on reasonable suspicion, rather than probable cause, because the reasonableness clause of the Fourth Amendment was the benchmark for assessing constitutionality of an investigatory procedure). *But see* Camara v. Mun. Court, 387 U.S. 523 (1967) (holding that the inspection of homes by safety inspectors without probable cause or without warrants violates the Fourth Amendment).

80. *See* Yee v. City of Escondido, 503 U.S. 519, 527–28 (1992) (holding that voluntarily renting your land to mobile home owners does not amount to a per se governmental taking); F.C.C. v. Florida Power Corp., 480 U.S. 245, 252–53 (1987) (holding that the FCC's installation of utility poles did not constitute as a per se governmental taking). *But see* Loretto v. Teleprompter Manhattan CATV Corp., 458 U.S. 419, 439 n.17 (1982) (holding that a landlord's option to cease renting a building did not mean that it had voluntarily consented to its taking by the Government by failing to do so).

81. *Compare* California Housing Sec. v. United States, 959 F.2d 955, 960 (Fed. Cir. 1992) (holding that the Government's seizure of a failed savings and loan was not a taking requiring just compensation because it was in keeping with customary expectations in the industry), *with Skinner,* 489 U.S. at 627 (concluding that the warrantless testing of railroad employees blood alcohol concentrations did not violate the Fourth Amendment in part because they had voluntarily accepted employment in a pervasively regulated industry), *and* United States v. Burger, 482 U.S. 691, 703–04 (1987) (upholding a New York statute that authorized frequent warrantless inspections of licensed "chop shops" because they were part of a pervasively regulated industry), *and* United States v. Biswell, 406 U.S. 311, 316 (1972) (upholding the warrantless inspection of a federally licensed gun dealer's showroom because selling firearms was a "pervasively regulated business"), *and* United States v. Castelo, 415 F.3d 407, 409–10 (5th Cir. 2005) (upholding the warrantless weighing and inspection of commercial trucks operating on state highways because trucking was a heavily regulated industry).

82. *See, e.g.*, Texaco, Inc. v. Short, 454 U.S. 516 (1982) (holding that a State statute extinguishing the property rights of owners of mineral estates that had gone unused for a long time was not a taking because it was the owners' failure to use the mineral estates that caused their property rights to lapse).

83. *See* Customer Co. v. Sacramento, 895 P.2d 900, 910–11 (Cal. 1995) (noting that officers must be permitted to respond to emergency situations which danger the public without being hampered by constitutionally-mandated liability for damage to private property that result from their duties); Warden v. Hayden, 387 U.S. 294, 298–99 (1967) (holding that a warrantless search of a robbery suspect's house, including a washing machine where he could have concealed his gun, did not violate the Fourth Amendment because the officers were in "hot pursuit" of the suspect at the time).

84. *Compare* Bowditch v. Boston, 101 U.S. 16, 18–19 (1880) (recognizing an exception to the prohibition against uncompensated takings to prevent the spreading of a fire or to forestall other grave threats to the lives and property of others), *with* Michigan v. Tyler, 436 U.S. 499, 509–10 (1978) (holding that fire fighters could enter a burning building and remain on the premises for a reasonable amount of time without a warrant to put out and investigate the cause of the fire without violating the Fourth Amendment).

85. *See* Meltz, *supra* note 73, at 313.

overlaps, at least in practice, with other scholars' proposals regarding due process as a limitation on the Government's powers of search and seizure.[86]

Of course, if courts applied these necessity-based exceptions to a new constitutionalized property test under the Fourth Amendment, the new test could be just as malleable and poor at protecting privacy in a high-tech world as the current *Katz* test. All of these property-law exceptions, however, would be narrower than the current exceptions under the *Katz* test's assumption-of-risk concepts, under which courts often find Government intrusions not to be searches and seizures at all or dictate that interested parties have defaulted any rights in such property.[87] In comparison to the current *Katz* test, the test proposed in this Article would be doctrinally cleaner and more predictable in its application, because a Government trespass would be recognized as a search for Fourth Amendment purposes, even if, for example, it was justified as the lesser of two evils. A property-based test, even with exceptions, would also be more privacy-protective because it would employ more presumption (that Government conduct is a search that requires a warrant issued on the basis of probable cause) and less rebuttability (currently embodied in the Court's reasonableness-balancing jurisprudence, under which exceptions to the warrant requirement often swamp its rule)[88] than that of current jurisprudence. In doing so, this property-based test would recognize the social value to protecting privacy in the property that matters most to people today and would be more consistent with current social norms.[89]

86. *See, e.g.*, Herman, *supra* note 4.

87. *See supra,* Section II.

88. *Cf.* Swire, *supra* note 4. While the Court often pronounces that the exceptions to the warrant requirement are supposed to be limited and disfavored, that pronouncement has become more of a disclaimer to be added automatically before recognition of yet another of its "narrow" exceptions. *See, e.g.,* Kentucky v. King, 563 U.S. 452, 459 (2011) (noting that the Fourth Amendment generally required a search warrant issued on the basis of probable cause then holding that it permitted warrantless entry into King's home to prevent the destruction of evidence as long as the police did not create the exigency through an actual or threatened Fourth Amendment violation); California v. Acevedo, 500 U.S. 565, 580 (1991) (noting that warrantless searches were *per se* unreasonable under the Fourth Amendment, subject only to a few specifically established and well-delineated exceptions, then holding that probable cause to search a vehicle justified the warrantless search of any containers therein); Horton v. California, 496 U.S. 128 (1990) (noting that warrantless searches were *per se* unreasonable under the Fourth Amendment, subject only to a few specifically established and well-delineated exceptions, then holding that the Fourth Amendment did not prohibit the warrantless seizure of evidence in plain view, even if the discovery of the evidence was not inadvertent); United States v. Robinson, 414 U.S. 218 (1973) (holding that a search of Robinson's person without a search warrant, the inspection of a crumpled cigarette package found on his person, and the seizure of heroin capsules found in the package were permissible).

89. *Cf. Thyroff,* 864 N.E.2d at 1277 ("[S]ociety's reliance on computers and electronic data is substantial, if not essential."); Ariana Eunjung Chung, *After Death, Fight for Digital Memories,* WASH. POST, Feb. 3, 2005, at A1.

IV. CONCLUSION

High-tech invasions of privacy inflict serious harms that demand a more appropriate legal remedy than the one crafted half a century ago in a concurring opinion. The law of property has a more constructive role to play in modern Fourth Amendment jurisprudence than old concepts of reasonableness. A new doctrine of Fourth Amendment property could serve as a unifying principle to rationalize and expand the Amendment's privacy protections. As Richard Epstein has noted, in a different context:

> *One dividend of strong trespass rules is that they protect the privacy of the property owners, as they did even before privacy counted as an independent legal interest. . . . Everyone is, in the long run, better off if no one is in a position to snoop, so that by operation of law, boundaries of property are extended outward incrementally to accommodate that result.*[90]

90. Richard A. Epstein, *Cybertrespass,* 70 U. Chi. L. Rev. 73, 75–76 (2003).