Washington Law Review

Volume 92 | Number 4

12-1-2017

Orwell's *1984* and a Fourth Amendment Cybersurveillance Nonintrusion Test

Margaret Hu

ORWELL'S *1984* AND A FOURTH AMENDMENT CYBERSURVEILLANCE NONINTRUSION TEST

Margaret Hu*

Abstract: This Article describes a cybersurveillance nonintrusion test under the Fourth Amendment that is grounded in evolving customary law to replace the reasonable expectation of privacy test formulated in *Katz v. United States*. To illustrate how customary law norms are shaping modern Fourth Amendment jurisprudence, this Article examines the recurrence of judicial references to George Orwell's novel, *1984*, within the Fourth Amendment context when federal courts have assessed the constitutionality of modern surveillance methods. The Supreme Court has indicated that the Fourth Amendment privacy doctrine must now evolve to impose meaningful limitations on the intrusiveness of new surveillance technologies.

A cybersurveillance nonintrusion test implicitly suggested by the Supreme Court in *United States v. Jones* first shifts the vantage point of the Fourth Amendment analysis from an individual-based tangible harm inquiry to an inquiry of a society-wide intangible harm—whether the modern surveillance method creates a "*1984* problem" for society. A cybersurveillance nonintrusion test requires the government to justify the intrusion of the surveillance on society. A new test would remediate increasingly ineffective Fourth Amendment jurisprudence currently grounded in property and tort law. The Article argues that the adoption of a cybersurveillance nonintrusion test and the abandonment of the current privacy test is not only required; but, in practice, is already used by the federal courts.

---

* Associate Professor of Law, Washington and Lee University School of Law. I deeply appreciate the helpful comments from and conversations with those who have generously taken the time to help me with this work, including Jack Balkin, Bill Banks, Kate Bartlett, Alvaro Bedoya, Stuart Benjamin, Joseph Blocher, Jamie Boyle, Dru Brenner-Beck, Ryan Calo, Guy Charles, Bobby Chesney, Jack Chin, Geoff Corn, Andrew Christensen, Michael Dreeben, Charlie Dunlap, John Eller, Josh Fairfield, Nita Farahany, Michael Froomkin, David Gray, Lisa Griffin, Amos Guiora, Mitu Gulati, Keith Guzik, Larry Helfer, Stephen Henderson, John Inazu, Trina Jones, Jj Kidder, Steve Leckar, Maggie Lemos, Rachel Levinson-Waldman, Erik Luna, Tim MacDonnell, Bill Marshall, Marc Miller, Russ Miller, Steve Miskinis, Lise Nelson, Jeff Powell, Jed Purdy, Arti Rai, Christopher Slobogin, Dan Tichenor, Ernie Young, and apologies to anyone whom I may have inadvertently omitted. I am also grateful for the feedback received from participants at the Yale Law Information Society Project's Ideas Lunch; the Duke Law Faculty Workshop; the Duke Law Junior Faculty Summer Scholarship Retreat; the National Security Law Faculty Workshop, jointly hosted by the University of Texas School of Law and South Texas College of Law; the surveillance and society panel discussion at the Law and Society Annual Conference; the domestic terrorism panel discussion at the Law, Ethics, and National Security (LENS) Conference hosted at Duke Law; the "Politics of Surveillance" symposium, hosted by the Wayne Morse Center for Law and Politics at the University of Oregon School of Law; and the "Transatlantic Dialogue on Surveillance Methods" Symposium hosted by the Max-Planck Institute in Freiburg, Germany. For their excellent research assistance, I would like to thank Rossana Baeza, Emily Bao, Lauren Bugg, Russell Caleb Chaplain, Mark Dewyea, Alexandra Klein, and Carroll Neale. All errors and omissions are my own. Finally, many thanks to the *Washington Law Review* for their wonderful editorial care.

INTRODUCTION

The disclosures provided by former National Security Agency (NSA) contractor Edward Snowden[1] revealed a pervasive post-9/11 surveillance apparatus[2] and rapidly proliferating cybersurveillance[3] architectures.[4]

---

1. *See generally* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014) (discussing in detail the history of the Snowden disclosures).

2. Scholars and experts have examined the legal implications of the mass surveillance activities of the NSA and the intelligence community in work both preceding and following the disclosures of former NSA contractor Edward Snowden. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 759–72 (2014) (describing NSA mass surveillance before and after the Snowden disclosures); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 4, 22–41 (2015) (outlining the origins of current NSA programs and the relevant authorities); Margot E. Kaminski & Shane Witnov, *The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech*, 49 U. RICH. L. REV. 465, 5–31 (2015) (applying First Amendment implications of surveillance programs); Orin S. Kerr, *A Rule of Lenity for National Security Surveillance Law*, 100 VA. L. REV. 1513, 2–22 (2014) (arguing that Congress should adopt a rule of narrow construction of the surveillance statutes); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Content Collection After Snowden*, 66 HASTINGS L.J. 1, 1–76 (2014) (outlining a dynamic conception of national security surveillance justifying programs disclosed by Snowden but calling for increased transparency and accountability); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269, 271–90 (2012) (proposing an intra-agency separation of powers pitting part of the Justice Department against itself, creating competition for interpretations of statutory and constitutional surveillance law); Margo Schlanger, *Intelligence Realism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L SEC. J. 112, 116–206 (2015) (describing how the "intelligence legalism" phenomenon offers inadequate protection of individual liberties); Christopher Slobogin, *Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine*, 102 GEO. L.J. 1721, 1722–26 (2014) (arguing that any legislative delegation to law enforcement should be subject to several prerequisites); Omer Tene, *A New Harm Matrix for Cybersecurity Surveillance*, 12 COLO. TECH. L.J. 391, 392–403 (2014) (outlining new parameters for analysis of the privacy impact of communications monitoring programs); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 843–901 (2014) (explaining how the multiplicity of surveillance techniques is eroding the notice restraints on illegal searches); Stephen I. Vladeck, *Big Data Before and After Snowden*, 7 J. NAT'L SEC. L. & POL'Y 333, 334 (2014) (noting that some of the most well-known programs were "the PRISM program under section 702, and the bulk telephone metadata program under section 215 of the USA PATRIOT Act"); Stephen I. Vladeck, *Standing and Secret Surveillance*, 10 I/S: J.L. & POL'Y FOR INFO. SOC'Y 551, 575–77 (2014) (noting pitfalls of legal challenges to NSA programs).

3. *See* LAWRENCE LESSIG, CODE VERSION 2.0, at 209 (2006) (describing cybersurveillance or "digital surveillance" as "the process by which some form of human activity is analyzed by a computer according to some specified rule. . . . [T]he critical feature in each [case of surveillance] is that a computer is sorting data for some follow-up review by some human"); Mark Andrejevic, *Surveillance in the Big Data Era*, *in* EMERGING PERVASIVE INFORMATION AND COMMUNICATION TECHNOLOGIES (PICT): ETHICAL CHALLENGES, OPPORTUNITIES, AND SAFEGUARDS 55, 56 (Kenneth D. Pimple, ed. Law, Governance and Technology Ser. No. 11, 2014) (explaining that big data surveillance is defined by "the imperative . . . to monitor the population as a whole" because "otherwise it is harder to consistently and reliably discern useful patterns"); David Lyon, *Surveillance, Snowden and Big Data: Capacities, Consequences, Critique*, 1(2) BIG DATA & SOC. 1 (2014).

Prior to these revelations, the Supreme Court had already signaled that existing Fourth Amendment doctrine must evolve to accommodate limitations on government intrusiveness in light of increasingly comprehensive and invasive cybersurveillance technologies.[5] In both

4. Experts increasingly describe big data surveillance or cybersurveillance in architectural terms. *See, e.g.*, JENNIFER STISA GRANICK, AMERICAN SPIES: MODERN SURVEILLANCE, WHY YOU SHOULD CARE, AND WHAT TO DO ABOUT IT (2017); BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 48 (2015) ("This has evolved into a shockingly extensive, robust, and profitable surveillance architecture."); Margaret Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV. 773, 788, 813, 816, 832 (2015) (describing the architecture of cybersurveillance and its proponents' aspirations); Margaret Hu, *Taxonomy of the Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679, 1690 (2015) ("Under big data cybersurveillance architecture, big data tools appear to track and isolate suspicious data and not suspicious persons."); GREENWALD, *supra* note 1, at 90–120 (exploring the cooperation between private industry and the NSA). Several important works have been published in recent years, shedding light on mass surveillance technologies as well as the policy and programmatic framework of cybersurveillance and covert intelligence gathering. *See, e.g.*, JULIA ANGWIN, DRAGNET NATION: A QUEST FOR PRIVACY, SECURITY, AND FREEDOM IN A WORLD OF RELENTLESS SURVEILLANCE 17–18 (2014) (describing how the government, private companies, and even criminals use technology to indiscriminately collect vast amounts of personal data); SHANE HARRIS, @WAR: THE RISE OF THE MILITARY-INTERNET COMPLEX (2014) (describing the unique threat of cyber threats); SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE (2010) (detailing the acceleration of mass surveillance in the U.S.); ROBERT O'HARROW, JR., NO PLACE TO HIDE 34, 145 (2006) (describing the architecture of databases containing vast amounts of personal data); DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 158–80 (2011) (detailing the vulnerability of the big data surveillance network); JEFFREY ROSEN, THE NAKED CROWD: RECLAIMING SECURITY AND FREEDOM IN AN ANXIOUS AGE 147 (2004) (surveying post-9/11 surveillance architecture and questioning whether justification outweighs risks to constitutional democracy).

5. *See, e.g.*, Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2477 (2014) (stating that a warrantless search is reasonable only if it falls within a specific exception to the Fourth Amendment's warrant requirement); United States v. Jones, 565 U.S. 400, 402–13 (2012) (concluding that the government's installation of a GPS device on defendant's vehicle constituted a "search" within the meaning of the Fourth Amendment). A number of scholars have discussed the transformation of the Fourth Amendment in response to technological developments. *See, e.g.*, Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 177 (arguing that Fourth Amendment precedent supports judicial recognition of a reasonable expectation of privacy in stored email that accords warrant-level protection); Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1, 51–83 (2005) (considering how privacy guarantees can be adapted in light of ubiquitous technology); Deven R. Desai, *Constitutional Limits on Surveillance: Associational Freedom in the Age of Data Hoarding*, 90 NOTRE DAME L. REV. 579, 591–632 (2014) (examining the implications of the growing technology of backward-looking surveillance for Fourth Amendment jurisprudence); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181, 1181–1328 (2016) (arguing that reclaiming the original meaning of the Fourth Amendment is essential for understanding the scope of its protections in the face of new technologies); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 805–80 (2016) (arguing that the Fourth Amendment's existing language can be adapted to address new surveillance technologies); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 547–631 (2017) (suggesting using the principle of informational security as the organizing framework for a digital Fourth Amendment); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of*

United States v. Jones,[6] a decision that preceded the Snowden revelations, and *Riley v. California*,[7] a decision issued in the immediate aftermath of the revelations, the Supreme Court has struggled with adapting Fourth Amendment[8] jurisprudence to modern surveillance technologies.[9]

The development of a new legal privacy doctrine supplanting the groundbreaking "reasonable expectation of privacy" test established in

---

Law, Not Fact, 70 MD. L. REV. 681, 681–749 (2011) (concluding that courts should decide, per constitutional precedent, that applications for location data must satisfy the probable cause standard of the Fourth Amendment's warrant requirement); David Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. 1181, 1181–205 (2015) (arguing that rights guaranteed by the Fourth Amendment are collective rather than individual); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 101–26 (2013) (proposing that developers of surveillance technologies should include constraints on the aggregation and retention of data along with use and access limitations to provide a framework of Fourth Amendment pre-commitments preserving law enforcement interests while minimizing threats to privacy); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 978–1026 (2007) (arguing for the adoption of practical applications delineated in divergent state jurisprudence to protect third-party information); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 285–329 (2015) (considering how Fourth Amendment law should adapt to the global nature of Internet-based surveillance); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 311–54 (2012) (proposing a "mosaic theory" of the Fourth Amendment, under which courts evaluate a collective sequence of government action as an aggregated whole to consider whether the activity constitutes a search); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527, 527–615 (2017) (outlining a new, multifaceted approach for both courts and law enforcement to utilize when determining whether the Fourth Amendment is implicated by public surveillance); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393, 1393–437 (2002) (arguing for the adoption of a proportionality principle dictating that "search" be defined broadly for Fourth Amendment purposes); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1513–15 (2010) (arguing that courts' current approach to the Fourth Amendment has "led to a complicated morass of doctrines and theories" and also ignored problems caused by "inadequately constrained government power, lack of accountability of law enforcement officials, and excessive police discretion").

6. 565 U.S. 400 (2012).

7. __ U.S. __, 134 S. Ct. 2473 (2014).

8. The Fourth Amendment of the U.S. Constitution 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."

U.S. CONST. amend. IV.

9. *See generally* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016); DAVID GRAY, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017); Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757 (1994); Anthony G. Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349 (1974).

1967 by *Katz v. United States*[10] has yet to occur.[11] The *Katz* test formulated fifty years ago remains intact and presents a foundational inquiry for the development of all modern Fourth Amendment privacy jurisprudence. Yet, that test does not appear to be offended by cybersurveillance and dataveillance[12] tools. Emerging surveillance tools are capable of subjecting all citizens and noncitizens alike to mass, suspicionless criminal and national security profiling through the amassing and analysis of potentially limitless and comprehensive digitized data.[13]

This Article argues that, in the absence of new Fourth Amendment doctrine, federal courts, including the Supreme Court, are guided by cultural norms about what constitutes overreaching or unreasonable government surveillance. To illustrate this customary law[14] dimension of current Fourth Amendment jurisprudence, this Article examines the consistent recurrence of Orwellian rhetoric in judicial hearings and decisions analyzing the constitutionality of emerging cybersurveillance techniques and technologies. For example, George Orwell's novel *1984*[15]

---

10. 389 U.S. 347 (1967).

11. *See id.* at 361 (Harlan, J., concurring); Erwin Chemerinsky, *Is It Time To Go High-Tech on the Fourth Amendment?*, ABA J. (Feb. 4, 2014), http://www.abajournal.com/news/article/chemerinsky_is_it_time_to_go_high_tech_on_the_fourth_amendment/ [https://perma.cc/MS2H-NWT4] ("On Jan. 17, [2014,] the U.S. Supreme Court granted certiorari in two cases that hopefully will force it to bring the Fourth Amendment into the 21st Century. . . . The court has had the chance to deal with this question in recent years and has failed to do so.").

12. Roger Clarke is credited with introducing the term "dataveillance" and defines dataveillance as systematic monitoring or investigation of individuals' actions, activities, or communications through the use of information technology. *See* Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. ACM 498, 499 (1988).

13. *Id.* For an excellent overview of the types of data collected and analyzed by the government for criminal and national security profiling, see RACHEL LEVINSON-WALDMAN, BRENNAN CTR. FOR JUSTICE, WHAT THE GOVERNMENT DOES WITH AMERICANS' DATA (2013). For a summary of the implications of big data surveillance, see VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK (2013); Anita L. Allen, *Protecting One's Own Privacy in a Big Data Economy*, 130 HARV. L. REV. F. 71 (2016); Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1094 (2013); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

14. Customary law "is generally considered to have two elements: state practice and *opinio juris.* State practice refers to general and consistent practice by states, while *opinio juris* means that the practice is followed out of a belief of legal obligation." Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AM. J. INT'L LAW 757, 757 (2001) (citing RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 102(2) (AM. LAW INST. 1987)); *see also* IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 4–11(5th ed. 1998); MICHAEL BYERS, CUSTOM, POWER, AND THE POWER OF RULES 130 (1999); ANTHONY A. D'AMATO, THE CONCEPT OF CUSTOM IN INTERNATIONAL LAW 49 (1971).

15. GEORGE ORWELL, 1984 (1949).

was invoked during the Supreme Court oral argument in *United States v. Jones* on at least six separate occasions.[16] Often, the *1984* "parade of horribles" rhetoric allows the federal judiciary to depart from settled Fourth Amendment precedent to restrain the government surveillance method or cybersurveillance program in question. *Jones* addressed the constitutionality of warrantless GPS tracking, yet it is significant to note that other cases in lower federal courts addressing the government's bulk telephony metadata surveillance program—the first NSA program revealed by the Snowden disclosures[17]—have provoked a similar reaction, with a district court explicitly referring to the NSA program as "almost-Orwellian."[18]

Under customary law, established community standards or social norms that can be construed as objectively verifiable and long-standing are given the force of law.[19] Customary international law, to take one example, enshrines universal or nearly universal principles of human rights into a well-recognized body of customary law: international human rights law.[20] Customary domestic law has been defined as "the common

16. Transcript of Oral Argument at 13, 25, 27, 33, 35, 57, United States v. Jones, 565 U.S. 400 (2012) (No. 10-1259).

17. Klayman v. Obama, 957 F. Supp. 2d 1, 10 (D.D.C. 2013).

18. *Id.* at 33 (holding that the NSA's bulk telephony metadata surveillance program was "almost-Orwellian" and likely to be violative of the Fourth Amendment). Judge Leon of the District Court of D.C. stated: "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval." *Id.* at 42.

19. Although customary law is often associated with "Customary International Law," some scholars have explored the "Customary Domestic Law" dimension of customary law. *See, e.g.*, Katharine T. Bartlett, *Tradition as Past and Present in Substantive Due Process Analysis*, 62 DUKE L.J. 535, 540 (2012) (explaining how tradition is a limiting principle operating as a limiting criterion "prevent[ing] courts from substituting their own subjective preferences for those of the legislatures" who "are free to depart from tradition" whereas "courts are not"). Moreover, the concepts of "constitutional conscience," "constitutional redemption," and "constitutional conventions" arguably embody customary law principles. *See, e.g.*, JACK M. BALKIN, CONSTITUTIONAL REDEMPTION 35 (2011) (explaining how constitutional law develops via various constructions, institutions, statutes, and practices that have built up around the text); H. JEFFERSON POWELL, CONSTITUTIONAL CONSCIENCE: THE MORAL DIMENSION OF JUDICIAL DECISION, 80–103 (2008) (contending that the Constitution requires judges to decide cases in good faith, using the "constitutional virtues" of candor, intellectual honesty, humility about the limits of constitutional adjudication, and willingness to admit that they do not have all the answers); Curtis A. Bradley & Neil S. Siegel, *Historical Gloss, Constitutional Conventions, and the Judicial Separation of Powers*, 105 GEO. L.J. 255, 257–322 (2017) (explaining how historical practice might be invoked to support nonlegal but obligatory norms of acceptable government behavior or "constitutional conventions").

20. Customary International Law "is typically defined as the collection of international behavioral regularities that nations over time come to view as binding as a matter of law." Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113, 1116 (1999) (citing, *inter alia*, RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES

law that develops on the national level and is authoritative in . . . [the United States] and in any common law country."[21] Domestic customary law; however, evades easy definition. Domestic customary law often refers to the domestic application of customary international law. In *The Paquete Habana*,[22] the Court established that customary international law "is part of" customary domestic law.[23]

More recently, the Second Circuit, in *Filártiga v. Peña-Irala*,[24] signaled a willingness to move toward the domestic incorporation of customary international law norms and standards. The Second Circuit recognized that "domestic jurisdiction" has been "left by international law for regulation by States."[25] It concluded that "[t]here are, therefore, no matters which are domestic by their 'nature.' All are susceptible of international legal regulation and may become the subjects of new rules of customary law of treaty obligations."[26] Domestic customary law encompasses a wide range of subjects beyond simple incorporation of customary international law.[27]

---

§ 102(2) (AM. LAW INST. 1987)). The very concept of Customary International Law and the applicability of its legal boundaries, however, are contested in some academic debates. *See, e.g.*, Curtis A. Bradley & Jack L. Goldsmith, *Customary International Law as Federal Common Law: A Critique of the Modern Position*, 110 HARV. L. REV. 815, 815–76 (1997) (concluding that, absent authorization by the federal political branches, customary international law should not have the status of federal law); Curtis A. Bradley & Mitu Gulati, *Withdrawing from International Custom*, 120 YALE L.J. 202, 241–75 (2010) (arguing that the conventional wisdom that nations cannot unilaterally withdraw from the unwritten rules of customary international law is difficult to justify).

21. Brief for Appellant at 45, Gipson v. Callahan, 157 F.3d 903 (5th Cir. 1998) (No. 97-51021).

22. 175 U.S. 677 (1900).

23. *Id.* at 700.

> International law is part of our law, and must be ascertained and administered by the courts of justice of appropriate jurisdiction as often as questions of right depending upon it are duly presented for their determination. For this purpose, where there is no treaty and no controlling executive or legislative act or judicial decision, resort must be had to the customs and usages of civilized nations, and, as evidence of these, to the works of jurists and commentators who by years of labor, research, and experience have made themselves peculiarly well acquainted with the subjects of which they treat. Such works are resorted to by judicial tribunals, not for the speculations of their authors concerning what the law ought to be, but for trustworthy evidence of what the law really is.

Id. (citing Hilton v. Guyot, 159 U.S. 113, 163, 164, 214, 215 (1895)); s*ee also* Berta E. Hernández-Truyol & Kimberly A. Johns, *Global Rights, Local Wrongs, and Legal Fixes: An International Human Rights Critique of Immigration and Welfare "Reform,"* 71 S. CAL. L. REV. 547, 591 n.224 (1998).

24. 630 F.2d 876 (2d Cir. 1980).

25. *Id.* at 888–89 (quoting Lawrence Preuss, *Article 2, Paragraph 7 of the Charter of the United Nations and Matters of Domestic Jurisdiction*, Hague Receuil (Extract 149) at 8, *reprinted in* THE LAW OF NATIONS 23–24 (Herbert W. Briggs ed., 1952)).

26. *Id.*; *see also* Kadic v. Karadzic, 70 F.3d 232, 238 n.1 (2d Cir. 1995) (relying on language from *Filártiga* regarding treaties and customary international law).

27. Although much important scholarship is conducted in this field, an exhaustive discussion of

This Article contends that, in assessing the societal impact of cybersurveillance, the Supreme Court and other federal courts have implicitly recognized that privacy customs or anti-surveillance customs exist and have normative value in the Fourth Amendment context. The federal judiciary, with increasing frequency, marks unconstitutional transgressions resulting from modern surveillance techniques by resorting to dystopian *1984*-related tropes.[28] Regardless of how well-supported the government's position is by preexisting Fourth Amendment precedent, the Supreme Court and lower courts have questioned whether the Fourth Amendment should operate to protect society from the "*1984* problem" posed by emerging mass surveillance programs and cybersurveillance technologies.[29]

As these decisions accumulate, it is apparent that Fourth Amendment jurisprudence lacks a clear, unifying data privacy doctrine.[30] Prior Fourth

---

domestic customary law and customary international law goes beyond the scope of this Article. *See, e.g.*, *supra* notes 18–23 and accompanying text. *See also* Richard Craswell, *Do Trade Customs Exist?*, *in* THE JURISPRUDENTIAL FOUNDATIONS OF CORPORATE AND COMMERCIAL LAW 118 (Jody S. Kraus & Steven D. Walt eds., 2000) (discussing and citing the work in so-called pragmatics—better described to non-philosophers as linguistic pragmatism); Richard A. Epstein, *The Path to the T.J. Hooper: The Theory and History of Custom in the Law of Tort*, 21 J. LEGAL STUD. 1, 10 (1992) (suggesting that parties unfamiliar with customs of the trade may reject any proposed term because it is unascertainable whether it conforms to the usage, thus leaving the matter to be governed by the usage); Frederick Schauer, *Pitfalls in the Interpretation of Customary Law*, *in* THE NATURE OF CUSTOMARY LAW: LEGAL, HISTORICAL, AND PHILOSOPHICAL PERSPECTIVES 13, 32 (Amanda Perreau-Saussine & James Bernard Murphy eds., 2007) (comparing the imagined operation of custom to "the marketplace of ideas"); Henry E. Smith, *Community and Custom in Property*, 10 THEORETICAL INQ. L. 5, 5–41 (2009) (proposing an informational theory of custom in property law); George Rutherglen, *Custom and Usage as Action Under Color of State Law: An Essay on the Forgotten Terms of Section 1983*, 89 VA. L. REV. 925, 925–77 (2003) (analyzing the meanings of "custom" and "usage" to determine the scope of Section 1983 and to determine the scope of congressional power under Section 5 of the Fourteenth Amendment); Bradley & Goldsmith, *supra* note 20, 903–07 (explaining how customary international law continues to be relevant to domestic federal common law).

28. *See* Thomas P. Crocker, *Dystopian Constitutionalism*, 18 U. PA. J. CONST. L. 593, 595–96 (2015) (discussing the "rich tradition of using contrastive dystopian states in constitutional argument").

29. Riley v. California, __ U.S. __, 134 S. Ct. 2473 (2014); Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); United States v. Jones, 565 U.S. 400 (2012); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 142 F. Supp. 3d 172 (D.D.C. 2015); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015); *see also* Donohue, *Bulk Metadata Collection*, *supra* note 2; Donohue, *Section 702*, *supra* note 2; Hu, *Small Data Cybersurveillance v. Big Data Cybersurveillance*, *supra* note 4; Orin S. Kerr, *The Future of Internet Surveillance Law*, 72 GEO. WASH. L. REV. 1139 (2004); Richards, *supra* note 13; Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281; Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008).

30. The Post-Snowden litigation revealed a highly fractured Fourth Amendment as the constitutionality of the NSA's bulk telephony metadata program has been analyzed by various federal

Amendment precedent that appears to be technologically obsolete has been ignored or discarded[31] as the federal judiciary endeavors to avoid the "*1984* problem." Specifically, by tying the Fourth Amendment protections to subjective and objective expectations of privacy through the *Katz* test, the Court adopted a Fourth Amendment line of analysis that experts note is problematic in two ways: it is both circular[32] and self-defeating.[33] Expectations of privacy change in response to social and

courts. *See Klayman*, 957 F. Supp. 2d at 9 (finding that the court lacked jurisdiction to review Administrative Procedure Act [APA] claim but could hear Fourth Amendment constitutional challenges to the NSA's conduct; and granting motion for injunction but staying the order pending appeal); Obama v. Klayman, 800 F.3d. 559, 561 (D.C. Cir. 2015) (reversing district court and remanding for further proceedings); *Klayman*, 142 F. Supp. 3d at 190–98 (concluding plaintiffs' claim that Section 215 program is unconstitutional under the Fourth Amendment has a likelihood of success on the merits and ordering injunction, blocking the final 20 days of the Section 215 program, prior to the implementation of the USA FREEDOM Act's reforms to metadata collection); Obama v. Klayman, No. 15–5307, 2015 WL 9010330 (D.C. Cir. Nov. 16, 2015) (granting an emergency motion for a stay pending appeal); Klayman v. Obama, 805 F.3d 1148 (D.C. Cir. 2015) (denial of emergency petition for rehearing en banc); ACLU v. Clapper, 959 F. Supp. 2d 724, 750–52 (S.D.N.Y. 2013) (dismissing complaint in part on grounds that subscribers do not have legitimate expectation of privacy in telephony metadata held by third parties under Fourth Amendment precedent); ACLU v. Clapper, 785 F.3d at 792 (vacating dismissal of complaint, finding that bulk collection of telephone metadata exceeded scope of statutory authority, remanding for argument on constitutional issues, and affirming district court's denial of preliminary injunction); ACLU v. Clapper, No. 14-42-CV, 2015 WL 4196833 (2d Cir. June 9, 2015) (ordering stay of proceedings pending parties' supplemental briefing in light of passage of USA FREEDOM Act); ACLU v. Clapper, 804 F.3d 617, 618 (2d Cir. 2015) (denying motion for preliminary injunction, declining to reach constitutional issues for prudential reasons, and remanding for further proceedings in district court).

31. Christopher Slobogin, *Is the Fourth Amendment Relevant in a Technological Age?*, *in* CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE 11 (Jeffrey Rosen & Benjamin Wittes eds., 2011).

32. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 60–61 (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 U.C.L.A. 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."); Amsterdam, *supra* note 9, at 383–86 (contending that *Katz*'s reasoning is circular); Jonathan Simon, Katz *at Forty: A Sociological Jurisprudence Whose Time Has Come*, 41 U.C. DAVIS L. REV. 935, 956–57 (2008) (citing Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring)); Richard Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 187) ("*Katz* is said to be circular because social expectations of privacy are themselves presumably influenced by the policy choices of government, including the Supreme Court.").

33. *See, e.g.*, Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1328 (2002) ("By leaving the decision to adopt new surveillance technologies largely to the discretion of law enforcement, the Supreme Court's current jurisprudence largely stands the amendment on its head."); Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV. 904, 923 (2004) (arguing that the decreasing effectiveness of *Katz* allows for a "very odd constitutional regime where the most common and extensive searches—those using effective new technologies—are placed outside of the Fourth Amendment").

technological developments.[34] The normalization of surveillance diminishes societal and individual expectations of privacy. Justice Breyer, during oral argument in *United States v. Jones*, recognized the possibility of this paradox: ubiquitous surveillance in a democratic society.[35] Consequently, repeated references to *1984* during the *Jones* oral argument and other Supreme Court cases underscores the normative contours of the Fourth Amendment—considerations that have become increasingly central to the judicial inquiry.

In recent years, federal courts have been invited to analyze the constitutionality of emerging surveillance methods and big data cybersurveillance. As cybersurveillance tools are rapidly deployed for law enforcement and national security purposes, it is now possible to review a body of cybersurveillance law. A broader analysis of these cases allows one to track the future trajectory of the Fourth Amendment through the explicit framing and naming of a clear jurisprudential trend. This Article identifies that trend as a quickly evolving cybersurveillance nonintrusion test that appears to be displacing the *Katz* test.

Prior to the development of modern mass surveillance capacities and cybersurveillance methods, "physical intrusions and bodily intrusions were primarily at the forefront of the Fourth Amendment inquiry."[36] With the advent of increasingly invasive cybersurveillance technologies, the physicality of the intrusion under the Fourth Amendment does not represent the anchoring concern of the Court.[37]

---

34. *See Jones*, 565 U.S. at 427 (Alito, J., concurring).

35. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 24 ("[W]hat would a democratic society look like if a large number of people did think that the government was tracking their every movement over long periods of time[?]").

36. Margaret Hu, *Cybersurveillance Intrusions and the* Katz *Privacy Test*, 55 AM. CRIM. L. REV. (forthcoming 2018) (companion symposium piece to this article). "The term physical intrusions . . . refers to seizures of individuals." *Id.* (citing Safford United Sch. Dist. v. Redding, 557 U.S. 364, 375 (2009) (permitting a search of a student when it is reasonable in relation to the scope of the circumstances justifying the search); California v. Hodari D., 499 U.S. 621, 626 (1991) (explaining that a seizure of an individual for an arrest requires either a show of force or submission to authority); United States v. Mendenhall, 446 U.S. 544, 554 (1980) (explaining that a Fourth Amendment seizure has occurred when, under the circumstances, a reasonable person would believe that he was not free to leave); Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (permitting a brief investigatory detention and search of outer clothing for weapons as a "reasonable search under the Fourth Amendment")). "The term bodily intrusions refers to actions that intrude into an individual's body." *Id.* (citing Birchfield v. North Dakota, __ U.S. __, 136 S. Ct. 2160, 2184 (2016) (concluding that warrantless blood tests are not permitted under the Fourth Amendment because they are "significantly more intrusive" than breath testing); Maryland v. King, __ U.S. __, 133 S. Ct. 1958, 1977 (2013) (finding that "the intrusion of a cheek swab to obtain a DNA sample is a minimal one"); Schmerber v. California, 384 U.S. 757, 770–71 (1966) (finding that exigent circumstances permitted warrantless blood testing to secure evidence of blood alcohol content)).

37. Hu, *Cybersurveillance Intrusions and the* Katz *Privacy Test*, *supra* note 36 (citing *Jones*, 565

Court decisions addressing unprecedented government surveillance capacities justify their refusal to apply settled precedent by following an inquiry that centers on cybersurveillance nonintrusion. This Article demonstrates that, in light of rapidly emerging technological developments, a cybersurveillance nonintrusion test may be more appropriate than the *Katz* test.[38] It describes how a cybersurveillance nonintrusion test grounded in customary law can replace the Fourth Amendment privacy test that is currently grounded in property and tort law and dependent on the notion that privacy turns on non-disclosure.

Under the *Katz* test, the Court leads with an interrogation of whether an individualized and subjective "reasonable expectation of privacy" has been offended.[39] Next, *Katz* requires courts to ask whether society would objectively ratify the individual's subjective expectation of privacy.[40] The cybersurveillance nonintrusion test implicitly suggested by the Supreme Court in *Jones* first shifts the vantage point of the Fourth Amendment analysis from an individual-based tangible harm inquiry to an inquiry of a society-wide intangible harm. Other scholars have taken the perspective that the Fourth Amendment provides more than individual protection—David Gray argues that "rights secured by the Fourth Amendment are fundamentally collective rather than individual."[41] A cybersurveillance nonintrusion test also shifts the burden from the individual. Rather than require an individual to establish a reasonable expectation of privacy, the cybersurveillance nonintrusion test requires the government to justify the intrusion of the surveillance on society.

A cybersurveillance nonintrusion test significantly differs in many material respects from the *Katz* privacy test. In assessing the constitutionality of cybersurveillance under the cybersurveillance nonintrusion test, the Court has suggested that the two-part *Katz* test can

---

U.S. at 405 ("Our later cases, of course, have deviated from that exclusively property-based approach [to the Fourth Amendment]."); *id.* at 414 (Sotomayor, J., concurring) ("In *Katz*, this Court enlarged its then-prevailing focus on property rights by announcing that the reach of the Fourth Amendment does not 'turn upon the presence or absence of a physical intrusion.'" (citation omitted))); *see also* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2483–84, 2489 (2014) (describing case precedent addressing searches incident to arrest and pointing out that the scope of privacy intrusions is far greater with access to digital data).

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

39. *Id. But see* Orin S. Kerr, Katz *Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. CHI. L. REV. 113, 114–15 (2015) (arguing that *Katz* is actually a one-step test and the subjective prong of the *Katz* test is irrelevant).

40. *Katz*, 389 U.S. at 361.

41. GRAY, *supra* note 9; Gray, *Dangerous Dicta*, *supra* note 5, at 1183; *see also* David Gray, *A Collective Right To Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189, 191–92 (2015).

be reversed: the leading analytical inquiry under the Fourth Amendment would commence with an interrogation of whether a society-wide, objective expectation of governmental cybersurveillance nonintrusion has been offended.[42] This Article contends that federal courts are already making such assessments and that the courts are doing so based on what they gauge to be the limits of what a court can reasonably ratify under existing precedent while still adhering to perceived norms of what is socially intolerable in a free society. Essentially, courts appear to be considering whether the modern surveillance method creates a "*1984* problem" for society and why the Fourth Amendment should operate to avoid it. The secondary inquiry of a cybersurveillance nonintrusion test would concern itself with whether an individualized, subjective "reasonable expectation of privacy" transgression has occurred.

Adoption of the cybersurveillance nonintrusion test would render moot the preexisting Third Party Doctrine under Fourth Amendment jurisprudence.[43] The Court's leading inquiry under a cybersurveillance nonintrusion test would no longer turn on assessments of individualized "expectations of privacy." Thus, whether an individual has voluntarily shared digital data with a "third party," such as an Internet company or telecommunications company, would no longer control the Fourth Amendment privacy test. Sharing metadata or data with a third party telecommunications company would not preclude Fourth Amendment protection on the grounds that an individual could not subjectively possess a reasonable expectation of privacy in this metadata because the metadata had already been shared with the company.

This Article concludes that, especially in light of the Snowden disclosures, technological developments, and a shift in individual and social expectations of privacy, a sharp correction of the Fourth Amendment doctrine—namely the adoption of a cybersurveillance nonintrusion test and abandonment of the *Katz* test—is warranted. It is undisputed that the Court has been forced to grapple with how best to preserve the integrity of the Fourth Amendment in light of technological advances.[44] Cybersurveillance advancements pose a threat that extends beyond individualized harms. Individualized harms form the basis of property and tort law that has traditionally anchored the Fourth

42. *See* Transcript of Oral Argument, United States v. Jones, supra note 16, at 12–13, 44, 51; Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, *supra* note 36.

43. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (articulating the Third Party Doctrine).

44. *See, e.g.*, United States v. Jones, 565 U.S. 400, 417–18 (2012) (Sotomayor, J., concurring) (questioning the applicability of the Third Party Doctrine to modern technology and Fourth Amendment analysis).

Amendment analysis. Cybersurveillance, however, increasingly implicates the search and seizure of identity, posing a challenge of mass harms to the inalienable, autonomous rights of entire populations of individuals. Consequently, a society-wide or community-wide framework of customary law is now more appropriate to preserve the first principles of the Fourth Amendment. The Court itself appears ready to reevaluate its Fourth Amendment jurisprudence in light of the rise of an Information Society, ubiquitous digital data collection and analysis methods, and big data surveillance technologies.[45]

This Article proceeds in three parts. Part I addresses the constitutional implications raised by the big data cybersurveillance and dataveillance capacities of the government. This part of the Article sets forth the Court's current Fourth Amendment doctrine on individual and social privacy expectations that warrant constitutional protection: the "reasonable expectation of privacy" test first articulated in *Katz v. United States*. Technological developments increasingly normalize surveillance into our daily lives in nearly invisible and physically non-intrusive ways; however, scholars have questioned the efficacy of the Court's current Fourth Amendment jurisprudence and the preexisting privacy doctrine.[46] Part I concludes that current Fourth Amendment privacy jurisprudence provides no robust legal basis for enforcing meaningful limits on big data cybersurveillance.

Part II sketches out the contours of the Fourth Amendment "*1984* problem" posed by big data cybersurveillance. During the *Jones* oral argument, and in the Justices' concurrences in *Jones*, the Court made clear that Fourth Amendment jurisprudence has not yet developed a limiting principle to curtail the effects of rapidly advancing technology in the realm of cybersurveillance and dataveillance.[47] Various Justices on the

---

45. The Court is once again preparing to tackle the Fourth Amendment and changing technology. On June 5, 2017, the Court granted certiorari in *Carpenter v. United States*, 819 F.3d 880 (6th Cir. 2016). *See* Carpenter v. United States, No. 16-402, 2017 WL 2407484 (June 5, 2017). The question presented in *Carpenter* is "[w]hether the warrantless seizure and search of historical cell phone records revealing the location and movements of a cell phone user over the course of 127 days is permitted by the Fourth Amendment." Petition for a Writ of Certiorari at 10–11, *Carpenter*, 819 F.3d 880 (No. 16-402).

46. *See, e.g.*, CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT (2007) (observing that Fourth Amendment jurisprudence, read broadly, largely permits technological surveillance and arguing for regulatory reform to protect privacy).

47. *See, e.g.*, Kerr, *Mosaic Theory*, *supra* note 5, at 339 (discussing the *United States v. Jones* decision in context of the Justice Alito's concurrence and contending that it echoed a digital "mosaic theory" approach to the Fourth Amendment).

Court have used references to *1984* to identify culturally ingrained limits to tolerable government intrusiveness.[48]

In Part III, this Article asserts that the jurisprudence must evolve to establish limitations on government intrusiveness—limitations that are culturally ingrained—as part of an assessment of whether the newly emerging cybersurveillance method or mass surveillance program is considered objectively or subjectively reasonable. In light of the government's *1984*-like capacity to conduct the search and seizure of digitally constructed identities, the Court in *Jones* suggested that an inquiry centered around cybersurveillance nonintrusion, rather than privacy, might be more appropriate in the digital age.[49] Part III discusses recent decisions by both the Supreme Court and lower courts confronting modern surveillance technologies. It shows how those cases point the way toward a cybersurveillance nonintrusion test grounded in customary law to replace a privacy test that is often grounded in property and tort law. Such a test is results-oriented and avoids what federal courts fear may be judicial ratification of Orwellian surveillance with their corresponding constriction of individual privacy and autonomy.

This Article concludes that the evolution of Fourth Amendment jurisprudence is appropriate in light of the fact that the technology to be governed by new legal principles is still rapidly evolving. Moreover, recent decisions reflect a recurrent concern that the judiciary may over-restrain the government's ability to address national security issues, such as terrorist attacks on the home front.[50] The virtual and increasingly comprehensive nature of big data cybersurveillance presents unprecedented types of society-wide intangible harms. A dramatic revision of the Fourth Amendment doctrine is now required: abandonment of the *Katz* test and the adoption of a cybersurveillance nonintrusion test.

---

48. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13, 25–26, 33, 35, 57 (noting references to *1984*); *see also infra* sections II.A. and III.B.

49. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 10–11.

50. The issues raised by modern technology's intersection with the Fourth Amendment are breathtaking and this Article does not purport to address them comprehensively. For example, the global dimension of the Internet raises thorny Fourth Amendment questions, including how might the location of an internet user affect his or her "reasonable expectation of privacy" and how might the border search doctrine apply in the context of transnational internet use? *See* Kerr, *The Fourth Amendment and the Global Internet*, *supra* note 5. Similarly, some scholars have turned their attention to the data territoriality issues that attach to the Fourth Amendment. *See, e.g.*, Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 328–98 (2015) (exploring the unique features of data and highlighting the ways in which data undermines longstanding assumptions regarding the link between data location, and applicable rights and obligations).

I. FOURTH AMENDMENT AND CYBERSURVEILLANCE HARMS

Because of the narrow ground on which the Court resolved *Jones*, the case is less interesting for its holding than for the problems with current Fourth Amendment doctrine that the holding avoided. Part I discusses the collision of modern forms of cybersurveillance with current Court doctrine, as epitomized in the *Katz* test's protection of expectations of privacy. Part I begins with a discussion of how the *Katz* test emerged. *Katz*, and the decisions leading up to it, show the Court wrestling with the question of whether speech and certain forms of surveillance intrusions should be subject to protection by the Fourth Amendment which, textually, appears to be concerned with the protection of physical things or "effects."[51] The decision to evolve Fourth Amendment doctrine to protect individual expectations of privacy occurred after the Court had repeatedly confronted developing forms of government surveillance, most prominently wiretapping, that allowed increased monitoring of private conversations. Reexamining cases like *Katz* and its predecessors demonstrates parallels with the Court's current predicament. The Court reluctantly changed Fourth Amendment doctrine in the face of changing forms of government surveillance. Proponents of the transformation were concerned about the impacts of such surveillance on democracy, and opponents worried about judicial intrusion upon the government's ability to protect national security.

Next, this Part discusses current cybersurveillance techniques that enable breathtakingly encompassing surveillance of individuals that do not appear to offend expectations of privacy as they are understood within the *Katz* framework. Given that cybersurveillance means surveillance of entire sectors of society, rather than of specific individuals, it is necessary to understand why *Katz* cannot simply be supplemented, such as with the "mosaic theory." Both the D.C. Circuit and the Second Circuit have attempted to reconcile *Katz* with government cybersurveillance. In these decisions, it is possible to see the competing tensions between a fear of an Orwellian society and judicial caution about interference with the Executive branch's interests in national security. Concerns about national security often, but not always, permeate cases in which traditional Fourth Amendment doctrine collides with the big data reality of modern society. This Part concludes with an examination of *Riley v. California*, a case in which national security interests were not salient, where the Court showed a willingness to alter Fourth Amendment doctrine to protect digital data

51. *See infra* section I.A.

from police scrutiny in circumstances where other kinds of data would not normally be protected.

A. The Fourth Amendment's Privacy Doctrine

The following discussion offers a basic overview of the "reasonable expectation of privacy" protections offered by the Fourth Amendment. During the *Jones* oral argument, the Justices conceded that a protection of reasonable expectations of privacy would not restrain the use of increasingly comprehensive and invasive data-driven tracking techniques, which are rapidly evolving. The Justices appeared to signal that the evolution of these technologies now requires a parallel evolution of the Fourth Amendment doctrine to keep pace with modern cyber-developments.[52]

The "reasonable expectation of privacy" test emerged in a 1967 case, *United States v. Katz*.[53] *Katz* marked a departure from prior Fourth Amendment doctrine, one that was motivated by the Court's perceived need to come to grips with modern government surveillance techniques that were unrestrained by the Court's then-current Fourth Amendment doctrine.[54] The technology that concerned the Court was telephone wiretapping, the most effective form of police eavesdropping at the time.[55] The government's position in *Katz* was that the Court should simply apply existing precedent and conclude that eavesdropping had nothing to do with the concerns protected by the Fourth Amendment.[56] The government relied on two cases as the basis for its position: *Olmstead v. United States*[57] and *Goldman v. United States*.[58]

In the 1928 case of *Olmstead v. United States*, the Court addressed the constitutionality of extended government surveillance of a massive liquor bootlegging operation in Washington State.[59] The government placed

---

52. *See, e.g.*, Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 3–4.

> Chief Justice Roberts: Knotts, though, seems to me much more like traditional surveillance. You're following the car, and the beeper just helps you follow it from a—from a slightly greater distance. That was 30 years ago. The technology is very different, and you get a lot more information from the GPS surveillance than you do from following a beeper.

Id.

53. 389 U.S. 347 (1967).

54. *See id.* at 353.

55. *See id.* at 348.

56. *See id.* at 351–52 (discussing the government's arguments in the case).

57. 277 U.S. 438 (1928).

58. 316 U.S. 129 (1942).

59. *Olmstead*, 277 U.S. at 455–56.

wiretaps on phone lines coming from four of the suspects' residences, as well as from the operation's main office; all, the Court noted, "without trespass on any property of defendants."[60] The Court concluded that this unauthorized surveillance seemed unproblematic. The Fourth Amendment protects "material things—the person, the house, his papers, or his effects,"[61] but it did not protect phone calls because a phone conversation is not a thing and so cannot be searched or seized. Rather than a search of someone's effects, wiretapping simply involved "the sense of hearing and that only," and one could not construe "the words search and seizure as to forbid hearing or sight."[62] The home itself, and conversations held therein, are traditionally protected by the Fourth Amendment.[63] But the Court distinguished between phone calls and internal conversations, explaining that "one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside" and, in doing so, falls outside "the protection of the Fourth Amendment."[64] Telephone wires merely convey sensory impressions (sounds) that cannot be seized; and when they are tapped outside the space of the house, a trespass problem is also avoided.[65]

In *Goldman*, the government used a detectaphone: a device that enhanced a listener's ability on one side of a wall to hear conversations on the other side without a physical invasion.[66] Although the technology was different than a wiretap, the Court applied *Olmstead* and concluded that eavesdropping falls outside the purview of the Fourth Amendment.[67] The petitioners argued, without success, that the absence of a phone altered the analysis because in *Olmstead*, the Court had explained that resorting to a phone involved a choice to project one's voice to the world at large.[68] The principle that police cannot actually search or seize a conversation renders the speaker's intent to keep the conversation within the private confines of her home irrelevant. To be sure, the Court's rejection of petitioner's argument was more summary, perhaps because

60. *Id.* at 456–57.

61. *Id.* at 464.

62. *Id.* at 464–65.

63. *See generally* Boyd v. United States, 116 U.S. 616 (1886).

64. *Olmstead*, 277 U.S. at 466.

65. The Court distinguished the question of trespass and the Fourth Amendment, noting that even if the eavesdropping involved a trespass, that would not mean the police had violated the Fourth Amendment. *Id.* at 465.

66. Goldman v. United States, 316 U.S. 129, 131 (1942).

67. *Id.* at 135.

68. *Id.*

otherwise it might have had to address why *Olmstead* bothered to point out that one assumes any risk of wiretapping in electing to bring a phone into their house.[69]

After *Goldman*, speech fell outside the Fourth Amendment and was subject to any manner of surveillance without resort to a warrant. It was a "strange doctrine," Justice Murphy noted in his dissent, that protected writings but left vulnerable "the most confidential revelations between husband and wife, client and lawyer, patient and physician, and penitent and spiritual advisor" because they were not committed to paper.[70] Although *Goldman* insisted it did not matter if the speech subject to surveillance was whispered in the bedroom or spoken to a person on the other side of the country via telephone, the Court was clearly trying to grapple with an issue created by modern surveillance techniques. If the Court was only now realizing the oddity of speech being subject to unrestrained surveillance, even though the Fourth Amendment was more than a hundred and fifty years old, it was because only in the twentieth century was technology being developed that made surreptitious surveillance of conversations feasible and effective. Justice Murphy's dissent in *Goldman* counseled that the Court's interpretation of the Fourth Amendment must be "sufficiently liberal and elastic to make it serve the needs and manners of each succeeding generation," and then explained that a search today no longer requires "physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment."[71] Finally, the dissent emphasized "democratic rule" and the need to protect the individual from being "wholly subordinated to the interests of the state."[72] Orwellian specters of totalitarianism served as a placeholder marking a gap between the Court's current Fourth Amendment doctrine and the technologies available to the government that are unrestrained by that doctrine.

Justice Murphy's dissent in *Goldman* was consistent with the dissenting opinions fourteen years earlier in *Olmstead*.[73] Justice Brandeis noted that: "[s]ubtler and more far-reaching means of invading privacy have become available to the Government," and noted that the "progress

69. *Id.*

70. *Id.* at 141.

71. *Id.* at 138–39.

72. *Id.* at 142.

73. Olmstead v. United States, 277 U.S. 438, 473 (1928).

of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping."[74] Justice Brandeis also resorted to dramatic rhetoric in emphasizing that the Fourth Amendment must do more than protect "material things."[75] At stake was "man's spiritual nature," "his feelings," and "his intellect."[76] Although his pitch to revise Fourth Amendment doctrine went unheeded in 1928 and was again rejected by a majority of the Court in 1942, by the 1960s, the Court was coming to grips with the problem posed by twentieth century surveillance techniques and more receptive to arguments about the legality of such surveillance under the Fourth Amendment.

In the 1960 case of *Silverman v. United States*,[77] the Court signaled a willingness to start restraining government eavesdropping even as it attempted to do so without significantly altering its current Fourth Amendment doctrine. In *Silverman*, the police brought a "spike mike" into contact with the heating duct of a row house to hear conversations in the house.[78] *Olmstead* and *Goldman* appeared to dictate the result, leaving petitioners to argue that changing technology required overturning those cases in which technology provided the government with increasingly effective methods of eavesdropping on private conversations from remote distances.[79] The Court, however, declined to "contemplate the Fourth Amendment implications of these and other frightening paraphernalia which the vaunted marvels of an electronic age may visit upon human society."[80] Instead, the Court held that the police had made "an unauthorized physical encroachment within a constitutionally protected area," an individual's home, when they brought a microphone into contact with the house's heating system.[81] In reviewing its prior Fourth Amendment cases, the Court noted that it had upheld non-trespassory government surveillance. Although review of *Olmstead* and *Goldman*

74. *Id.* at 473–74. Perhaps presciently, Brandeis speculated about the kinds of pre-crime technologies I have discussed elsewhere: "[a]dvances in the psychic and related sciences may bring means of exploring unexpressed beliefs, thoughts and emotions." *Id.* at 474. *See, e.g.*, Hu, *Small Data Surveillance*, *supra* note 4, at 803 (describing how preemptive action may appear to be justified in the eyes of the government in certain situations); Hu, *Taxonomy of the Snowden Disclosures*, *supra* note 4, at 1684 (explaining how surveillance in day-to-day governance activities is often justified by pre-crime objectives).

75. *Olmstead*, 277 U.S. at 478.

76. *Id.*

77. 365 U.S. 505 (1961).

78. *Id.* at 506–07.

79. *Id.* at 508–09.

80. *Id.* at 509.

81. *Id.* at 510–12.

arguably provide no basis to conclude that the Court's observations on the question of trespass were integral to the Fourth Amendment holding.[82] In *Silverman*, conversations were still not "things" within the meaning of the Fourth Amendment, but there were now "constitutionally protected areas," and if the government's surveillance physically intruded into such an area, the surveillance offended the Fourth Amendment.[83]

Silverman's emphasis on physical intrusion did not survive long. Seven years later, the Court was ready to reestablish its Fourth Amendment doctrine on a new basis.[84] *Katz* involved government surveillance of a phone call made in a public phone booth. The parties, taking their cue from *Silverman*, attempted to argue that the phone booth was analogous to a home or some other "constitutionally protected area,"[85] but the Court abruptly dismissed this approach.[86]

In *Katz*, the Court brought the spoken word within the scope of protection of the Fourth Amendment.[87] The government, relying on the Court's jurisprudence, contended that because there was no physical intrusion on the phone booth—only electronic monitoring—there was no Fourth Amendment problem. The Court flatly rejected that formulation and instead offered up the reasonable expectation of privacy test.[88]

The Court explained that "[w]hat a person knowingly exposes to the public, even in his home or office," is without constitutional protection, "[b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[89] The Court rejected the notion that a person placing a phone call in a glass phone booth had surrendered constitutional protections because he was visible as he made the call.[90] What was relevant was his expectation that his words were shielded from being heard by third parties. Then, embracing the dissents

82. *Id.* at 509–10.

83. *Id.* at 512.

84. Katz v. United States, 389 U.S. 347 (1967).

85. *Id.* at 349.

86. The Court dismissed this approach, deriding the notion that "the correct solution of Fourth Amendment problems" can be "promoted by incantation of the phrase 'constitutionally protected area,'" *id.* at 350, but in fairness to the parties, they were only taking their cue from *Silverman*. Until *Katz*, eavesdropping by any means did not offend the Fourth Amendment unless it involved intrusion on a "constitutionally protected area." *Id.*

87. *Id.* at 353.

88. *Id.* at 350 (rejecting the parties' formulation); *id.* at 360 (Harlan, J., concurring) (reading the majority opinion as holding that "a person has a constitutionally protected reasonable expectation of privacy").

89. *Id.* at 351–52 (majority opinion).

90. *Id.* at 352.

in *Olmstead* and *Goldman*, the Court explained that Fourth Amendment protections must change as technology changes: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[91]

It is, however, Justice Harlan's concurrence that set forth the test commonly associated with *Katz*. It is a two-prong test: "first that a person have exhibited an actual (subjective) expectation of privacy."[92] The second prong of the test requires "the expectation [of privacy] be one that society is prepared to recognize as 'reasonable.'"[93] Thus, Justice Harlan noted that while a telephone booth is a public place, the act of closing the door establishes an expectation of privacy on the part of the individual entering the booth, and society views this expectation as reasonable.[94]

The Court acknowledged that in the past, it had required "searches and seizures of tangible property" as a prerequisite to finding a Fourth Amendment violation.[95] Justice Harlan, in his concurrence, noted that the trespass doctrine had become outdated and no longer suited to the realities of modern life in 1967 because surveillance and intrusion could be accomplished without physical intrusion: "[i]ts limitation on Fourth Amendment protection is, in the present day, bad physics as well as bad law, for reasonable expectations of privacy may be defeated by electronic as well as physical invasion."[96]

Thus, in place of the trespass doctrine, *Katz* left a more flexible reasonable expectation of privacy test that effectively protected against government intrusion, physical or otherwise, so long as those subject to surveillance intended to keep their affairs private.[97] In response to the new test, Justice Black's dissent decried an expansion of the reach of the Amendment beyond its textual limitations and the arrogation of the Court of "omnipotent lawmaking authority," which "is dangerous to freedom."[98]

Related to this familiar originalist complaint arises a new theme, which remains in play in recent court decisions grappling with big data surveillance: judicial uncertainty regarding national security implications. To the extent the Court interposes the Fourth Amendment as a restraint on government surveillance in the name of democracy, the government

91. *Id.*

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

93. *Id.*

94. *Id.*

95. *Id.* at 352–53 (majority opinion).

96. *Id.* at 362 (Harlan, J., concurring).

97. *Id.*

98. *Id.* at 374 (Black, J., dissenting).

can restrain the Court by invoking the need for national security and its own obligation to protect democracy. In a footnote, the *Katz* Court reserved the question of whether a warrant would be required where national security was implicated.[99] Justice White's concurrence went further, stating that warrant procedures should not apply where the President or the Attorney General believe electronic surveillance is reasonable for national security purposes.[100] Justice Douglas (joined by Justice Brennan) in turn concurred to address Justice White and argue that the President and Attorney General cannot be trusted to decide when Fourth Amendment protections should or should not apply to persons accused of treasonous activity.[101] This debate was not relevant to the holding in *Katz*, but served to remind members of the Court that Fourth Amendment doctrine implicates national security concerns.

This narrative of how *Katz* came to be is relevant because the same dynamic is in play again today. At the time *Katz* was decided, the new test seemed much more expansive than the one it supplanted. But in the modern context of 24/7, 360-degree cybersurveillance and dataveillance, there have been a number of calls to again update the Fourth Amendment test to reflect our times.[102]

It is against this historical backdrop that this Article turns to *Jones*. The decision in *Jones* is most noteworthy for the fact that it evaded the troubling issues that vexed the Court. In this respect, *Jones* hearkens back to *Silverman*. In both cases, the Court was troubled by the notion that contemporary surveillance techniques were unrestrained by the Fourth Amendment and, in both cases, the Court balked from attempting to refashion its Fourth Amendment doctrine; instead, it found a more limited basis for finding the Fourth Amendment was violated on the facts before it. In both cases, the court's decision rested on a physical trespass.[103] *Jones*'s oral argument is equally worth considering because it demonstrates the same dynamic that was present in the cases leading to, and including, *Katz*. The Court evidences a growing restlessness with the current Fourth Amendment doctrine's impotence in the face of

99. *Id.* at 358 n.23 (majority opinion) ("Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is not a question presented by this case.").

100. *Id.* at 364 (White, J., concurring).

101. *Id.* at 359–60 (Douglas, J., concurring).

102. *See supra* note 5.

103. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (explaining that a physical intrusion by the Government into private property constitutes a Fourth Amendment search); Silverman v. United States, 365 U.S. 505, 512 (1961) (emphasizing that the decision finding that a search occurred is "based upon the reality of an actual intrusion into a constitutionally protected area").

increasingly comprehensive techniques of government surveillance. The references to *1984* in the oral argument serve to underscore the potency of deeply ingrained cultural norms regarding the appropriate limits on government intrusiveness in an age when technological innovation is rapidly changing the government's capacities. The substantial rhetorical force of *1984* nearly assured a government defeat in *Jones*. In effect, this result illuminated the "cultural software" embedded within the Fourth Amendment's "doctrinal hardware."[104]

B. Limits of the Fourth Amendment Mosaic Theory

It appears that the Court today is in much the same place as it was fifty years ago prior to the *Katz* decision. *Jones* represents one of the Court's closest engagements with the constitutionality of emerging ubiquitous tracking technologies. GPS technology enables surveillance through 24/7 data collection.[105] A GPS device transmits geospatial data that captures current locations multiple times per minute for as long as the device is left in place. Once a GPS device is installed, it automatically collects data without the need for any law enforcement intervention. This technology enables authorities to pinpoint the precise location of the device at any given time with minimal effort and resource expenditure.[106]

The comprehensive scale of such data collection is what appears to have led to the lower court in *Jones*, the D.C. Circuit Court of Appeals, holding that the detailed data trail recorded constitutes a Fourth Amendment violation by allowing the government to capture the entire mosaic of the suspect's activities, rather than the mere tile of the suspect's potential criminal activity.[107] In the wake of *Jones*, constitutional scholars have shown interest in the mosaic theory employed by the D.C. Circuit.[108]

---

104. *See generally* J. M. BALKIN, CULTURAL SOFTWARE: A THEORY OF IDEOLOGY (1998) (contending that the metaphor of cultural software opens a way for moving beyond entrenched perspectives and provides a more productive approach to theorizing ideology).

105. *See Jones*, 565 U.S. at 403; *supra* note 45 (discussing *United States v. Carpenter*, a case challenging law enforcement warrantless use of cell-site geolocational data, recently granted certiorari by the Supreme Court).

106. *See Jones*, 565 U.S. at 403.

107. *See* United Sates v. Maynard, 615 F.3d 544, 554 (D.C. Cir. 2010).

108. For a detailed discussion on the mosaic theory, see Kerr, *Mosaic Theory*, *supra* note 5, at 313 (discussing the *United States v. Jones* decision on GPS surveillance in the context of digital "mosaic theory"). Under the digital mosaic theory, courts evaluate the collective, aggregated whole of a surveillance sequence to determine whether the surveillance activity is properly construed as a search. *Id.* Kerr concludes courts should reject the theory as unworkable. *Id.* at 346 ("[T]he theory raises so many novel and puzzling questions that it would be difficult, if not impossible, to administer effectively as technology changes."); *see also* Fabio Arcila, Jr., *GPS Tracking Out of Fourth Amendment Dead Ends:* United States v. Jones *and the* Katz *Conundrum*, 91 N.C. L. REV. 1 (2012);

Under the mosaic theory, as articulated by the D.C. Circuit, acquisition of information that would not ordinarily be a Fourth Amendment search under *Katz* can transform into a search when the information collected is considered in the aggregate.[109] When subject to aggregation in the hands of the government, the mosaic of data may reveal an all-encompassing picture of an individual's private life as it is pieced together through an unrelenting survey of that individual's public movements and appearances. That mosaic, according the D.C. Circuit, must be subject to Fourth Amendment protection.[110] Despite this lower court precedent, the *Jones* Court declined to follow this "digital mosaic theory" of the Fourth Amendment.[111]

The Court in *Jones* struggled to find a new approach to the privacy doctrine.[112] For whatever efficacy the mosaic theory has in the context of bringing GPS surveillance within the shadow of the Fourth Amendment, it has severe shortcomings when brought to bear on the kinds of big data cybersurveillance methods unearthed by the Snowden disclosures. The mosaic theory is premised upon a small data world. In a small data world, a traditional notion of surveillance involves the tailing and tracking of an individual. In a big data world, the tailing and tracking of entire populations is now constant and effortless. Meanwhile, the big data

---

David Gray & Danielle Keats Citron, *A Shattered Looking Glass: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy*, 14 N.C. J.L. & TECH. 381 (2013); Gray & Citron, *Quantitative Privacy*, *supra* note 5; Stephen E. Henderson, *Real-Time and Historical Location Surveillance After* United States v. Jones*: An Administrable, Mildly Mosaic Approach*, 103 J. CRIM. L. & CRIMINOLOGY 803 (2013); Matthew B. Kugler & Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 SUP. CT. REV. 205; Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CONST. L. & PUB. POL'Y 1 (2012); Benjamin Wittes, *Databuse: Digital Privacy and the Mosaic*, GOV. STUDS., BROOKINGS INST. (Apr. 1, 2011), http://www.brookings.edu/research/papers/2011/04/01-databuse-wittes [https://perma.cc/XG99-6AHS].

109. *See* Kerr, *Mosaic Theory*, *supra* note 5, at 313.

110. *See* United States v. Maynard, 615 F.3d 544, 563–64 (D.C. Cir. 2010).

111. *See* United States v. Jones, 565 U.S. 400, 404–05 (2012) (emphasizing that the Fourth Amendment violation was a physical occupation of "private property for the purpose of obtaining information"). *But see* Kerr, *Mosaic Theory*, *supra* note 5, at 311, 326–29, 344 (contending that there are five votes on the Supreme Court ready to adopt the mosaic theory under the Fourth Amendment and then addressing why this might be a mistake because such an approach "would require courts to answer a long list of novel and challenging questions" and because courts should "retain the traditional sequential approach to Fourth Amendment analysis").

112. *See generally* BALKIN, *supra* note 104 (arguing that using the metaphor of cultural software to describe the tools of understanding opens a way for moving beyond entrenched perspectives and provides a more productive account of critical theory).

cybersurveillance techniques described above do not focus on individuals. They harvest data in mass quantities and preserve it.[113]

The effectiveness of big data cybersurveillance depends upon an ever-widening harvest of data without regard to specific individuals at the time of collection. As explained by the Chief Technology Officer (CTO) of the Central Intelligence Agency (CIA), Ira "Gus" Hunt, "the value of any [piece] of information is only known when you can connect it with something else that arrives at a future point in time."[114] Because "you can't connect dots you don't have, it drives us into a mode of, we fundamentally try to collect everything and hang on to it forever."[115] As the Second Circuit noted of this "vast new technological capacity for large-scale and automated review and analysis" of data harvested through surveillance, "[t]he more metadata the government collects and analyzes, . . . the greater the capacity for such metadata to reveal ever more private and previously unascertainable information about individuals."[116]

The mosaic theory, however, does not speak to this kind of big data cybersurveillance. The mosaic under consideration by the D.C. Circuit in *Jones* had as its centerpiece an individual whose life was gradually being subjected to datafication through automated 24/7 geolocational surveillance. Stephen Leckar, representing Antoine Jones, explained to the Justices during the oral argument of *Jones* that the collection of his client's geolocation data through warrantless GPS tracking was the search and seizure of data.[117] While it was certainly a departure from what is conventionally understood as a search—given that it was conducted by means of simply accumulating data on Mr. Jones's whereabouts over the course of twenty-eight days thanks to a (comparatively antiquated) GPS

---

113. *See, e.g.*, Hu, *Small Data Surveillance v. Big Data Cybersurveillance*, *supra* note 4, at 834 (describing how the government justifies retaining all data gathered, regardless of its apparent law enforcement value); *see also* DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW (2007); Andrejevic, *Surveillance in the Big Data Era*, *supra* note 3; Danah Boyd & Kate Crawford, *Critical Questions for Big Data*, 15 INF. COMM. & SOC. 662 (2012); Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMM. OF THE ACM 498 (1988); Julie E. Cohen, *The Surveillance-Innovation Complex: The Irony of the Participatory Turn*, *in* THE PARTICIPATORY CONDITION IN THE DIGITAL AGE (Darin Barney et al. eds., 2016); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Slobogin, *Panvasive Surveillance*, *supra* note 2.

114. *See, e.g.*, Ira "Gus" Hunt, Chief Technology Officer of the Central Intelligence Agency, Presentation at GigaOM Structure: Data Conference: The CIA's "Grand Challenges" with Big Data (Mar. 20, 2013, 10:27 AM), https://gigaom.com/2013/03/20/even-the-cia-is-struggling-to-deal-with-the-volume-of-real-time-social-data [https://perma.cc/HLV6-Y7T7].

115. *Id.*

116. ACLU v. Clapper, 785 F.3d 787, 794 (2d Cir. 2015).

117. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16.

device—it was still a search within what might be called the small data paradigm. Antoine Jones was targeted by authorities who used a GPS device to transform his daily movements into analyzable data. Big data cybersurveillance, however, does not pursue individuals for the sake of accumulating data. It accumulates data to ensure that all individuals are pursued. The big data horizontal collection of data[118] under mass cybersurveillance, allowing wide sweeps of "digital dossier" files to be kept on an entire population, facilitates the government to flip the files to the vertical collection of data (e.g., initiating an investigation where the government drills down on a particular suspect) at any given moment.

Hunt expressed it poignantly: in traditional surveillance, you "move data to the question."[119] Thus, the police have a question about whether a suspect is connected to a drug ring (e.g., Antoine Jones, as a suspected drug dealer). Law enforcement then must "move data to the question" by now accumulating data about the suspect (vertical collection of data in a small data world). In *Jones*, the government accumulated geolocational data through GPS tracking to analyze the accumulated data to answer the guiding question: is Mr. Jones involved in a drug ring?

By contrast, with big data, you "move the question to the data." Big data does not monitor and track individuals; it creates vast databases which remain available to authorities with questions about individuals as a resource, and the records can be detained potentially indefinitely. All individuals are suspects, and authorities possess the prerogative to consult any particular suspect's aggregated data at any given time (e.g., investigators can flip an inquiry from a horizontal investigation to a vertical investigation of a data profile at any given moment). The database, data screening protocol, algorithmic analysis, etc., can yield a profile that aids an official in answering an investigatory question.[120] Because the algorithmic-based determination or database search protocol is created without reference to specific individuals, there may not be a governmental need to undertake a surveillance operation to create a mosaic of the sort accumulated in *Jones*.[121] Rather, with big data cybersurveillance, the objectionable mosaic in Fourth Amendment terms

---

118. *See* Matt Sledge, *CIA's Gus Hunt on Big Data: We 'Try To Collect Everything and Hang On To It Forever*,' HUFFPOST TECH. (Mar. 20, 2013 4:52 PM), http://www.huffingtonpost.com/2013/03/20/cia-gus-hunt-big-data_n_2917842.html [https://perma.cc/ASY8-VWHC] (Power Point presentation by CIA Chief Technology Officer Ira "Gus" Hunt at GigaOM's Structure Data Conference on March 20, 2013).

119. *Id.*

120. *See generally Big Data and the Future of Privacy*, ELEC. PRIVACY INFO. CTR. (2014), http://epic.org/privacy/big-data/ [https://perma.cc/B6WX-PKTW].

121. *See* Kerr, *Mosaic Theory*, *supra* note 5.

can be constituted simply through a government-initiated data search through personally identifiable information harvested in other contexts where there appeared to be no Fourth Amendment concerns.[122]

This reversal—moving the question to the data rather than moving the data to the question—is paradigmatic. In other words, the government has the capacity to accumulate data on everything and everyone merely in anticipation of its relevance to future questions, rather than accumulating data in response to a present question. This is consistent with the growing interest in preemptive cybersurveillance to serve anticipatory crime prevention goals through precrime programs that purport to identify criminals before a crime has occurred.[123] In that case, what may start as a data pattern emerging from a sea of data becomes a specific individual. The individual, in turn, becomes the site of an intervention by authorities for the purpose of preventing a criminal or terrorist act.[124] It is not clear how the Fourth Amendment applies to this mode of law enforcement, which is why a dramatic revision of the doctrine is now necessary. If the proponents of big data can translate the accumulation of "unthinkably large" sets of data into precrime enforcement actions (statistical and probabilistic certainty that an individual will commit a crime or act of terrorism), how will the Fourth Amendment and other constitutional protections respond?

---

122. *Id.*

123. *See, e.g.*, Ian Kerr, *Prediction, Preemption, Presumption: The Path of Law After the Computational Turn*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 112 (Mireille Hildebrandt & Katja de Vries eds., 2013) (contending that predictive technologies facilitate a philosophy of pre-emption that shifts ex post facto systems of punishment to ex ante systems of prevention in a way that threatens due process); David Cole, *The Difference Prevention Makes: Regulating Preventive Justice*, 9 CRIM. L. & PHIL. 501, 503 (2014) (describing how threat risk assessments will attempt to predict criminal or terroristic predisposition); Daskal, *Pre-Crime Restraints*, *supra* note 13, at 331 (stating that many pre-crime constraints are less comprehensive but impose considerable and often underappreciated costs on the targeted individual regardless); Ferguson, *Big Data and Predictive Reasonable Suspicion*, *supra* note 113, at 351 (contending that law enforcement already uses predictive policing technology to predict areas of crime, but that big data will predict actions and possibly individual behavior); Elizabeth E. Joh, *Policing by the Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 56 (2014) (questioning whether predictive software based on historical crime data is comparable to other uses of third party information that have previously been held to justify a reasonable suspicion determination); *see also* Ian Kerr & Jessica Earle, *Prediction, Preemption, Presumption: How Big Data Threatens Big Picture Privacy*, 66 STAN. L. REV. ONLINE 65, 66 (2013); Mark L. Noferi & Robert Koulish, *The Immigration Detention Risk Assessment*, 29 GEO. IMMIGR. L.J. 45 (2015).

124. *See, e.g.*, Cole, *The Difference Prevention Makes*, *supra* note 123, at 501 (explaining that mass surveillance is increasingly deployed to prevent crime and terrorism before it occurs and describing how preventative policing is utilized).

C. The Need for a New Fourth Amendment Test

The *Katz* test currently invites the federal judiciary to evaluate the constitutionality of emerging cybersurveillance technologies, programs, and protocols on an individual, case-by-case basis, and to evaluate whether a particular individual's privacy interests were harmed. Each time, the analysis centers on an individualized, personally subjective point of view: did this person have a reasonable expectation of privacy?

Under post-*Katz* precedent such as *United States v. Miller*,[125] *United States v. Knotts*,[126] and other cases, scholars have noted that the *Katz* test is no longer workable in light of emerging technologies.[127] Modern cybersurveillance offers the government tools that should not be construed as simply sensory-enhancing, such as the beeper in *Knotts*, or access to documents already provided to a third party, such as the bank records at issue in *Miller*. In 1979, in a footnote in *Smith v. Maryland*,[128] the Court contemplated that there might come a day when the *Katz* test could fail:

> Situations can be imagined, of course, in which *Katz*' two-pronged inquiry would provide an inadequate index of Fourth Amendment protection. For example, if the Government were suddenly to announce on nationwide television that all homes henceforth would be subject to warrantless entry, individuals thereafter might not in fact entertain any actual expectation of privacy regarding their homes, papers, and effects. Similarly, if a refugee from a totalitarian country, unaware of this Nation's traditions, erroneously assumed that police were continuously monitoring his telephone conversations, a subjective expectation of privacy regarding the contents of his calls might be lacking as well. In such circumstances, where an individual's subjective expectations had been "conditioned: by influences alien to well-recognized Fourth Amendment freedoms, those subjective expectations obviously could play no meaningful role in ascertaining what the scope of Fourth Amendment protection

125. 425 U.S. 435 (1976).

126. 460 U.S. 276 (1983).

127. *See, e.g.*, Solove, *Fourth Amendment Pragmatism*, *supra* note 5, at 1511–12 (applying the *Katz* test to contemporary Fourth Amendment challenges); Slobogin, *supra* note 31, at 11–31 (describing how existing precedent is no longer workable given technological advances); Wittes, *Databuse: Digital Privacy and the Mosaic*, *supra* note 108, at 2 (arguing that past conceptions of privacy have become obsolete).

128. 442 U.S. 735 (1979).

> was. In determining whether a "legitimate expectation of privacy" existed in such cases, a normative inquiry would be proper.[129]

During oral argument in *Jones*, several Justices appeared ready to contemplate the type of re-visioning of *Katz* that *Smith v. Maryland* suggested might be needed one day.[130] Justices Alito and Sotomayor, in their concurrences in *Jones*, made clear their beliefs that new technologies, and the cybersurveillance consequences of these new technologies, require such a revision in the modern age.[131]

Moreover, a revision is particularly urgent in light of the fact that the "Third Party Doctrine" has left Fourth Amendment jurisprudence ambiguous in the post-Snowden age. The Third Party Doctrine exempts from Fourth Amendment protection information provided by an individual to a third party: an individual lacks a reasonable expectation of privacy under *Katz* once information is shared with another entity.[132]

The ambiguity of what Fourth Amendment protections may be appropriate as applied to NSA cybersurveillance, and how the courts should test this protection, was borne out in two split decisions in

---

129. *Id.* at 740 n.5.

130. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 24. Justice Ginsburg said:

> [T]he Fourth Amendment says—or it has been interpreted to mean that if I'm on a public bus and the police want to feel my luggage, that's a violation; and yet, this kind of monitoring, installing the GPS and monitoring the person's movement whenever they are outside their house in the car, is not? I mean, it just—something about it that—just doesn't parse.

Id.

Justice Breyer said "Start—what would a democratic society look like if a large number of people did think that the government was tracking their every movement over long periods of time." *Id.* Justice Kagan said:

> I mean, if you think about this, and you think about a little robotic device following you around 24 hours a day anyplace you go that's not your home, reporting in all your movements to the police, to investigative authorities, the notion that we don't have an expectation of privacy in that, the notion that we don't think that our privacy interests would be violated by this robotic device, I'm—I'm not sure how one can say that.

Id. at 57–58.

131. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring). Justice Alito concurred:

> In addition, the Katz test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.

Id. at 427 (Alito, J., concurring) (emphasis in original).

132. *See* Smith v. Maryland, 442 U.S. 735, 742 (1979).

Klayman v. Obama[133] and *ACLU v. Clapper*[134] in December 2013.[135] Shortly following the Snowden disclosures, the ACLU filed a lawsuit challenging the NSA's bulk telephony data collection in *ACLU v. Clapper* in the U.S. District Court, Southern District of New York. Larry Klayman, founder of Freedom Watch, filed a similar lawsuit challenging the NSA's bulk telephony data collection in the U.S. District Court for the District of Columbia.[136]

The Snowden disclosures of June 2013 revealed that a "bulk telephony metadata program" had been operated for the past seven years pursuant to section 215 of the PATRIOT Act, and had allowed for the suspicionless and indiscriminate metadata surveillance of all U.S. citizens and residents impacted by the program.[137] Specifically, this program allowed for the Foreign Intelligence Surveillance Court to compel telecommunications companies to produce telephony metadata (calls to and from subscribers, length of call, etc.) on all calls made by any subscriber, including U.S. citizens, on an ongoing, daily basis. On December 27, 2013, United States District Judge William H. Pauley III in the Southern District of New York, an appointee of President Clinton, upheld the constitutionality of the program in *ACLU v. Clapper*.[138] Judge Pauley relied upon the Third Party Doctrine, claiming that telephone metadata had been shared with phone providers and thus, the plaintiffs could not claim a reasonable expectation of privacy under the *Katz* privacy test: "[t]he collection of breathtaking amounts of information unprotected by the Fourth Amendment does not transform that sweep into a Fourth Amendment search."[139] In doing so, he echoed Justice Black's dissent in *Katz*, refusing to depart from settled doctrine to construe a conversation as something that could be "searched" or "seized" by the government.[140] Judge Pauley was now only applying and refusing to depart from the reasoning of *Katz*.

Another judge, facing the same legal issue, evidenced restlessness with *Katz*. Less than two weeks earlier, on December 16, 2013, United States District Judge Richard J. Leon in the District of Columbia came to the

133. 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

134. 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part*, *vacated in part*, *and remanded*, 785 F.3d 787, 821 (2d Cir. 2015).

135. For a more complete listing of the litigation surrounding bulk surveillance, see *supra* note 30.

136. *Klayman*, 957 F. Supp. 2d at 11.

137. *See, e.g.*, GREENWALD, *supra* note 1.

138. 785 F.3d 787 (2d Cir. 2015).

139. *Clapper*, 959 F. Supp. 2d at 752.

140. *See* Katz v. United States, 389 U.S. 347, 366–67 (1967) (Black, J., dissenting).

opposite result in *Klayman v. Obama*,[141] finding the NSA program unconstitutional. Although the facts of each case were identical, Judge Leon, unlike Judge Pauley, did not find that the Third Party Doctrine of *Smith v. Maryland* was controlling. Rather, Judge Leon used an "Orwellian" standard to infuse the *Katz* privacy test and the Fourth Amendment with normative force and cultural weight.[142] By reasoning that the NSA program presented an "Orwellian" technology of surveillance, Judge Leon held that a reasonable expectation of privacy had been violated.

In this manner, Judge Leon interpreted the Fourth Amendment through a customary law standard. In other words, in line with Judge Leon's reasoning in *Klayman*, "the lawful privacy interests of individuals . . . individuals' 'reasonable expectations of privacy'—depend on the interests that society recognizes through law and custom."[143] Judge Pauley, in contrast, did not appear to consider a customary law dimension of the Fourth Amendment. Judge Leon recognized that *Katz* and subsequent precedent based on it mandated the result arrived at by Judge Pauley, but concluded that such "reasonable expectation" analysis lead to a starkly unreasonable result when placed in the modern context of the "almost-Orwellian technology" available to the government.[144]

Katz precedent suggested that an individual could not have a reasonable expectation of privacy, largely because the data collected by the bulk telephony metadata program had already been shared with third parties and thus effectually disclosed. But ratifying that result at the second stage of the analysis leads to implications that summon the Orwellian rhetoric that increasingly finds its way into Fourth Amendment cases. Judge Leon, quoting Justice Alito's concurrence in *Jones*, noted that in effect "some may assume that these cultural changes will force people to 'reconcile themselves' to an 'inevitable' diminution of privacy that new technology entails."[145] Judge Leon then reversed course, and starting from the second *Katz* step, concluded such an Orwellian result was itself unreasonable,

---

141. *Klayman*, 957 F. Supp. 2d at 32, *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) ("I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.").

142. *Id.* at 33.

143. Nita Farahany, *Searching Secrets*, 160 U. PA. L. REV. 1239, 1241 (2012); *see also* Naomi Mezey, *Law as Culture*, 13 YALE J.L. & HUMAN. 35, 35–67 (2001).

144. *Klayman*, 957 F. Supp. 2d at 33.

145. *Id.* at 35 (citations omitted) (quoting United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring)).

explaining: "I think it is more likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable."[146]

One cannot expect that what they disclose to others is private. But one can expect that what one discloses to the public will still be shielded from government surveillance in the form of constant collection and indefinite retention.[147] Judge Leon departed from controlling Supreme Court precedent by arguing that the disclosed information surveilled was qualitatively different because it was quantitatively different: "[b]ut the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly*, what that information can tell the government about people's lives."[148] Is this departure principled? When does an unreasonable expectation of privacy for publicly disclosed data become reasonable? At what point does a quantitative difference in lawful data surveillance become a qualitative difference that renders it subject to Fourth Amendment scrutiny?[149] Judge Leon reasoned that the Third Party Doctrine was leading the federal court to an Orwellian tipping point where the underlying logic of the reasonable expectation of privacy test of *Katz* becomes unreasonable:

> When do present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.[150]

---

146. *Id.* at 36 (emphasis in original).

147. *See, e.g.*, *id.* at 35–37 (contending that cultural changes have resulted in a greater expectation of privacy that is viewed as reasonable by modern societal standards).

148. *Id.* at 35–36 (emphasis in original).

149. *See, e.g.*, Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2479, 2489 (2014) (explaining that because of their function, storage capacity, and cloud access, "[c]ell phones differ in both a quantitative and qualitative sense from other objects that might be kept on an arrestee's person"); United States v. Jones, 565 U.S. 400, 415–16 (2012) (Sotomayor, J., concurring) (pointing out that GPS surveillance "generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail" about that person's various associations); United States v. Cotterman, 709 F.3d 952, 964 (9th Cir. 2013) (en banc) (discussing the qualitative and quantitative distinctions in digital data and storage in comparison); *see also* Daskal, *The Un-Territoriality of Data*, *supra* note 50, at 365–69; Donohue, *Bulk Metadata Collection*, *supra* note 2, at 871–72; Gray & Citron, *Quantitative Privacy*, *supra* note 5, at 65–68.

150. Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (emphasis in original), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

Judge Leon's opinion was daring but did not survive review by the D.C. Circuit, which overturned the district court's grant of a preliminary injunction based on standing concerns.[151] Judge Pauley's *Katz* analysis, however, similarly failed to survive review by the Second Circuit, which reversed and remanded on the grounds that the government's bulk telephony surveillance was not authorized by the Foreign Intelligence Surveillance Act of 1978 as amended by the USA PATRIOT Act of 2001.[152] Although the Second Circuit invoked the doctrine of constitutional avoidance and expressly declined to reach plaintiffs' Fourth Amendment claim, the court was not reticent about expressing doubts regarding *Katz*'s continued applicability in modern times, suggesting, like Judge Leon, that we may have reached an Orwellian tipping point and looking to Congress for guidance with regard to whether the *Katz* test remained reasonable.[153] Unpacking the Second Circuit's thoughts on this matter helps to sharpen the contours of the Fourth Amendment dilemma raised by big data surveillance.

Again, the court conceded that *Katz* did not protect publicly disclosed metadata: "[w]e recognize that metadata exist in more traditional formats, too, and that law enforcement and others have always been able to utilize metadata for investigative purposes."[154] Quantitative increases in the scope of surveillance leads to qualitative differences: "[b]ut the structured format of telephone and other technology-related metadata, and the vast new technological capacity for large-scale and automated review and analysis, distinguish the type of metadata at issue here from more traditional forms."[155] Because modern data trails left by individuals are so much more comprehensive, the sphere of an individual's subjective expectation of privacy is radically reduced: "[s]uch expansive development of government repositories of formerly private records would be an unprecedented contraction of the privacy expectations of all Americans."[156] The court elsewhere elaborated on the theme of *Katz*'s potential obsolescence:

> [T]he very notion of an individual's expectation of privacy, considered in *Katz* a key component of the rights protected by the

151. *Klayman*, 800 F.3d at 561.

152. ACLU v. Clapper, 785 F.3d 787, 821 (2d Cir. 2015).

153. *Id.* at 826 ("In light of the asserted national security interests at stake, we deem it prudent to pause to allow an opportunity for debate in Congress that may (or may not) profoundly alter the legal landscape.").

154. *Id.* at 794.

155. *Id.*

156. *Id.* at 818.

> Fourth Amendment, may seem quaint in a world in which technology makes it possible for individuals and businesses (to say nothing of the government) to observe acts of individuals once regarded as protected from public view.[157]

And the reach of the government's eye appeared to be unprecedented: "the bulk collection of data as to essentially the entire population of the United States, something inconceivable before the advent of high-speed computers, permits the development of a government database with a potential for invasions of privacy unimaginable in the past."[158] The court further noted that the question of whether such warrantless surveillance by the government may be permissible "seem[s] much more threatening as the extent of such [personal] information [subject to surveillance] grows."[159] Like Judge Leon, the court noted that this state of affairs has brought emerging surveillance developments to that Orwellian tipping point where the viability of *Katz* must be addressed.[160]

The Second Circuit held, but only for standing purposes, that collecting metadata in a database amounts to a seizure for Fourth Amendment purposes.[161] It expressed uncertainty about whether judicial restraint was appropriate given the national security concerns the government cited as the justification for the mass surveillance. The court noted that perhaps a radical diminution of privacy was warranted "by national security needs in the face of the dangers of contemporary domestic and international terrorism."[162] Thus, the same uncertainty that appeared in *Katz* over how revising Fourth Amendment doctrine may impinge national security manifests as *Katz* appears increasingly on the verge of undergoing its own judicial revision. The Second Circuit was, in effect, attempting to balance traditional expectations of privacy understood as protected by the Fourth Amendment with the Executive's need for a free hand in matters affecting national security, and it looked to Congress to resolve the dilemma: "[t]he endorsement of the Legislative Branch of government provides some degree of comfort in the face of concerns about the reasonableness of the government's assertions of the necessity of the data collection."[163] Thus, like Judge Leon, the Second Circuit analyzed the two-step *Katz* test,

---

157. *Id.* at 822 (emphasis in original).

158. *Id.* at 824.

159. *Id.* at 822–23.

160. *Id.* at 823 (observing that in United States v. Knotts, 460 U.S. 276, 284 (1983), the Supreme Court opined that "if . . . dragnet type law enforcement practices . . . should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable").

161. *Id.* at 801.

162. *Id.* at 818.

163. *Id.* at 824.

largely concluding that the first step is no longer tenable because the "expectation of privacy" defined in *Katz*'s terms collapses in the context of modern, technologically dependent daily life and, in the second step, changed the question to inquire whether society should ratify the current state of affairs—whether *Katz* itself is "reasonable" anymore. Or, more precisely, the question is whether the contemporary sweep of government surveillance, permitted by *Katz*, is itself reasonable. The Court punted the question to Congress:

> A congressional judgment as to what is 'reasonable' under current circumstances would carry weight—at least with us, and, we assume, with the Supreme Court as well—in assessing whether [big data surveillance techniques] render obsolete the third-party records doctrine or, conversely, reduce our expectations of privacy and make more intrusive techniques both expected and necessary to deal with new kinds of threats.[164]

The national security justification[165] calls into question whether the judiciary has the competence to "update" the Fourth Amendment in the name of preserving its relevance. Resort to Congress provides an avenue of interrogating the Executive's potentially self-serving representations of the need for surveillance in the face of modern threats. Indeed, Justice Douglas' concurrence in *Katz* opposed a "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant" where national security was involved because that Branch cannot be trusted to restrain itself.[166] That is not because the Executive is disingenuous, but because by constitutional design, "the Executive Branch is not supposed to be neutral and disinterested" and thus a magistrate is needed to determine when such surveillance is justified.[167] Near the end of *Clapper*, Judge Lynch's majority opinion for the Second Circuit developed the same theme, arguing that reconciling the public interest in privacy with the government's need for surveillance is a task involving "all three branches of government."[168] In his *Clapper* concurrence, Judge Sack cautioned that the adversarial system of most

---

164. *Id.* at 824–25.

165. *See, e.g.*, ACLU v. Clapper, 959 F. Supp. 2d 724, 745 (S.D.N.Y. 2013) (describing justification for bulk telephony metadata collection under statutory framework and how Congress remains informed regarding foreign intelligence surveillance); Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013) (discussing balance between the national security interests of the United States and the individual liberties of citizens), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

166. United States v. Katz, 389 U.S. 347, 359–60 (1967) (Douglas, J., concurring).

167. *Id.* at 359.

168. *See* ACLU v. Clapper, 785 F.3d 787, 826 (2d Cir. 2015).

courts might bolster the FISC's ability to objectively interrogate government representations about the need for surveillance rather than functioning largely as a rubber stamp.[169] Nevertheless, Judge Sack's concurrence emphasized that Congress must take the lead in determining the propriety of the growing government surveillance capacity.[170]

Judge Leon, meanwhile, after remand from the D.C. Circuit, held in 2015 that plaintiffs, by amending their complaint to add new plaintiffs, had cured their standing problem and once again granted a preliminary injunction (which was almost immediately vacated by the D.C. Circuit).[171] In the 2015 opinion, Judge Leon acknowledged the Second Circuit's view that Congress should take the lead in determining what was "reasonable" for purposes of revising Fourth Amendment doctrine, and countered with a much more robust view of the judiciary's responsibility to address constitutional violations where it finds them.[172] As Judge Leon explained: "this Court cannot, and will not, sit idle in the face of likely constitutional violations for fear that it might be viewed as meddling with the decision of a legislative branch that lacked the political will, or votes, to *expressly* and unambiguously authorize the Program for another six months."[173] Even in his 2013 decision, Judge Leon had explained that his task was "the latest chapter in the Judiciary's continuing challenge to balance the national security interests of the United States with the individual liberties of our citizens."[174]

As discussed above, *Katz* involved surveillance of criminal activity and, as a sub-current, the Justices debated the implications of their groundbreaking holding on national security.[175] For Judge Leon, that debate is not one in which the separation of powers doctrine calls for a collaborative effort. Rather, it plays out in the context of the Supreme Court's "special needs" doctrine.[176] That line of cases creates an exception to the general rule that "warrantless searches 'are *per se* unreasonable

169. *Id.* at 831 (Sack, J., concurring).

170. *Id.* at 832 ("[I]t is Congress that must decide in the first instance under what circumstance the government can obtain data touching upon conflicting national security and personal privacy interests.").

171. Klayman v. Obama, 142 F. Supp. 3d 172, 198 (D.D.C. 2015), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015); *see also supra* note 30.

172. *See Klayman*, 142 F. Supp. 3d at 183 n.12.

173. *Id.* (emphasis in original).

174. Klayman v. Obama, 957 F. Supp. 2d 1, 43 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

175. *See supra* notes 165–170 and accompanying text.

176. *See Klayman*, 957 F. Supp. 2d at 37–42.

under the Fourth Amendment.'"[177] Such cases arise where there is a special need for the government to proceed without a warrant, and in determining that such a warrantless search is proper, courts weigh the privacy interest compromised against the character of the government's intrusion as well as the need for and efficacy of the search.[178] Thus, having gone beyond *Katz* and found the collection of bulk metadata to constitute a search, Judge Leon then had to determine whether the government needed a warrant for such a search or whether national security concerns drew the bulk telephony metadata program within the ambit of the special needs doctrine.

As Judge Leon noted, there were already a number of cases in which the special needs doctrine had permitted searches to confront terrorist threats.[179] Had Judge Leon been drawing and relying upon such conclusions outside the context of the special needs analysis, he would have been at the very limits of, if not beyond, the judiciary's competence. The special needs doctrine, and the government's resort to it as a last line of defense, allowed Judge Leon to apply the law to facts, resulting in findings about the efficacy of the bulk telephony program in combatting terrorism. Yet, the government could not establish special need here because it could not establish "that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics."[180]

D. Big Data and the Fourth Amendment Outside the National Security Context

Much of Judge Leon's reasoning about modern expectations of privacy in the context of a big data society is echoed in the Supreme Court's recent decision of *Riley v. California*. There, applying a comparable exception to the Fourth Amendment warrant requirement, the Court had to balance a person's privacy interest in the data stored on a cell phone against the government's interest in such data when found in the possession of an arrested suspect.[181] The Court was receptive to arguments that big data is different, and altered existing precedent that suggested that anything on

177. City of Ontario v. Quon, 560 U.S. 746, 760 (2010) (emphasis in original).

178. *See Klayman*, 957 F. Supp. 2d at 38.

179. *Id.* at 38–39 (citing Second Circuit cases addressing permitting warrantless searches in vulnerable transportation hubs).

180. *Id.* at 40.

181. *See* Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2484–85 (2014).

an arrestee's person is fair game at the time of arrest.[182] Importantly, however, there were no arguments about national security implications and the government's interest in pursuing and stopping criminal activity was not enough to carry the day.[183]

As noted above, the question of whether an activity constitutes a search, the issue in *Katz*, is distinct from the follow-up question of whether a search remains reasonable for Fourth Amendment purposes, even in the absence of a warrant.[184] The Court has permitted warrantless searches in a number of circumstances, including the "search incident to arrest" doctrine discussed in *Riley*.[185] In *Riley*, the Court heard two consolidated cases that presented the same issue: whether police officers arresting an individual are entitled to search the contents of a suspect's cell phone for incriminating evidence.[186] The officers in both cases relied upon the "search incident to arrest doctrine," which the Court's precedent established as bright line categorical rule allowing a search of a suspect's person at the time of arrest.[187] Thus, as the Court explained in *Riley*, while a search of a suspect's house was not authorized, the search of "personal property . . . immediately associated with the person of the arrestee" is permissible.[188] Even if such a warrantless search may be perceived under some circumstances as unreasonable, this concern is overcome by the need to ensure the safety of the arresting officer and the need to preserve evidence on a suspect's person that might be destroyed or concealed.[189]

In explaining that the doctrine provides a bright line rule and that officers are entitled to examine what is on the suspect's person at the time of the arrest, even if there is no plausible argument that their safety requires such an examination or that material evidence might otherwise be destroyed, the Court was setting forth why the government should have won the case—just as it should have won the case in *Katz* and just as it should have won in *Klayman* and *Clapper* by virtue of *Katz*. Indeed, the

182. *Id.* at 2485 ("We therefore decline to extend *Robinson* to searches of data on cell phones, and hold instead that officers must generally secure a warrant before conducting such a search.").

183. *Id.*

184. *See supra* section I.A.

185. *Riley*, 134 S. Ct. 2473 at 2477–79.

186. *Id.* at 2482.

187. *Id.* at 2483.

188. *Id.* at 2484 (citing United States v. Chadwick, 433 U.S. 1, 15 (1977)).

189. *Id.* at 2483 (articulating the concerns as to whether these types of warrantless searches may be perceived as unreasonable); *id.* at 2484 (citing *Chadwick*, 433 U.S. at 15).

Court went so far as to say "a mechanical application of [the relevant precedent] might well support the warrantless searches at issue here."[190]

The Court's reasoning followed the familiar contours of cases refashioning settled doctrine. The Court explained that the cell phone is "based on technology nearly inconceivable just a few decades ago" when it established its governing "search incident to arrest" precedent.[191] Cell phones, while a physical object on the person, are different because of the amounts of data they contain. Quantitative difference, again, becomes a qualitative difference.[192] The quantity of information available on a phone is incomparable to what a person could physically carry were that information not in the form of data and, as such, searches of such data "implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse."[193] In his concurrence, Justice Alito pointed out the oddity that personal information in the form of letters, messages, and photos, when carried physically on the person are fair game but storing them electronically on the phone shields them from the arresting officer's search.[194] Essentially, the Court's holding appeared to accord greater protection to electronic data than tangible objects. Nevertheless, Justice Alito supported the Court's holding for lack of a "workable alternative" that provides clear guidance to the police in a world where "the nature of the electronic devices that ordinary Americans carry on their persons would continue to change."[195]

The Court was motivated by more than just the quantity of information accessible on a cell phone. It recognized that the cell phone is integral to modern society, noting they are ubiquitous and that "more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives."[196] Although Orwellian rhetoric does not find its way into *Riley*, the Court nevertheless considers the implications of "[a]llowing the police to scrutinize such records on a routine basis" and rejects it.[197]

---

190. *Id.* at 2484.

191. *Id.*

192. *Id.* at 2489 (noting that a phone can store "millions of pages of text" and that "[w]e expect that the gulf between physical practicability and digital capacity will only continue to widen in the future").

193. *Id.* at 2488–89.

194. *Id.* at 2497 (Alito, J., concurring) ("[T]he Court's broad holding favors information in digital form over information in hard-copy form.").

195. *Id.*

196. *Id.* at 2490 (majority opinion).

197. *Id.*

A significant observation from *Riley* is that the informational data on the cell phone is likely unprotected from a search under *Katz* because by storing such data on a cell phone, the data has been disclosed to third parties (the service providers) and, thus, there is arguably no longer any reasonable expectation of privacy. The Court notes, as a reason for protecting such data in the context of the search incident to arrest doctrine, that data on cell phones is stored on a network and accessed through remote servers.[198] The Court notes this by way of suggesting that such data is arguably not even physically present on the person of an arrestee, but the same observation could be mustered to defeat an argument that the arrestee ever had an expectation of privacy concerning such networked data.

The government suggested that an officer should at least be able to search the phone log, relying on precedent holding that use of a pen register did not offend the Fourth Amendment because the information gathered, having already been disclosed to a third party, was not subject to an expectation of privacy.[199] The Court rejected that argument because the question in the relevant case, *Smith v. Maryland*, was whether a search had even occurred, while in *Riley*, the government conceded that a search had occurred—the issue was whether a cell phone may be searched without a warrant incident to a lawful arrest.[200] Consequently, if examining publicly disclosed data does not constitute a search within the meaning of the Fourth Amendment, there can be no question whether the non-search was unreasonable absent a warrant.

Riley has answered the question of whether examining cellphone or smartphone data is a search in the first place.[201] There is an objective social expectation that police cannot routinely rifle through cellphone or smartphone data at the time of arrest without a warrant.[202] This, in turn, likely makes any subjective expectation of privacy for such data reasonable, regardless of how many other entities have access to or store such "private" personal information. The Court recognized the government's countervailing interest in accessing such information for law enforcement purposes.[203] The Court rejected arguments about protecting officer safety—that a cell phone search could alert officer's to

198. *Id.* at 2491.

199. *Id.* at 2492.

200. *Id.* at 2482 ("The two cases before us concern the reasonableness of a warrantless search incident to a lawful arrest.").

201. *Id.* at 2484.

202. *Id.* at 2492.

203. *Id.*

approaching criminal accomplices—because there was no "evidence to suggest that their concerns are based on actual experience."[204] The Court similarly rejected concerns about destruction of evidence—remote wiping of cell phones—because the Court had "been given little reason to believe that either problem is prevalent."[205] By requiring evidence of the claimed problem of remote deletion of phone data, the Court applied a judicially created test to determine when warrantless searches are reasonable.[206] This evaded any uncertainty that the Court was stretching its competence in evaluating whether the government needed warrantless access to cell phones to address criminal enterprises.

Riley did not address national security, evading the complexity of concerns that attempts to address international terrorism often adds. Even so, Justice Alito's concurrence echoed the Second Circuit's request for guidance in *Clapper*: "[l]egislatures [which], elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future."[207] Whether *Riley* would come out the same way if the case had involved national security or a terrorist bomb threat is unclear. The Court noted that the exigent circumstances exception provides recourse for law enforcement in the face of "the more extreme hypotheticals that have been suggested."[208] *Riley* appears to be a clear statement that the Court believes the Fourth Amendment shields personal data from a warrantless search, even if it does not squarely address whether collecting such data even comes within the ambit of a search or seizure under the Fourth Amendment. But its holding will not be fully tested (and potentially narrowed) until *Riley* is invoked as precedent in the context of a case implicating national security concerns.

II. CONTOURS OF THE *1984* CYBERSURVEILLANCE PROBLEM

What role, if any, will the Fourth Amendment play in restraining rapidly evolving data surveillance, or dataveillance, technologies, and cybersurveillance programs that now constitute what some scholars have described as the post-9/11 "National Surveillance State?"[209] The Fourth

204. *Id.* at 2485.

205. *Id.* at 2486.

206. *Id.* at 2478.

207. *Id.* at 2497–98 (Alito, J., concurring).

208. *Id.* at 2494 (majority opinion).

209. *See* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1

Amendment protects ordinary citizens from mass surveillance and suspicionless surveillance fishing expeditions.[210] Increasingly, therefore, ordinary citizens and other private parties are seeking Fourth Amendment protection from the expanding encroachment and intrusiveness of bureaucratized cybersurveillance and big data cybersurveillance.[211] These technologies execute surveillance through digital data, and big data- and database-driven methodologies that are increasingly comprehensive in scope.[212]

References to dystopian literature emerge to contextualize judicial results and evoke police state or totalitarian implications in federal court decisions. In effect, dystopian references mark the limits of current legal doctrines when confronted by the fast-changing social realities of a technologically driven economy and society. The invocation of dystopian narrative provides an extra-legal framework to explain why a potential legal result is intolerable even when, in a strictly legal framework, the result is not problematic at all. This invocation signals a critical need in the law: taking the pulse of the Constitution and related legal doctrines to ensure democratic vitality.[213] Thomas Crocker argues that dystopian

---

(2008); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006).

210. *See, e.g.*, Gray, *A Collective Right*, *supra* note 41, at 191 (arguing that "contemporary tracking technologies threaten the collective security of the people from unreasonable searches"); Tracey Maclin, *When the Cure for the Fourth Amendment Is Worse Than the Disease*, 68 S. CAL. L. REV. 1, 9 (1994); Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1107 (2002) ("[B]y obtaining private sector records, the government can conduct the type of 'fishing expeditions' that the Framers feared.") (citing LEONARD W. LEVY, ORIGINS OF THE BILL OF RIGHTS 158 (1999)).

211. *See* Clapper v. Amnesty Int'l USA, __ U.S. __, 133 S. Ct. 1138 (2013) (presenting prima facie challenges to the Foreign Intelligence Surveillance Amendments Act of 2008, which empowers the FISC court to authorize surveillance without a showing of probable cause that the target of surveillance is an agent of a foreign power).

212. Biometric databases, particularly DNA databases, are increasingly relied upon for a variety of criminal law purposes, including "DNA trawling" or "DNA fishing" for prosecution and conviction, as well as using DNA databases for genetic profiling to assess any predictive or diagnostic value. *See, e.g.*, David H. Kaye, *Please, Let's Bury the Junk: The CODIS Loci and the Revelation of Private Information*, 102 NW. U. L. REV. COLLOQUY 70, 71–81 (2007) (analyzing the medical and biological implications of DNA records in the National DNA Index System, and its local and state components); David H. Kaye, *Rounding Up the Usual Suspects: A Legal and Logical Analysis of DNA Trawling Cases*, 87 N.C. L. REV. 425, 425 (2009) (discussing how prosecutors may identify defendants by "fishing through a database of DNA types to find a match"); Andrea Roth, *Safety in Numbers? Deciding When DNA Alone Is Enough To Convict*, 85 N.Y.U. L. REV. 1130, 1131–85 (2010) (arguing that the numerical nature of pure cold hit evidence requires courts and deciders of fact to consider more carefully the sufficiency of the DNA method).

213. *See, e.g.*, Crocker, *Dystopian Constitutionalism*, *supra* note 28, at 595 (suggesting that a dystopian analysis provides a method through which constitutional values are articulated and applied in contrast to values and practices the American polity agrees it wishes to avoid).

constitutional analysis "provides a method through which constitutional values are articulated and applied in contrast to values and practices the American polity agrees it wishes to avoid."[214] Such rhetorical outbursts have no legal value in the sense that they are, of course, no more than just rhetoric.[215] But they are valuable in this context as a marker for the limits and gaps of our traditional legal discourse.

References to George Orwell's *1984* conjure up specific and widely recognized images of a police state,[216]

---

214. *Id.*

215. Courts are often resistant to parties raising these arguments. *See, e.g.*, Camara v. Gonzales, 166 Fed. App'x 840, 844 (6th Cir. 2006) ("This Court, however, does not have the authority to overturn federal regulations based on policy arguments, nor do the writings of George Orwell or any other fiction writer provide this Court with any legal authority."). Courts do, however, regularly refer to Orwell independently. *See infra* notes 216–21.

216. *See, e.g.*, Florida v. Riley, 488 U.S. 445, 466–67 (1989) (Brennan, J., dissenting) (describing the dangers of unchecked law enforcement); United States v. Mitchell, 652 F.3d 387, 409 (3d Cir. 2011) (explaining how DNA testing may empower the government to conduct DNA "dragnets"); United States v. Weikert, 504 F.3d 1, 14–15 (1st Cir. 2007) (describing potential governmental abuses of stored DNA information); Johnson v. Quander, 440 F.3d 489, 499 (D.C. Cir. 2006) ("[G]enetic fingerprints differ somewhat from their metacarpal brethren, and future technological advances in DNA testing (coupled with possible expansions of the DNA Act's scope) may empower the government to conduct wide-ranging 'DNA dragnets' that raise justifiable citations to George Orwell."); United States v. 15324 Cty. Highway E, Richland Ctr., 219 F.3d 602, 603 (7th Cir. 2000) (referencing the possibility of an Orwellian-type dystopia resulting from government abuse of surveillance technology), *vacated sub nom.* Acker v. United States, 533 U.S. 913 (2001); Cramer v. Consolidated Freightways, Inc., 209 F.3d 1122, 1135–36 (9th Cir. 2000) (Fisher, J., dissenting in part) (making reference to Orwell and mass surveillance); United States v. Kyllo, 190 F.3d 1041, 1050 (9th Cir. 1999) (Noonan, J., dissenting), *rev'd*, 533 U.S. 27 (2001) (describing the unappealing nature of an Orwellian surveillance state); United States v. Heinz, 983 F.2d 609, 619 (5th Cir. 1993) (Parker, J., concurring in part and dissenting in part) (arguing that no "chinese wall" allowing team prosecutors access to the ill-gotten gains because it would be an unacceptable risk of sanctioning Orwellian investigative techniques and creating a Kafka-like judicial administration); United States v. Cuevas-Sanchez, 821 F.2d 248, 251, nn.4–5 (5th Cir. 1987) (describing how indiscriminate video surveillance raises the spectre of the Orwellian state); United States v. Torres, 751 F.2d 875, 877 (7th Cir. 1984) (describing how certain surveillance techniques are "reminiscent of the 'telescreens' by which 'Big Brother' in George Orwell's 1984 maintained visual surveillance of the entire population"); *id.* at 887 (Cudahy, J., concurring); United States v. Penn, 647 F.2d 876, 882 (9th Cir. 1980) (explaining how a reversal of the suppression order at issue "would lead to systematic government programs to 'persuade' young children to inform against their parents, as in the societies created by George Orwell and Adolf Hitler"); United States v. Finazzo, 583 F.2d 837, 841–42 (6th Cir. 1978) ("The novels of Kafka and George Orwell evoke some of the same fears and concerns we feel when we contemplate the possibility that wholesale eavesdropping and wiretapping by federal and local police could spread and become customary."), *vacated*, 441 U.S. 929 (1979); Klayman v. Obama, 957 F. Supp. 2d 1, 29, 33 (D.D.C. 2013) (arguing that future technological advances in DNA testing might enable the government to carry out searches that raise justifiable references to George Orwell), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015); United States v. McCotry, No. IP 06-CR-25-01-H/F, 2006 WL 2460757, at *16 (S.D. Ind. July 13, 2006) (discussing how courts have a "strong preference" for searches conducted pursuant to a warrant), *rev'd sub nom.* United States v. Hollingsworth, 495 F.3d 795 (7th Cir. 2007) (quoting *Penn*, 647 F.2d at 882); Hansen v. Turnage, No. C88-30261 RPA, 1988

mass surveillance,[217] torture,[218] tyranny,[219] and thought crime.[220] *1984* often serves as a placeholder to explain how the law has failed to preserve individual autonomy, dignity, and rights in the face of changing social and political circumstances.[221] The moral force of *1984* can be attributed in part to Orwell's commitment to the democratic experiment.[222] Scholars have observed that the democratic principles embodied by the Constitution and the Declaration of Independence animated Orwell's philosophical vision for his novel.[223] Orwell concludes *1984* with an excerpt of the Declaration of Independence,[224] and as Akhil Amar, Jack Balkin, and others have explained, the Declaration of Independence animates and anchors the Constitution.[225] As a heuristic for a surveillance

---

WL 147881, at *3 (N.D. Cal. July 28, 1988) (discussing privacy concerns implicated in police searches); Capua v. City of Plainfield, 643 F. Supp. 1507, 1511 (D.N.J. 1986) (arguing that surveilling an individual's "off duty activities . . . is George Orwell's 'Big Brother' Society come to life"); Martinez v. Winner, 548 F. Supp. 278, 334 (D. Colo. 1982) (stating that "[n]o one wishes to live in a society of the kind described in George Orwell's *1984* or Ray Bradbury's *Fahrenheit 451*, and no federal court is going to be willing to grant its imprimatur to police intrusion into the security of an activist's person, house, papers and effects without strict adherence to Fourth Amendment standards"), *aff'd in part*, *rev'd in part*, 771 F.2d 424 (10th Cir. 1985).

217. *See, e.g.*, *supra* note 216 and *infra* notes 230–34 and accompanying text.

218. *See, e.g.*, United States v. Weber, 451 F.3d 552, 554 (9th Cir. 2006) (referencing Orwell in describing plethysmograph testing); Conner v. Sticher, 801 F.2d 1266, 1269 (11th Cir. 1986) (Clark, J., dissenting) (describing how state officials manipulated the plaintiffs' perception of reality comparable to the manipulation described in Orwell's *1984*).

219. *See, e.g.*, United States v. Black, 750 F.3d 1053, 1057 (9th Cir. 2014) ("The government verges too close to tyranny when it sends its agents trolling through bars, tempts people to engage in criminal conduct, and locks them up for unconscionable periods of time when they fall for the scheme.").

220. *See, e.g.*, *Weber*, 451 F.3d at 554; *id.* at 570–71 (Noonan, J., concurring) (arguing that there "is a line at which the government must stop" in surveillance).

221. *See, e.g.*, *id.* at 570–71; United States v. Kyllo, 190 F.3d 1041, 1050 (9th Cir. 1999) (Noonan, J., dissenting) (expressing concern that the majority regards the "Orwellian dangers as speculative and at most potential"), *rev'd*, 533 U.S. 27 (2001); *Penn*, 647 F.2d at 882 ("[A] reversal of the suppression order here would lead to systematic government programs to 'persuade' young children to inform against their parents, as in the societies created by George Orwell and Adolf Hitler."); Brian C. Murchison, *Speech and the Truth-Seeking Value*, 39 COLUM. J.L. & ARTS 55, 100 (2015) ("Perhaps the cases do not involve acts of power as audacious or violent as that imagined by Orwell, but the strong doctrines developed by courts display a wariness of power all the same, particularly its ability to come between the individual and his 'world.'").

222. GEORGE ORWELL, WHY I WRITE 8 (Penguin 2005) (1946) ("Every line of serious work that I have written since 1936 has been written, directly or indirectly, *against* totalitarianism and *for* democratic Socialism, as I understand it.").

223. *See* CHRISTOPHER HITCHENS, WHY ORWELL MATTERS 103–14 (2003).

224. ORWELL, 1984, *supra* note 15, at 311−12.

225. *See, e.g.*, AKHIL REED AMAR, THE UNWRITTEN CONSTITUTION 253–55 (2012) ("The Constitution's enactment was widely understood as an implementation and extension of the Declaration's ringing language . . . ."); JACK M. BALKIN, CONSTITUTIONAL REDEMPTION 23−24

state and how democratic principles are betrayed, *1984* is easily adopted by federal courts to characterize phenomena not yet adequately addressed by legal tools.[226] Specifically, through references to Orwell's *1984* in the context of the "reasonable expectation of privacy" standard in Fourth Amendment cases, federal courts, including the Supreme Court, increasingly express concern about mass surveillance as a social norm and the potential of constitutionalizing that norm.[227]

Part II begins again with *Jones*, but then considers some earlier Court decisions in which Justices signaled to *1984* to emphasize the problems of surveillance. This Part illustrates how such rhetoric recurs at junctures where the Fourth Amendment doctrine, although followed logically, appears to fail to adequately address evolutions in government surveillance. References to Orwell are, of course, pure rhetoric. Yet, this rhetoric emerges in the gap between legal doctrine and surveillance methods, and serves as a means for the Court to recognize the existence of the gap—and the problems that it creates. Section B of Part II looks at two dissenting opinions in earlier Court opinions—Justice Harlan's dissent in *United States v. White*,[228] and Justice Brennan's dissent in *Florida v. Riley*[229]—and notes the recurrence of similar rhetoric in parallel circumstances. In each of these cases, the Justices invoking such rhetoric shifted the focus from an individual's expectation of privacy to a broader social expectation about the limits of government intrusion.

(2010) (contending that the Declaration of Independence anchors "[t]he ultimate goal of our constitutional order . . . to produce not merely democratic procedures but a *democratic culture*") (emphasis in original).

226. *See, e.g.*, Crocker, *supra* note 28, at 603–06 (describing the elements of dystopian analysis).

227. This argument appears to be consistent with Critical Legal Studies. Mark Tushnet explains that it is possible to "abandon" constitutional rights if they are "defined on too abstract a level to be helpful in resolving the claims presented in particular cases." Mark Tushnet, *Critical Legal Studies: An Introduction to its Origins and Underpinnings*, J. LEGAL EDUC. 505, 516 (1986) ("According to the critique of rights, people cannot know what rights they have, and there are no political methods that guarantee those rights. The term 'Kafkaesque' is perfectly appropriate and provides a clue to the justification for the constructive program—or for the program of interminable critique. For by invoking Kafka's vision, the term allows CLS to say that it, like Kafka, is describing the condition of the modern world.").

228. 401 U.S. 745 (1971).

229. 488 U.S. 445 (1989) (plurality opinion).

A. Orwell and the Fourth Amendment

It is unsurprising that *1984*[230] was invoked by the Supreme Court during oral argument in *United States v. Jones*[231] in response to the government's contention that twenty-four-hour locational surveillance does not present a Fourth Amendment problem.[232] Additionally, in the post-Snowden litigation concerning the constitutionality of the NSA's bulk telephony data program, Judge Leon also invoked images of *1984*, characterizing the NSA's mass collection of U.S. telephone data as "almost Orwellian," before rejecting a mechanical application of current precedent to ratify the program.[233] Judge Leon explained, "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approval."[234]

Yet, while *Jones* marked one of the most recent collisions between cybersurveillance technology and the limits of traditional Fourth Amendment doctrine,[235] the Supreme Court has yet to come to grips with the full implications of the modern cybersurveillance world that Judge Leon conjured in *Klayman v. Obama*.[236] In *Jones*, the Supreme Court

---

230. ORWELL, 1984, *supra* note 15.

231. 565 U.S. 400 (2012).

232. Transcript of Oral Argument, United States v. Jones, *supra* note 16 at 13, 25, 27, 33, 35, 57.

233. Klayman v. Obama, 957 F. Supp. 2d 1, 32–33 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

234. *Id.* at 42.

235. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011)*; see also supra* note 45 (discussing the Court's grant of certiorari in Carpenter v. United States, 819 F.3d 880 (6th Cir. 2016)).

236. 957 F. Supp. 2d 1 (D.D.C. 2013). *See, e.g.*, Sherry F. Colb, *A World Without Privacy: Why Property Does Not Define the Limits of the Right Against Unreasonable Searches and Seizures*, 102 MICH. L. REV. 889, 890 (2004) (contending that while existing Fourth Amendment doctrine nominally protects normatively and empirically reasonable expectations of privacy, in practice the doctrine protects only but not privacy); William Funk, *Electronic Surveillance of Terrorism in the United States*, 80 MISS. L.J. 1491, 1492 (2011) (describing how combating international terrorism, or the war on terror, has confused the historical distinction between intelligence gathering and law enforcement); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409, 410–65 (2007) (outlining an analytical framework for Fourth Amendment issues that can be applied more broadly to future technological enhancements). Some scholars focus on statutory frameworks for governing surveillance technologies and for structuring domestic and foreign intelligence surveillance law. They recommend the enactment of congressional legislation, rather than reliance upon the Fourth Amendment, as the best prescription to any potential harms emanating from modern cybersurveillance. *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 806 (2004) (contending that the legislative branch rather than the judiciary should create the primary investigative

considered the constitutionality of the warrantless 24/7 tracking of a criminal suspect through a GPS-tracking device attached to a vehicle.[237] Law enforcement agents attached a GPS device to Antoine Jones's Jeep while it was located in a public parking lot in Maryland.[238] The device remained on Jones's vehicle for the next four weeks undetected.[239] During that time, at ten-second intervals, the device calculated and transmitted the vehicle's precise location to law enforcement computers that recorded and stored the data transmitted.[240] Ultimately, this GPS tracking enabled the government to discover the whereabouts of a stash house containing large amounts of narcotics.[241]

The Court decided the case on narrow grounds and temporarily avoided larger and lingering questions regarding what expectations of privacy are reasonable within the realm of cybersurveillance.[242] Nor does *Jones*

---

rules when technology is advancing); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 609–73 (2003) (describing how misconceptions about both the law and technology of the Internet has led to significant misunderstandings about Internet surveillance law and the effect of the USA Patriot Act); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1308 (2004) (explaining that the Supreme Court drew distinctions between domestic and "foreign intelligence" surveillance and what procedures were required under the Fourth Amendment) ("Supporters of surveillance could gain by a statutory system that expressly authorized foreign intelligence wiretaps, lending the weight of congressional approval to surveillance that did not meet all the requirements of ordinary Fourth Amendment searches. Critics of surveillance could institutionalize a series of checks and balances on the previously unfettered discretion of the President and the Attorney General to conduct surveillance in the name of national security.").

237. United States v. Jones, 565 U.S. 400, 402 (2012).

238. *Id.* The government had applied for, and received a warrant to install the device on the Jeep. *Id.* The warrant authorized installing the device within ten days in the District of Columbia. *Id.* at 402–03. The government installed the device eleven days later in Maryland. *Id.*

239. *Id.* at 403.

240. *Id.*; Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 50.

241. *Jones*, 565 U.S. at 402–04.

242. *See id.* at 411–13. The appropriate role of cybersurveillance in governance and promulgating security goals, as well as database privacy rights, are topics that have also formed the basis of rich academic discourse in recent years. *See, e.g.*, ROSEN, THE NAKED CROWD, *supra* note 4, at 29–30 (discussing the disconnect between invasive governmental policies and the purpose they were designed to serve and stating that "there is a grave danger . . . that our emotional response to the new fears that menace us will lead us to adopt ineffective and unnecessarily invasive architectures of identification and risk profiling that could linger long after the fears that inspired them have passed"); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1265–305 (2004) (recommending that warrants supported by probable cause should be required for the majority of uses of electronic surveillance); James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty and Hard-Wired Censors*, 66 U. CIN. L. REV. 177 (1997) (explaining how the conceptual structure of digital libertarianism lead its practitioners to ignore ways in which the government can use privatized enforcement and state-backed technologies to evade restraints on the exercise of legal power over the internet); Wittes, *Databuse: Digital Privacy and the Mosaic*, *supra* note 108, at 18 (describing the ideal balance between security and privacy rights).

articulate a limiting principle to restrain government intrusiveness with regard to comprehensive dataveillance and cybersurveillance.[243] As Justice Alito commented in his concurrence in *Jones*, when confronted with a "21st-century surveillance technique," the Court resorted to "18th-century tort law."[244] Yet, as the dramatic cybersurveillance disclosures provided by Snowden demonstrate, the GPS device considered in *Jones* is already antiquated by twenty-first century standards.[245]

As President Obama explained in an interview after the Snowden disclosures: "[i]n some ways, the technology and the budgets and the capacity [at NSA] have outstripped the constraints. And we've got to rebuild those [constraints] in the same way that we're having to do on a whole series of capacities . . . [such as] drone operations."[246] Federal courts, including the Supreme Court, are necessarily engaged in an attempt to develop those constraints in their effort to keep the Fourth Amendment relevant. Their recognition of the limits of current doctrine is evidenced by a recurrence of dystopian *1984*-styled rhetoric when confronted with modern governmental surveillance technologies. A central principle underpinning *1984*, and one that was not lost on several of the Supreme Court Justices during oral argument in *Jones*, is the notion

---

243. Multiple scholars have explored in depth the constitutional implications of technological advances in surveillance and the incorporation of such technologies in national security policy. *See, e.g.*, SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE: A NEW SOCIAL CONTRACT TO DEFEND FREEDOM WITHOUT SACRIFICING LIBERTY 6 (2011) (providing a new means to understand intelligence "in its modern context"); DAVID COLE & JULES LOBEL, LESS SAFE, LESS FREE: WHY AMERICA IS LOSING THE WAR ON TERROR 101 (2007) ("[T]here are deep-rooted reasons why government officials are unlikely to balance security and the rule of law fairly or accurately in times of crisis."); DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION: SACRIFICING CIVIL LIBERTIES IN THE NAME OF NATIONAL SECURITY (1999) (arguing that the war on terror can be fought without secret searches and guilt by association); Slobogin, *supra* note 31, at 11–46 (describing legal challenges associated with virtual surveillance as crime prevention and counterterrorism tools); JON L. MILLS, PRIVACY: THE LOST RIGHT (2008) (considering the role of the right to privacy in the modern day's intrusive world); Kerr, *Equilibrium-Adjustment Theory*, *supra* note 235, at 479 (describing how judicial decisions interpreting the Fourth Amendment are infamous for their "byzantine patchwork of protections"); Jonathan Zittrain, Comment, *Searches and Seizures in a Networked World*, 119 HARV. L. REV. F. 83, 84 (2005) (arguing that any retrieval of information stored on a computer hard drive should be considered a distinct Fourth Amendment search). *See, e.g.*, Hutchins, *supra* note 236, at 413 (arguing that existing Fourth Amendment jurisprudence can effectively rein in the use of emerging GPS technology).

244. *Jones*, 565 U.S. at 418 (Alito, J., concurring).

245. *See* GREENWALD, *supra* note 1; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/YM93-7869].

246. Ellen Nakashima, *NSA Morale Down After Edward Snowden Revelations, Former U.S. Officials Say*, WASH. POST (Dec. 7, 2013), http://www.washingtonpost.com/world/national-security/nsa-morale-down-after-edward-snowden-revelations-former-us-officials-say/2013/12/07/24975c14-5c65-11e3-95c2-13623eb2b0e1_story.html [https://perma.cc/UE8Y-VNK2].

that individual autonomy must be preserved to maintain a functional democratic society.[247] This principle has been deployed in the court of public opinion to illuminate a growing concern over various newly emerging cybersurveillance and dataveillance programs.[248]

During oral argument of *Jones*, the references to *1984* suggested that the Court was deeply disturbed by the implications of a ruling ratifying potentially untrammeled surveillance.[249] The oral argument expressed a need to avoid "an omen of *1984*,"[250] "a *1984*-type invasion"[251] of privacy, "the so-called *1984* scenarios,"[252] and the "*1984* [M]inistry of [L]ove, [M]inistry of—of [P]eace problem."[253] In *Jones*, *1984* served as a cultural touchstone establishing the boundaries of socially acceptable monitoring of citizens even if such monitoring did not violate any reasonable expectation of privacy under the Fourth Amendment's *Katz* test.

In *Jones*, the Court considered whether government GPS-enabled surveillance of an individual's every movement, every minute of every day for as long as the government may wish, raises a Fourth Amendment problem.[254] On the one hand, it is settled law that there are typically little or no Fourth Amendment protections for our movements in public places because there is no reasonable expectation of privacy in places where other people can naturally observe us.[255] In a small data world, the Court has previously drawn a line between what is public and private.[256] Vehicle movements along public roads cannot be considered private and, therefore, are not constitutionally protected from government surveillance.[257] Thus, a lot more of nothing—in the form of all-encompassing tracking of your movement in public spaces through GPS

247. ORWELL, 1984, *supra* note 15.

248. *See, e.g.*, Adam Liptak, *Court Asks If 'Big Brother' Is Spelled GPS*, N.Y. TIMES (Sept. 10, 2011), http://www.nytimes.com/2011/09/11/us/11gps.html [https://perma.cc/9TJ4-PV9T] (discussing the Court's potential decision on the constitutionality of warrantless GPS tracking in advance of oral argument in United States v. Jones, 565 U.S. 400 (2012)).

249. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13, 25–26, 33, 35, 57.

250. *Id.* at 27.

251. *Id.* at 57.

252. *Id.* at 25.

253. *Id.* at 35.

254. *See* United States v. Jones, 565 U.S. 400, 402–03 (2012).

255. *See, e.g.*, Hutchins, *supra* note 236, at 413 (arguing that existing Fourth Amendment jurisprudence can effectively be read to rein in the use of GPS as one emerging tracking technology).

256. *See, e.g.*, United States v. Katz, 389 U.S. 347, 359–61 (discussing the test for privacy expectations).

257. *See, e.g.*, *Jones*, 565 U.S. at 406 (discussing the government's contention that the location of a vehicle—when visible to all—means there is no reasonable expectation of privacy).

surveillance—is still nothing. Or, as Judge Sentelle of the D.C. Circuit quipped, "[t]he sum of an infinite number of zero-value parts is also zero."[258] According to Judge Sentelle's logic, if under the law, (A) we lack any reasonable expectation of privacy with regard to our public comings and goings; therefore, it follows that (B) we lack any reasonable expectation of privacy in the government's accumulation of data tracking our every movement in a public space every day for as many days, or months, or years, as the government wishes, without our knowledge or consent.[259] In other words, quantitative differences cannot become qualitative differences under the relevant legal test.

And yet, to say that unlimited and comprehensive surveillance of the kind facilitated by 24/7 GPS tracking is not legally cognizable as a Fourth Amendment problem struck several of the Justices as troubling. Both specific Justices and counsel during oral argument invoked *1984* to serve as a benchmark against which to measure what they considered to have been the intuitively unreasonable result sought by the government's argument, regardless of how legally sound, because of its potentially anti-democratic implications.[260]

The government countered that sophisticated tracking techniques, such as the use of remote GPS monitoring technologies, proved even more reasonable than other accepted surveillance methods. Specifically, the government contended that because remote data-driven surveillance does not offend the expectation of freedom from physical or sensory-based intrusion,[261] one of the traditional bulwarks of Fourth Amendment protection, it must be reasonable. The government's rationale suggests a gradual diminishment of Fourth Amendment protections. As individuals become accustomed to continuous location tracking, and such data is accumulated and stored by the government and third parties, the government's argument becomes more persuasive. That is, there is no reasonable expectation of privacy left to be violated by cybersurveillance or dataveillance facilitated by common digital surveillance technologies and government programs.

---

258. United States v. Jones, 625 F.3d 766, 769 (D.C. Cir. 2010) (Sentelle, J., dissenting from denial of rehearing en banc).

259. *Id.*

260. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 57–58; *see also* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

261. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 8–9.

B. Dystopian Narratives as Constitutional Touchstones

Some scholars have asserted "analogies to Orwell are just about always useless."[262] Other scholars have contended that *1984* does not accurately capture the types of issues and harms presented by modern cybersurveillance technologies[263] and present-day democratic societies.[264] Nevertheless, as Orin Kerr has argued, Fourth Amendment jurisprudence has historically struggled to mediate between unacceptable extremes: anarchy (where the police are rendered toothless) and dystopia (where police dominate society).[265] References to *1984* during oral argument in *Jones* make clear which side of the spectrum the Court was concerned with. This concern is not limited to GPS technology, but encompasses new technologies that facilitate automated, automatic, and continuous government surveillance on a widespread basis. This Orwellian tipping point recurs in various court decisions addressed to GPS and cybersurveillance technologies and it marks the gap between current Fourth Amendment doctrine and what courts regard as socially intolerable results from straightforward application of existing precedent.[266]

---

262. LESSIG, *supra* note 3, at 208. One critic explains that a natural aversion to Orwell may be the result of over-used *1984* metaphors and an over-veneration of the author; Orwell "requires extricating from a pile of saccharine tablets and moist hankies; [as] an object of sickly veneration and sentimental over-praise." HITCHENS, *supra* note 223, at 3.

263. *See, e.g.*, DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 25–26 (2011) (asserting that Kafka provides a better metaphor than Orwell to complement an understanding of the contemporary contours of surveillance); Ric Simmons, *Why 2007 Is Not Like* 1984*: A Broader Perspective on Technology's Effect on Privacy and Fourth Amendment Jurisprudence*, 97 J. CRIM. L. & CRIMINOLOGY 531, 531–36 (2007) (arguing that technologies have enhanced privacy and that surveillance technologies engaged by law enforcement represent a response to enhanced levels of privacy enabled by newly introduced technologies); Kerr, *Internet Surveillance Law After the USA Patriot Act*, *supra* note 236, at 673 (contending that the PATRIOT Act did not result in Orwellian expansion of Internet surveillance powers by government, explaining that "a focus on the details of the legislation suggests that the Act that has been portrayed as the road to Big Brother does not actually head there").

264. *See* Michael Moynihan, *Sorry, We're Not Living in Orwell's '1984'*, NEWSWEEK (June 19, 2013), http://mag.newsweek.com/2013/06/19/sorry-we-re-not-living-in-orwell-s-1984.html [https://perma.cc/TXT6-JZHD].

265. Kerr, *Equilibrium-Adjustment Theory*, *supra* note 235, at 488; *see also id.* at 499–501.

266. Past scholarship has noted a connection between Orwell and the Fourth Amendment. *See, e.g.*, Arcila, Jr., *supra* note 108, at 3 (observing that the Supreme Court compared law enforcement's aggressive use of GPS tracking to dystopia and George Orwell's *1984*); Crocker, *supra* note 28, at 595–632 (highlighting numerous judicial references to Orwell's dystopian future and the modern surveillance state); Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299, 301 (2010) (contending that despite Orwell's fearful vision and the government's technological ability to intrude on privacy, the Fourth Amendment on its face seems to prohibit such surveillance).

As one scholar has explained, *1984* "depict[s] the completely bureaucratized society, in which man is a number and loses all sense of individuality."[267] This is presented as an uncomfortable parallel to current bureaucratized measures whereby individuals such as Mr. Jones—or, as the government conceded, even the Justices themselves[268]—could be subject to the search and seizure of identity, and dissected by their geolocational data. With the advent of big data cybersurveillance technologies, some experts note that protecting privacy as a legal doctrine, such as through a defense of the *Katz* reasonable expectation of privacy test, can no longer be the primary concern.[269] Given the comprehensiveness of ubiquitous mass cybersurveillance technologies, the predominant concern now is how to protect the "sanctity of the individual."[270] With the search and seizure of identity, the key harm is metaphysical and philosophical: the steady erosion of autonomy and self-determination, and the slow backslide away from a commitment to a vision of inalienable rights that comes with such identity-centered searches and seizures.

Since *Katz*, the Court has frequently confronted how best to preserve a reasonable expectation of privacy in light of an increasing adoption of unreasonable surveillance technologies and modern surveillance practices. In *United States v. White*[271] and *Florida v. Riley*,[272] two cases nearly twenty years apart, dissenting Justices highlighted their concern about where the burden of protecting individual expectations of privacy lay. In both opinions, the dissenters pointed out the harm done to Fourth Amendment values—with potentially disastrous (or even dystopian) consequences—by constitutionalizing surveillance as a norm.

---

267. Erich Fromm, *Afterword*, *in* ORWELL, *supra* note 15.

268. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 9–10.

> CHIEF JUSTICE ROBERTS: You think there would also not be a search if you put a GPS device on all of our cars, monitored our movements for a month? You think you're entitled to do that under your theory?
>
> MR. DREEBEN: The Justices of this Court?
>
> CHIEF JUSTICE ROBERTS: Yes. (Laughter.)
>
> MR. DREBEEN: Under our theory and under this Court's cases, the Justices of this Court when driving on public roadways have no greater expectation of—

Id.

269. *See* Chemerinsky, *supra* note 11 (arguing that the current jurisprudence on the Fourth Amendment should be altered to accommodate changing technology and forms of information that can be seized).

270. MAYER-SCHÖNBERGER & CUKIER, *supra* note 13, at 17.

271. 401 U.S. 745 (1971).

272. 488 U.S. 445 (1989) (plurality opinion).

In *United States v. White*, White appealed from a 1966 federal narcotics conviction arguing that the use of a radio transmitter without a warrant by a government informant violated his Fourth Amendment rights.[273] The informant carried the transmitter on his person. Some of the conversations between White and the informant took place in the informant's home, with an agent listening to the conversations from the informant's kitchen closet. Other conversations took place elsewhere, including White's home, and government agents listened to the conversations with radio equipment.[274] The Seventh Circuit reversed White's conviction, concluding that *Katz* prohibited the agents' testimony.[275] The Supreme Court concluded that the Seventh Circuit erred by "misinterpret[ing] both the *Katz* case and the Fourth Amendment and in any event erred in allying the *Katz* case to events that occurred before that decision was rendered by this Court."[276] Relying on prior precedent involving informant and undercover agent conversations,[277] the Court concluded that "[i]f the law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent, neither should it protect him when that same agent has recorded or transmitted the conversations which are later offered in evidence to prove the State's case."[278] Under the *Katz* framework, this expectation of privacy fails because society would not ratify such an expectation of privacy.

Justice Harlan dissented in a notable and oft-cited opinion in which he discussed his concerns surrounding unchecked law enforcement use of technology. He explained that, while technology can be used for enforcing criminal laws, given "the stream of current developments in Fourth Amendment law . . . it must be held that third-party electronic monitoring, subject only to the self-restraint of law enforcement officials, has no place in our society."[279] Justice Harlan did not intend to prohibit the use of

---

273. *White*, 401 U.S. at 746–47.

274. *Id.* at 747.

275. *Id.* ("The Court of Appeals read *Katz v. United States* as overruling *On Lee v. United States*, and interpreting the Fourth Amendment to forbid the introduction of the agents' testimony in the circumstances of this case." (citations omitted)).

276. *Id.*

277. *See, e.g.*, Hoffa v. United States, 385 U.S. 293, 314 (1966) (referencing the government's use of informers and undercover agents); Lewis v. United States, 385 U.S. 206, 208–11 (1966) (discussing the acceptable use of undercover agents to garner evidence); Lopez v. United States 373 U.S. 427, 451–52 (1963) (discussing the secret electronic transmission or recording of private communications via undercover agent); On Lee v. United States, 343 U.S. 747, 749–50 (1952) (evaluating the admissibility of evidence collected by an undercover agent).

278. *White*, 401 U.S. at 752.

279. *Id.* at 790 (Harlan, J., dissenting).

"electronic eavesdropping," rather, he believed that law enforcement officers should obtain a warrant based on probable cause.[280] Such a requirement is, Justice Harlan explained, necessary to protect "the expectation of the ordinary citizen" to engage in free private conversations without worrying about whether his words will be used against him out of context years later.[281] Justice Harlan's opinion suggests that the warrant requirement of the Fourth Amendment protects "a measure of privacy and a sense of personal security throughout our society."[282]

Electronic surveillance troubled Justice Harlan because of the complexity of attempting to balance the issues in context of the Fourth Amendment, and due to the "prevalence of police utilization" of "the numerous devices that make technologically feasible the Orwellian Big Brother."[283] For Justice Harlan, the fundamental principles of the Fourth Amendment protect core democratic values and traditions by "plac[ing] limitations on the means and circumstances by which the government may collect information about its citizens by intruding into their personal lives."[284] These principles, as well as the capabilities of modern technology, led Justice Harlan to conclude that electronic surveillance by law enforcement requires a different analysis: "the burden of guarding privacy in a free society should not be on its citizens; it is the government that must justify its need to electronically eavesdrop."[285] Nearly twenty years later, Justice Brennan raised many of these arguments in a dissent that dealt not with increased surveillance capacities due to technology, but with invasive law enforcement surveillance practices.[286]

In *Florida v. Riley*, a plurality of the Supreme Court concluded that an individual lacked an expectation of privacy in the contents of his greenhouse that were visible from a police helicopter hovering at 400 feet.[287] Justice Brennan dissented, arguing that the plurality opinion "reads almost as if *Katz v. United States* had never been decided."[288] Justice

280. *Id.* ("It would prevent public officials from engaging in that practice unless they first had probable cause to suspect an individual of involvement in illegal activities and had tested their version of the facts before a detached judicial officer.").

281. *Id.*

282. *Id.*; *see also* David Gray, *Fourth Amendment Remedies as Rights: The Warrant Requirement*, 96 B.U. L. REV. 425, 479 (2016).

283. United States v. White, 401 U.S. 745, 770 (1971) (Harlan, J., dissenting).

284. *Id.* at 792.

285. *Id.* at 793.

286. Florida v. Riley, 488 U.S. 445, 456–68 (Brennan, J., dissenting).

287. *Id.* at 451–52 (plurality opinion).

288. *Id.* at 456 (Brennan, J., dissenting) (citation omitted).

Brennan argued that the plurality misapplied *Katz*'s focus on whether officers violate a reasonable expectation of privacy, such as an individual's expectation of privacy in his curtilage, rather than whether officers had a legal right to be where they were when they engaged in surveillance.[289] The better inquiry under this case, Justice Brennan explained, was whether such surveillance "is consistent with the 'aims of a free and open society.'"[290] He rejected the plurality's suggestion that such surveillance might be a Fourth Amendment problem because of interference with the occupant's normal use as irrelevant to the meaning of the Fourth Amendment.[291] Fundamental principles behind the Fourth Amendment such as personal privacy, security, dignity, and protection from arbitrary government invasions arguably mandated a different result in *Florida v. Riley*, at least according to Justice Brennan.[292]

The real problem, Justice Brennan pointed out, is not whether intimate activities could be observed,[293] but whether there was any limiting principle behind aerial surveillance that could observe any citizen at any time.[294] Citing both Justice Harlan's dissent in *White*, and Anthony Amsterdam's *Perspectives on the Fourth Amendment*, Justice Brennan concluded that *Florida v. Riley* seemed to switch the burden of protecting privacy to the citizen, rather than requiring the government to justify its decisions.[295] Justice Brennan ended his opinion with a sobering reminder of the potential for constitutionalizing dystopian norms through decisions that, though consistent with precedent, ultimately undermine fundamental values behind the Fourth Amendment. He pointed out that "the police surveillance methods [the plurality] would sanction were among those

---

289. *Id.*

290. *Id.* at 457 (quoting Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974)).

291. *Id.* at 461–62 ("If through noise, wind, dust, and threat of injury from helicopters the State 'interfered with respondent's normal use of the greenhouse or of other parts of the curtilage,' Riley might have a cause of action in inverse condemnation, but that is not what the Fourth Amendment is all about.").

292. *Id.*

293. *Id.* at 463 ("Where in the Fourth Amendment or in our cases is there any warrant for imposing a requirement that the activity observed must be 'intimate' in order to be protected by the Constitution?").

294. *Id.* at 464 ("If the Constitution does not protect Riley's marijuana garden against such surveillance, it is hard to see how it will prohibit the government from aerial spying on the activities of a law-abiding citizen on her fully enclosed outdoor patio.").

295. *Id.* ("As Professor Amsterdam has eloquently written: 'The question is not whether you or I must draw the blinds before we commit a crime. It is whether you and I must discipline ourselves to draw the blinds every time we enter a room, under pain of surveillance if we do not.'" (quoting Anthony Amsterdam, *Perspectives on the Fourth Amendment*, 58 MINN. L. REV. 349, 403 (1974))).

described 40 years ago in George Orwell's dreadful vision of life in the 1980s."[296] Quoting from a passage in *1984* that described helicopter surveillance into people's windows, Justice Brennan concluded: "Who can read this passage without a shudder, and without the instinctive reaction that it depicts life in some country other than ours?"[297]

Both Justices Brennan and Harlan reached for *1984* to contextualize and explore the complexities and dangers of unchecked law enforcement intrusions into citizens' lives. Those intrusions, while apparently constitutional—which is to say consistent with existing law and precedent interpreting the Fourth Amendment—nevertheless raised concerns about the erosion of core constitutional principles underlying the Fourth Amendment absent revision of court doctrine. Both the majority in *White* and the plurality in *Florida v. Riley* place the burden of restraining government intrusion on the citizen who must demonstrate a reasonable expectation of privacy as the basis to restrain the government.[298] Yet, Justice Brennan and Justice Harlan, uncomfortable with the result of that judicial inquiry, urge that the Fourth Amendment should place the burden on the government to justify the kind of intrusion the Court is asked to endorse as consistent with the Fourth Amendment.

Justice Brennan and Justice Harlan used Orwellian references to highlight the danger of constitutionalizing unconstitutional norms through rote application of existing precedent—a strategy that the Supreme Court justices used in the *Jones* oral argument. In each case, resort to rhetoric implicitly conceded that there is simply inadequate legal vocabulary or doctrinal principles yet developed to help the Court address the potential indiscriminate mass surveillance consequences that can be facilitated by new surveillance technologies.

III. CUSTOMARY LAW AND THE FOURTH AMENDMENT

Judicial appeals to Congress to provide guidance in how Fourth Amendment doctrines should evolve acknowledge the Legislative branch's fact-finding authority. And, in congressional testimony, Congress has previously heard that an evaluation of the Fourth Amendment requires an assessment of cultural values and societal

296. *Id.* at 466.

297. *Id.* at 467.

298. The Court did not actually apply the *Katz* test to the circumstances in *United States v. White* because the events in the case occurred before the Court had decided *Katz*. *See* United States v. White, 401 U.S. 745, 747 (1971). The Court concluded that the Seventh Circuit had erred by applying *Katz*. *Id.*

customs. In 1975, Congress convened intelligence oversight activities under what is now referred to as the "Church Committee."[299] The Committee was convened in response to media reports that claimed the CIA had been engaging in domestic operations against antiwar protestors and other individuals during the Nixon Administration.[300] It had a broad mission: to investigate "governmental operations with respect to intelligence activities and of the extent, if any, to which illegal, improper, or unethical activities were engaged in by any agency of the Federal Government . . . ."[301] The hearings and reports of the "Church Committee" fell within the jurisdiction of the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, under the chairmanship of Senator Frank Church. The House Select Committee on Intelligence under the chairmanship of Representative Otis Pike conducted parallel hearings.[302]

Pursuant to the Church Committee proceedings, Congress held hearings focused on how federal wiretapping surveillance implicated the Fourth Amendment and staged a general investigation of the issue in a way that cannot typically occur in a courtroom. On October 29, 1975, Attorney General Edward H. Levi testified before the U.S. Senate as part of a series of congressional investigatory activities to "discuss the relationship between electronic surveillance and the Fourth Amendment."[303] Attorney General Levi explained:

> Our understanding of the purposes underlying the [F]ourth [A]mendment has been an evolving one. It has been shaped by subsequent historical events, by the changing conditions of our modern technological society, and by the development of our own traditions, customs, and values. . . . [O]ur perceptions of the language and spirit of the [A]mendment have gone beyond the historical wrongs the [A]mendment was intended to prevent. The Supreme Court has served as the primary explicator of these evolving perceptions and has sought to articulate the values the [A]mendment incorporates. [304]

---

299. *See* S. Res. 21, 94th Cong. (1975) (establishing the Select Committee to Study Governmental Operations with Respect to Intelligence Activities).

300. *See* Christopher M. Ford, *Intelligence Demands in a Democratic State: Congressional Intelligence Oversight*, 81 TUL. L. REV. 721, 739–40 (2007).

301. *See* S. Res. 21, 94th Cong. (1975) at 1.

302. *See* Ford, *supra* note 300, at 746.

303. *The National Security Agency and Fourth Amendment Rights: Hearing before the Select Comm. To Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 84 (1975) (written and oral statement of Edward H. Levi, Attorney General of the United States).

304. *Id.* at 93.

The focus of the Fourth Amendment, therefore, involves keeping its literal text relevant to the changing context in which it must apply: the evolving "traditions, customs, and values"[305] in which the Fourth Amendment must remain relevant if a living Constitution is to persist.

Attorney General Levi explicitly pointed out the limitations of the *Katz* privacy test. He explained that *Katz* in of itself does not provide a limiting principle on "unlimited governmental intrusions[,]" and, therefore, cannot of itself provide a vehicle to assess whether a government surveillance program or practice "would pose too great a danger to the spontaneity of human thought and behavior."[306] Quoting Justice Harlan's dissent in *United States v. White*, Levi observed that assessments of privacy "are in large part reflections of laws that translate into rules the customs and values of the past and present."[307] Levi concluded that the proper interpretation of the Fourth Amendment necessitates "[a] weighing of values" and understanding the circumstances surrounding both privacy expectations and "the need for an intrusion and its likely effect."[308] Levi's testimony was intended to inform statutory efforts to provide proper oversight to the intelligence community in light of emerging electronic surveillance capacities. The Church Committee's efforts ultimately led to the enactment of the Foreign Intelligence Surveillance Act (FISA).[309]

The Church Committee and FISA are examples of the Legislative branch intervening to protect judicially created Fourth Amendment doctrine. As we have seen, there remains an active, ongoing debate on whether or not Congress is in a better position than the federal courts to determine the boundaries of the Fourth Amendment in light of changing

---

305. *Id.*

306. To be clear: the test emplaced by *Katz* cannot assess the intrusiveness of government programs, but, as Levi noted, the emergence of the *Katz* test reflected a judicial assessment about the intrusiveness of the government's growing ability to monitor phone conversations. *Id.* at 75 ("*Katz* turned ultimately on an assessment of the effect of permitting such unrestrained intrusions on the individual in his private and social life. The judgement was that a license for unlimited governmental intrusions upon every telephone would pose too great a danger to the spontaneity of human thought and behavior.").

307. *Id.* (quoting United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting) ("The analysis must, in my view, transcend the search for subjective expectations or legal attribution of assumptions of risk. Our expectations, and the risks we assume, are in large part reflections of laws that translate into rules the customs and values of the past and present.")).

308. *Id.* ("A weighing of values is an inescapable part in the interpretation and growth of the Fourth Amendment. Expectations, and their reasonableness, vary according to circumstances. So will the need for an intrusion and its likely effect. These elements will define the boundaries of the interest which the Amendment holds as 'secure.'").

309. *See* Donohue, *Bulk Metadata Collection*, *supra* note 2, at 766 ("Chaired by Senator Frank Church, the Committee uncovered a range of disconcerting domestic surveillance operations—including some conducted by the NSA—prompting Congress to pass the FISA.").

technology and national security needs.[310] In his concurrence in *Riley v. California*, Justice Alito pointed out that after *Katz*, Congress enacted a statute that "authorizes but imposes detailed restrictions on electronic surveillance[,]" rather than leaving the development of legal doctrine around electronic surveillance to federal courts.[311]

Insofar as the query is whether a search is reasonable absent a warrant—the question of *Riley v. California*—the issue involves transposing the original intent of the Fourth Amendment into modern circumstances such that the Amendment remains viable. In this sense, it is logical to seek legislative guidance. Deciding what is reasonable involves a broad social inquiry requiring courts to evaluate competing interests of a citizenry to be free from untrammeled surveillance and the government's real need to meet threats of terrorism and criminal activity.

Justice Alito's plea for legislative intervention, as well as other judicial pleas, appear to be aimed toward obtaining guidance from the legislative branch on the proper parameters of surveillance programs and practices. Justice Alito explained in *Riley v. California* that "it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond" to rapidly changing technological developments and social norms.[312] Be that as it may, courts do not always have the luxury of waiting for Congress to legislatively resolve what otherwise might pose a Fourth Amendment problem. Courts must decide cases and controversies as they reach them.

Where those cases and controversies involve the Fourth Amendment in a collision with cybersurveillance, the judiciary must decide whether and how the cultural norms of Fourth Amendment values are to be protected. The second step of *Katz*—assessing a socially reasonable expectation of privacy—requires a judicial response that examines Fourth Amendment

---

310. *See, e.g.*, Riley v. California, __ U.S. __, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring) (observing that new technologies are making it easier for the government to collect information about the everyday lives of ordinary Americans); Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 51–52 (discussing the privacy implications in light of contemporary technological developments such as the potential for warrantless GPS tracking).

311. *Riley v. California*, 134 S. Ct. at 2497 (Alito, J., concurring) ("The regulation of electronic surveillance provides an instructive example. After this Court held [in *Katz*] that electronic surveillance constitutes a search even when no property interest is invaded . . . Congress responded by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 82 Stat. 211. . . . Since that time, electronic surveillance has been governed primarily, not by decisions of this Court, but by the statute, which authorizes but imposes detailed restrictions on electronic surveillance." (citations omitted)).

312. *Id.* at 2497–98.

first principles. Yet, these principles require new doctrine to guide the judiciary if it is to sustain the Fourth Amendment at all. Such norms—a kind of constitutional customary law—start to reveal themselves at the point where the "reasonable expectation" of *Katz* leads to patently unreasonable results—an Orwellian tipping point that courts thus far "know it when [they] see it,"[313] even if they have not as yet been able to comfortably articulate a new doctrine. Indeed, caution about articulating such a new doctrine appears warranted given that, as courts repeatedly note in decisions confronting big data-type surveillance, technology is rapidly evolving. Given the current state of affairs, it may be best if, for the time being, constitutional doctrine remains flexible, with an eye toward making sure the results of decisions avoid blessing Orwellian outcomes rather than focusing on adhering to a consistent and internally logical doctrine that may lose its constitutional relevance on the eve of its first formulation. Meanwhile, as courts are forced to achieve results in the face of unsteady doctrine, those accumulating results may themselves start to form the contours of a contemporary "customary law of privacy" from which the dots can be connected to establish the tenets of a doctrine. It appears that several Justices of the Court during *Jones*'s oral argument, by invoking *1984*, had "sought to articulate the values the Amendment incorporates."[314] In short, the Court recognized that the Fourth Amendment doctrine must now evolve to accommodate limitations on government intrusiveness in light of increasingly comprehensive and invasive cybersurveillance technologies.[315]

Currently, the Fourth Amendment is the site of multiple challenges to the intrusiveness of cybersurveillance and dataveillance on private lives.[316] Of course, as the government conceded during the oral argument in *Jones*, these cybersurveillance and dataveillance programs may also implicate equality and First Amendment protections, among other concepts.[317] Other scholars have examined the implications of digitalized decision making on due process rights, or "technological due process."[318]

---

313. *See, e.g.*, Jacobellis v. Ohio, 378 U.S. 184, 197 (1964) (Stewart, J., concurring) (explaining a case-by-case approach to judicial decision-making).

314. Prepared Statement of Edward H. Levi, *supra* note 303, at 93.

315. *See, e.g.*, United States v. Jones, 565 U.S. 400, 415–17 (2012) (Sotomayor, J., concurring) (observing that technological advances that have made possible non-trespassory surveillance techniques will further affect the *Katz* test by impacting the development of societal privacy expectations).

316. *See, e.g.*, *supra* notes 30, 50.

317. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 23.

318. *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1301–13 (2008) (articulating a new model of technological due process as a means for an agency to

But, for present purposes, the focus of this discussion remains on whether and how the Fourth Amendment poses a restraint on government cybersurveillance capacities.

This Part returns to *Jones*, with an initial focus on the legal precedents and arguments the government invoked. The government focused on *Knotts*, a case that the government persuasively suggested was directly on point. This discussion is intended to clarify how normative, or customary, the Court's Fourth Amendment doctrine already is. The government and Court argued about normative expectations of privacy changing to accommodate technological conveniences. Justice Alito's concurrence embraced much of this discussion, expressly noting the danger of the "reasonable expectations of privacy" coming to embrace its unreasonable diminution.[319]

A. Privacy Customs and the Fourth Amendment

The oral argument transcript in *Jones* demonstrates real concern on the bench that prior precedent was driving the Court into a corner in which it would have to affirm a government position whose implications, although resisted by the government, were clearly viewed by several Justices as Orwellian. Thus, while normally the oral argument transcript is of negligible importance in comparison to the written decision that follows, here the give and take of the discussion, and its frequent departure from the legal issue into broader social concerns, shows the deeper concerns animating the final compromise that was the published opinion. Orwellian rhetoric is rife in that discussion, and it marks a broad cultural understanding of what protections the Fourth Amendment should afford—even if, legally speaking, that is not what the Fourth Amendment in fact currently protects. These expectations are found in an ordinary citizen's understanding of the Fourth Amendment, regardless of how those expectations on the "street" diverge from what Fourth Amendment precedent indicates is actually protected by the Constitution.[320] The dystopian rhetoric employed by several Justices reveals their beliefs that a normative conceptualization of the relationship between citizen and

---

choose between automation or human discretion); Margaret Hu, *Big Data Blacklisting*, 67 FLA. L. REV. 1735, 1759 (2015) (arguing that big data permits exclusion to be based on an abstraction, for example digitally inferred or algorithmically anchored guilt or suspicion); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 619 (2011) (contending that the real harm is not the mere accessing of information, which is generally publicly available, but rather what is then done with the already-disclosed information).

319. *Jones*, 556 U.S. at 419 (Alito, J., concurring in judgment).

320. *See, e.g.*, *supra* notes 19–35 and accompanying text; *infra* Table 1 and accompanying text.

government exists,[321] one that, strictly speaking, carries no legal weight—but one which nevertheless exerts a kind of gravitational pull on the development of legal doctrine.[322]

Much of the *Jones* argument revolved around the Court's 1982 case, *United States v. Knotts*,[323] which set forth the relevant legal standard and, as applied to the facts, is not distinguishable in any material way from *Jones*, according to the government. In an attempt to rebut the government's contention, Jones's attorneys relied on a caveat in the *Knotts* opinion, whereby the Court explained that should the precedent one day open the door to over-intrusive government surveillance, the Court would then be willing to revisit its holding or at least consider whether different constitutional principles ought to shape the result.[324] *Knotts*, following *Katz*, explained that the Fourth Amendment applies where "the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action."[325] The Court in *Knotts* elaborated on the nature of the second prong of the *Katz* test as asking whether "the individual's expectation, viewed objectively, is 'justifiable' under the circumstances."[326]

Thus, and relevantly here, we can characterize the standard as customary in nature insofar as the second prong involves asking whether society would ratify an individual's expectation of privacy "under the circumstances" in which the individual held it. In other words, the second step involves asking whether the individual's privacy expectation coincides with a broader social norm or whether it is just peculiar to that individual. Moreover, what is reasonable is to some extent contextually defined and, therefore, subject to change as the context changes.

Circumstantial reason leaves ample room for litigants to maneuver, but also allows the Court to maintain a flexible Fourth Amendment doctrine. In *Jones*, the government argued that the apparent intrusiveness of its progressively comprehensive surveillance methods is mediated by a

---

321. *See generally* Kerr, *The Mosaic Theory*, *supra* note 47 (arguing that the Fourth Amendment doctrine should evolve to help preserve the balance of power between citizen and government in the face of emerging technologies).

322. The topic that is central to a robust debate in the international law context is the appropriate role of custom in law, and how and when custom transforms into something that is cognizable as embodying the force of law. *See, e.g.*, Bradley & Gulati, *supra* note 20.

323. 460 U.S. 276 (1983).

324. *See id.* at 283–84 (1983) (justifying the Court's reservation of the issue for a later time).

325. *Id.* at 280 (quoting Smith v. Maryland, 442 U.S. 735 (1979)) (citations omitted).

326. *Id.* at 281 (quoting Katz v. United States, 389 U.S. 347, 353 (1967)).

public increasingly accustomed to being monitored by new forms of technology.[327] In short, the expectations of privacy are diminishing as people come to understand that they are enmeshed in a weave of various surveillance technologies and that they voluntarily assent to a number of them. Jones's attorneys argued that expectations of privacy have not adapted to technological changes, thus exposing large swaths of society to quotidian surveillance in ways that were not considered practicable before.[328] Put differently, increasingly comprehensive surveillance cannot be socially normalized as "reasonable" because a society in which such all-encompassing surveillance is the norm is prima facie unreasonable—that is, it is something out of *1984*.[329]

This legal quandary posed by *Jones* is what makes it distinguishable from *Knotts*.[330] In *Knotts*, law enforcement officers were able to discover the location of a secluded methamphetamine drug laboratory by enclosing a transmitting device in a can of chloroform sold to one of the defendants.[331] The car carrying the chloroform transmitted beeping signals, enabling police to track the car even after pursuing agents abandoned a physical tail.[332] In *Jones*, the government argued that GPS is simply a more technologically efficient and advanced beeper—the GPS device is simply a super-beeper.[333]

In *Knotts*, the Court concluded there was no Fourth Amendment violation.[334] It began by claiming that the beeper provided no more than locational information, explaining that "[t]he governmental surveillance conducted by means of the beeper in this case amounted principally to the following of an automobile on public streets and highways."[335] By this logic, because a car driving down the road is subject to public scrutiny, one cannot reasonably expect their location to be private; "[a] person traveling in an automobile on public thoroughfares has no reasonable

327. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 57.

328. *Id.* at 33–34, 44, 48.

329. *See generally* ORWELL, 1984, *supra* note 15; s*ee also* Florida v. Riley, 488 U.S. 445, 466–67 (1989) (Brennan, J., dissenting) (quoting from *1984* and concluding the opinion by arguing that "[w]ho can read this passage without a shudder, and without the instinctive reaction that it depicts life in some country other than ours?").

330. *See generally* Hutchins, *supra* note 236 (outlining the legal implications of the *Knotts* opinion).

331. United States v. Knotts, 460 U.S. 276, 278–80 (1983).

332. *Id.* at 278.

333. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 4, 13, 60–61.

334. *Knotts*, 460 U.S. at 281.

335. *Id.*

expectation of privacy in his movements from one place to another."[336] As the Court noted, by driving on the road, one is submitting to "[v]isual surveillance."[337] However, one does not necessarily expect to constantly transmit their location to the public through means of an electronic beeper.

Yet, the Court refused to find a qualitative difference between old-fashioned eyeballing and this form of electronic surveillance: "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[338]

Thus, according to the Court, technology that amplifies the capacity to see what could be seen by the naked eye does not alter the Fourth Amendment analysis.[339] For example, using a searchlight to explore the deck of a ship only reveals information that was already available to the naked eye, albeit under limited conditions (i.e., during daylight hours to a person situated in visual proximity to the deck).[340] Similarly, the use of a phone entails surrendering the number one has dialed to the third party telecommunications provider because "[t]he switching equipment that processed those numbers is merely the modern counterpart of the operator who, in an earlier day, personally completed calls for the subscriber."[341] Thus, the human element might drop out of the surveillance equation completely, rendered obsolete by technological improvements.

The automation of surveillance makes a quantitative increase in the level of surveillance scrutiny to which a person can be subject feasible. Thus, practically speaking, this diminishes one's expectation of privacy even if, from a legal perspective, there is no reasonable expectation of privacy for things such as public location. Thus, in *Knotts*, there was no basis to sanction the use of a beeper that continuously transmitted locational information to the police as long as there was no expectation of

---

336. *Id.*

337. *Id.* at 282.

338. *Id.*

339. By contrast, technology that creates new capacities can invade Fourth Amendment protections. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 35–36 (2001) (acknowledging that the rule the court adopts must account for more sophisticated technologies that are already in use or being developed). In *Kyllo*, however, the Court added a fascinating qualifier to when "sense-enhancing" technology might not be a search: "where . . . the technology in question is not in general public use." *Id.* at 34. The Court did not define "general public use," but the term raises the possibility that if technology becomes sufficiently widespread and in use, it might be "exemp[t] from constitutional scrutiny." Morgan Cloud, *Rube Goldberg Meets the Constitution: The Supreme Court, Technology and the Fourth Amendment*, 72 MISS. L.J. 5, 48–49 (2002).

340. United States v. Knotts, 460 U.S. 276, 282–83 (1983) (citing United States v. Lee, 274 U.S. 559, 563 (1927)).

341. *Id.* at 283 (quoting Smith v. Maryland, 422 U.S. 735, 744–45 (1979)).

privacy regarding such locational information in the first place. In other words, "scientific enhancement . . . raises no constitutional issues which visual surveillance would not also raise."[342]

That should have put an end of the matter in *Knotts*; nevertheless, the Court saw fit to entertain a "parade of horribles" argument that, based on the reasoning of the case, should have been dismissed off-hand: "[r]espondent does not actually quarrel with this analysis, though he expresses the generalized view that the result of the holding sought by the government would be that 'twenty-four hour surveillance of any citizen of this country will be possible, without judicial knowledge or supervision.'"[343] In response to this contention, the Court observed that merely alleging that the police are becoming more effective is insufficient evidence of a constitutional violation, and that "the 'reality hardly suggests abuse.'"[344] As a result, *Knotts* held there was no Fourth Amendment violation where the beeper merely enhanced law enforcement's existing surveillance capabilities, while also noting that "if such dragnet-type law enforcement practices as respondent envisions should eventually occur, there will be time enough then to determine whether different constitutional principles may be applicable."[345]

In other words, *Knotts* suggested that should the technological capabilities of law enforcement change in such a manner that enhancement of current surveillance abilities amounted to a qualitatively different kind of surveillance, then at that future date, the Court might scrutinize other constitutional principles to discover a limiting principle regarding the conduct *Knotts* appears to sanction.[346] Because the *Knotts* court either did not take seriously the hypothetical proffered by plaintiff regarding the flowering of a dragnet scheme of 24/7 surveillance, or believed such capabilities to have been too distant and abstract to address head-on in 1982, it decided to kick the proverbial can down the road. By 2010, the D.C. Circuit concluded that the futuristic "parade of horribles" set forth in *Knotts* in fact reflected the current state of affairs.[347] As such, at oral argument, Justice Breyer reflected this sentiment in his statement to the Government's counsel in *Jones*: "if you win this case, then there is

342. *Id.* at 285.

343. *Id.* at 283 (citation omitted).

344. *Id.* at 283–84 (quoting *Zurcher v. Stanford Daily*, 436 U.S. 547, 566 (1978)).

345. *Id.* at 284 (citation omitted).

346. *Id*.

347. *See, e.g.*, United States v. Maynard, 615 F.3d 544, 568 (D.C. Cir. 2010) (reversing conviction because it was obtained using evidence procured through warrantless GPS tracking in violation of the Fourth Amendment).

nothing to prevent the police or the government from monitoring 24 hours a day the public movement of every citizen of the United States."[348]

Jones marks a measured victory for those seeking more robust Fourth Amendment protections in the face of technological advances, as the Court's resolution of the case was largely designed to reject the government's main contention that the Court's established Fourth Amendment precedent permits warrantless GPS surveillance for any length of time. Nevertheless, *Jones* avoided the larger and unresolved question of what should replace the prevailing two-prong Fourth Amendment reasonable expectation of privacy test to adequately address the emerging dragnet-type cybersurveillance and dataveillance technologies at the disposal of government and law enforcement actors.

Jones picked up where *Knotts* left off and, from the government's perspective during the Supreme Court oral argument, is indistinguishable from it. The GPS device in *Jones* neither provided information about what was inside Jones's Jeep, nor conversations and activities carried out while in the Jeep. It merely transmitted locational data on a constant basis.[349] *Knotts* expressly stated that there was no reasonable expectation of privacy with regard to the location of a vehicle driving along public roads because such a vehicle was exposed to the general public.[350] The GPS device operated similarly to the beeper device in *Knotts* except that it made long-term, comprehensive surveillance feasible, the results of which were automatically recorded as data subject to law enforcement review at their convenience.[351] *Knotts* went out of its way to establish that technological innovations that merely amplify existing surveillance capacities do not raise any constitutional issues, provided that the surveillance is restricted to movements subject to no reasonable expectation of privacy.[352] Justice Alito, in his *Jones* concurrence, declined to "accept . . . the holding in *United States v. Knotts*" and criticized the majority for deciding a case about a twenty-first century surveillance technique "based on 18th-century tort law."[353]

In *Jones*, the government attempted to articulate a number of distinctions previously drawn by the Court to show it was acting in accord

348. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13.

349. *See* United States v. Jones, 565 U.S. 400, 429.

350. United States v. Knotts, 460 U.S. 276, 281 (1983).

351. *See* United States v. Maynard, 615 F.3d 544 (D.C. Cir. 2010); Brief for Respondent, United States v. Jones, 565 U.S. 400 (2012); Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 57.

352. *See Knotts*, 460 U.S. at 282–83.

353. *Jones*, 565 U.S. at 418–21 (Alito, J., concurring) (citation omitted).

with settled precedent permitting warrantless surveillance, including: public versus private spaces in *Knotts*; interference with possessory interests versus technical trespasses in *United States v. Karo*;[354] and open fields doctrine versus trespass law violations in *Oliver v. United States.*[355] The government explained, "there are enclaves of Fourth Amendment protection that this Court has recognized" and the usage of the GPS technology at issue in *Jones* does not fall within these specified enclaves.[356] The government also reminded the Court that it previously dealt with surveillance technology that at the time of the Court's contemplation "seemed extraordinarily advanced."[357]

During oral argument in *Jones*, the Deputy Solicitor General, Michael Dreeben, explained to the Court, "if this Court agrees with principles in *Knotts* and *Karo* and applies them to this case, the [privacy] remedy is through legislation."[358] Congress indeed has taken action to protect privacy interests legislatively in light of advancing electronic communication technologies.[359] The "privacy mosaic theory" advanced by the D.C. Circuit to preserve the Fourth Amendment's protections in *Jones* was met with the government's counter-theory, an investigation mosaic theory.[360] The government argued that the point of any investigation is to piece together a mosaic and that the Court has allowed the government in the past to utilize tools to build that mosaic.[361] GPS is not the only tool that helps in the development of the mosaic, the government explained, "[s]o does a pen register. So does a garbage pull. So does looking at everybody's credit card statement for a month. All of those things this Court has held are not searches."[362] During the *Jones* oral argument, the government concluded, "[i]f this Court believes that there is an excessive chill created by an actual law or universal practice of monitoring people through GPS, there are other constitutional principles [such as the Equal Protection Clause and the First Amendment] that are

354. 468 U.S. 705 (1984).

355. 466 U.S. 170 (1984).

356. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 12.

357. *Id.* at 13.

358. *Id.* at 11–12.

359. *See generally* Electronic Communication Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (2006).

360. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 16; DAVID COLE, ENEMY ALIENS: DOUBLE STANDARDS AND CONSTITUTIONAL FREEDOMS IN THE WAR ON TERRORISM (2003) (noting that government has argued regularly that it builds a mosaic around terrorist suspects).

361. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 16.

362. *Id.* at 16.

available."[363] The government also concluded, "if the Court believes that there needs to be a Fourth Amendment safeguard as well [as a legislative one], we have urged as a fallback position that the Court adopt a reasonable suspicion standard."[364]

Justice Alito's concurrence, in which Justice Kagan joined, recognized the potentiality of the "reasonable expectation" test to actually accommodate ever-increasing government intrusiveness.[365] Justice Alito noted that the "hypothetical reasonable person" is presumed to have a "well-developed and stable set of privacy expectations. But technology can change those expectations."[366] People accept diminished privacy as a "tradeoff" for the "increased convenience or security" of new technology and "even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable."[367] In other words, the test is grounded in changing social norms that the Court must then give effect to as a form of customary law—the custom here being the general expectation about what can reasonably be kept private.

B. Preserving Reasonable Expectations in an Unreasonable Cybersurveillance State

Unlike the D.C. Circuit, which had relied upon a digital mosaic theory, the *Jones* Court did not seem to have any clear direction on how to distinguish *Knotts*.[368] The oral argument did not seem to address the fact that Jones had no reasonable expectation of privacy when traveling on public thoroughfares. Instead, as noted above, it was the aspects of the case that *Knotts* held immaterial that seemed most objectionable in *Jones*—that the surveillance was automatic and effortless, and that it was all-encompassing. The context in which an average individual had no reasonable expectation of privacy had changed between *Knotts* and *Jones*: The National Surveillance State had acquired surveillance technology that, unrestrained, appeared itself unreasonable.

Justice Alito's concurrence does not fully explain how he would have resolved the case; however, he offers a critical shift away from privacy

---

363. *Id.* at 23.

364. *Id.* at 26.

365. *See* United States v. Jones, 565 U.S. 400, 426–27 (2012) (Alito, J., concurring).

366. *Id.*

367. *Id.*

368. *See, e.g.*, Kerr, *Mosaic Theory*, *supra* note 5, at 323–24 (discussing that *Jones* argued on appeal that *Knotts* was distinguishable because a GPS was "'light years away' from a radio beeper").

and toward intrusion: "[t]he best that we can do in this case is apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated."[369] It is not clear that existing Fourth Amendment doctrine is actually being applied in this formulation, since "intrusiveness" does not necessarily equate to a reasonable expectation of privacy.

Further, what constitutes over-intrusive surveillance remains unelaborated. Indeed, Justice Alito's concurrence avoids these questions by invoking a certitude that the Fourth Amendment bars the government's conduct: "[w]e need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[370] That perspective, which enables the analysis to proceed without elaboration, is precisely the hallmark of the Orwellian tipping point: it confirms the inference that something improper was before the Court while betraying uncertainty as to exactly why, legally speaking, the Constitution is offended. In the context of Justice Alito's concurrence, it enables an *ipse dixit* assertion that the Fourth Amendment is offended, while leaving it to later cases to parse out just when the government's surveillance transforms into an unreasonable search due to its prolonged nature.

The *Jones* argument had several moments where several of the Justices recognized that they were faced with an unreasonable state of affairs without the ability to articulate a legal doctrine that is violated by its presence. Here is Justice Breyer, early in the argument, speaking to the government's counsel:

> [I]f you win this case, then there is nothing to prevent the police or the government from monitoring 24 hours a day the public movement of every citizen of the United States. And—and the difference between the monitoring and what happened in the past is memories are fallible; computers aren't.
>
> And no one, or at least very rarely, sends human being to follow people 24 hours a day. That occasionally happens. But with the machines, you can. So, if you win, you suddenly produce what sounds like *1984* from their brief. I understand they have an interest in perhaps dramatizing that, but—but maybe overly. But it still sounds like it.[371]

369. *Jones*, 565 U.S. at 430 (Alito, J., concurring).

370. *Id.*

371. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13.

Justice Scalia pointed out that this tack was flawed in that, while it painted an unpleasant scenario, it failed to offer a legally cognizable constitutional problem. With characteristic cutting wit, he interjected at a later point in the argument, "[w]ell, it must be unconstitutional if it's scary . . . . I mean, what is it, the scary provision of what article?"[372] Yet, for all that, the Justices were uninhibited. Thus, Justice Breyer was unabashed in explaining the stakes: "what would a democratic society look like if a large number of people did think that the government was tracking their every movement over long periods of time?"[373]

Justice Ginsburg articulated, without being able to resolve, the problem of how reasonable expectations of privacy as set forth in current Court doctrine can lead to altogether unreasonable results in the context of current surveillance capabilities:

> But the Fourth Amendment protects us against unreasonable searches and seizures. And if I were to try to explain to someone, here's the Fourth Amendment, the Fourth Amendment says—or it has been interpreted to mean that if I'm on a public bus and the police want to feel my luggage, that's a violation; and yet, this kind of monitoring, installing the GPS and monitoring the person's movement whenever they are outside their house in the car, is not? I mean, it just—there's something about it that—that just doesn't parse.[374]

Several of the Justices, in other words, recognized the *1984* problem in light of *Katz* and *Knotts*, and suggested a modification of doctrine was necessary. The manner in which the Justices discussed this modification suggested that the *Katz* privacy test should lead with the societal inquiry first. Table 1 below shows why leading with the societal cybersurveillance intrusion inquiry before the individual subjective privacy interest would appear to have made more sense to some of the Justices during oral argument.

During the oral argument in *Jones*, several of the Justices suggested that the *Katz* privacy test appears to reach its limit where its reasonable expectations test risks the Court's ratification of an unreasonable state of government overreach.[375] At that juncture, Table 1 attempts to illustrate how an evolution of the *Katz* test occurs where, starting from the societal perspective, a federal court must assess the level of cybersurveillance

372. *Id.* at 37.

373. *Id.* at 24.

374. *Id.* at 23–24.

375. *See generally* Transcript of Oral Argument, United States v. Jones, *supra* note 16.

intrusion it is asked to ratify and interrogate whether it is unreasonable. At that point, the court must unmoor itself from preexisting Fourth Amendment doctrine and, on the facts, hold against the government's cybersurveillance practice.[376]

Table 1 attempts to set forth the four iterations that are possible under the *Katz* privacy test. Box A shows what is required to satisfy the *Katz* privacy test: subjective and objective expectations of privacy must be met. Boxes B, C, and D all demonstrate when the *Katz* privacy test is not satisfied. Box B illustrates that an individual may not enjoy a subjective expectation of privacy; nonetheless, society may assert a societal-wide expectation of privacy. Oppositely, Box C indicates that a person may hold an expectation of privacy, while society may not grant such a right. Finally, Box D demonstrates when neither individuals, subjectively, nor society at large, objectively, can assert a reasonable expectation of privacy under the Fourth Amendment.

Specifically, Table 1 focuses on the distinctions between Box B and Box D. Box B represents the viewpoint of several Justices during oral argument in *Jones*. The cybersurveillance intrusion presented in the facts in *Jones* appeared to lead to a split: some Justices appeared to agree that a subjective expectation of privacy does not exist to protect an individual from being tracked on public thoroughfares; however, an objective expectation of privacy prohibits warrantless GPS tracking. Box D represents the viewpoint of the government during oral argument in *Jones*. The government argued that there was neither a subjective nor objective expectation of privacy because, eventually, warrantless GPS tracking would become normalized.

376. *See generally* Florida v. Riley, 488 U.S. 445, 466–67 (1989).

Table 1:
The Four Iterations of the *Katz* Test

Subjective Expectation of Privacy Exists	**Subjective Expectation of Privacy Does Not Exist**
Objective Expectation of Privacy Exists	
Box A In *Katz v. United States*,[377] Fourth Amendment Violation: (1) *Subjective Inquiry*: Would a reasonable person expect that the information (e.g., data, electronic communication) should be kept from others? Yes. (2) *Objective Inquiry*: Would society ratify that the information should be kept private? Yes.	**Box B** In *United States v. Jones*,[378] several Justices at Oral Argument: (1) *Subjective Inquiry*: Would a reasonable person expect that geolocational data collected on public thoroughfares should be kept from others? No: *See United States v. Knotts*.[379] (2) *Objective Inquiry:* Would society ratify that the information should be kept private? Yes: the Fourth Amendment should protect against warrantless 24/7 GPS tracking based upon a commonly held understanding of protection against unreasonable intrusion.
Objective Expectation of Privacy Does Not Exist	
Box C *United States v. Jacobsen*[380] No Fourth Amendment Violation:	**Box D** Government at Oral Argument in *United States v. Jones*:[381]

377. 389 U.S. 347 (1967).
378. 565 U.S. 400 (2012).
379. 460 U.S. 276 (1983).
380. 466 U.S. 109 (1984).
381. 565 U.S. 400 (2012).

(1) *Subjective Inquiry*: Would a reasonable person expect that the contents of luggage should be kept from others? Yes. (2) *Objective Inquiry*: If a drug-sniffing dog does not search contents and only detects presence of drugs? No: No societal expectation of privacy.	(1) *Subjective Inquiry*: Would a reasonable person expect that geolocational data collected on public thoroughfares should be kept from others? No: *United States v. Knotts*.[382] (2) *Objective Inquiry*: As tracking technologies become more integrated, GPS will become reasonable.[383] Government: No societal expectation of privacy.[384] Justices: Sounds like *1984*.[385]

Table 1 illustrates the government's assertion during the oral argument in *Jones* that, under *Katz* and *Knotts*, the Justices should find that the facts of *Jones* fall into Box D: No Subjective Individual Expectation of Privacy and No Objective Societal Expectation of Privacy. The government contended that Mr. Jones should not be able to argue that he has a subjective expectation of privacy because information gathered on movements traveled over public thoroughfares is not private under *Knotts*.[386] The government also implied that as GPS tracking becomes more normalized, warrantless 24/7 GPS tracking does not offend society.[387] The Justices seemed to respond by saying, "that sounds Orwellian."[388] Yet, the Justices seemed to concede that the facts in *Jones* would preclude it from Box A. Because of *Knotts*, the facts of *Jones* fall into Box B. However, Box B would not lead to a Fourth Amendment violation under the *Katz* privacy test. Therefore, Table 1 explains why the

382. 460 U.S. 276 (1983).

383. *See* Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 57.

384. *See id.*

385. *Id.* at 13.

386. *See* Appellee's Petition for Rehearing En Banc at 15, United States v. Jones, 615 F.3d 544 (D.C. Cir. 2010) (No. 08-3034) (arguing that electronic tracking is merely a substitute for visual surveillance).

387. *Id.*

388. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13 (Justice Breyer: "[s]o, if you win, you suddenly produce what sounds like *1984* from their brief. . . . And so, what protection is there, if any, once we accept your view of the case, from this slight futuristic scenario that's just been painted and is done more so in their briefs?").

Katz test failed in *Jones*. Table 1 further illustrates why the Court appeared to seek a way to resolve *Jones* without resort to the *Katz* test.

In other words, the Court was faced with a conundrum: if the Court's reasonable expectation of privacy jurisprudence is explained to a reasonable person, in this context, warrantless 24/7 surveillance does not appear reasonable. Justice Roberts takes up this point at another juncture in the *Jones* oral argument:

> You can see, though, can't you, that 30 years ago if you asked people does it violate your privacy to be followed by a beeper, the police following you, you might get one answer, while today if you ask people does it violate your right to privacy to know that the police can have a record of every movement you made in the past month, they might see that differently?[389]

Justice Roberts articulated distinctions that do not make a difference under *Knotts*. He is intuitively asserting, however, that the average person on the street would assent to the notion that such a scenario would constitute a Fourth Amendment violation. While the D.C. Circuit's holding rested within the *Knotts* framework, the argument before the Court seemed to proceed in a different direction. The Justices seemed to be wrestling with the notion of whether *Knotts* was itself reasonable in the modern age of cybersurveillance.[390] The argument cuts both ways. One avenue, advanced briefly by the government at oral argument, contended that what is reasonable is subject to change and that as technology such as GPS becomes normalized, expectations of privacy will alter to accommodate them. Put differently, the reasonable expectation of privacy exists in an increasingly diminished sphere as the public itself grows to embrace technologies that effectually turn the private into public. Thus Deputy Solicitor General Michael Dreeben advances this line of defense at oral argument:

> Mr. Chief Justice, advancing technology cuts in two directions. Technological advances can make the police more efficient at what they do through some of the examples that were discussed today: Cameras, airplanes, beepers, GPS. At the same time, technology and how it's used can change our expectations of privacy in the ways that Justice Alito was alluding to. Today perhaps GPS can be portrayed as a *1984*-type invasion, but as people use GPS in their lives and for other purposes, our

389. *Id.* at 22.

390. Katz v. United States, 389 U.S. 347 (1967).

> expectations of privacy surrounding our location may also change. For that —[391]

At that point, however, the Deputy Solicitor General was cut off because the thrust of the argument was clear and unacceptable:

> JUSTICE KAGAN: Dreeben, that—that seems too much to me. I mean, if you think about this, and you think about a little robotic device following you around 24 hours a day anyplace you go that's not your home, reporting in all your movements to the police, to investigative authorities, the notion that we don't have an expectation of privacy in that, the notion that we don't think that our privacy interests would be violated by this robotic device, I'm—I'm not sure how one can say that.[392]

Yet, it is worth noting that Justice Kagan's concerns, once again, do not register a problem under *Knotts*. If the "robotic device" following you around is observing nothing other than what could be observed by a bystander on a public road, then the fact of automation is itself a distinction without a difference under *Knotts*. But Justice Kagan did not attempt to articulate a legal principle here; rather, she rehearsed a set of circumstances that appear intuitively unacceptable—dystopian, anti-democratic, and Orwellian.

Table 2 (below) offers up a new type of test that the Court implied might be needed in light of both (A) shifting government practices in virtual searches and seizures, and search and seizures of identity; and (B) the type of conditioned acquiescence to surveillance that the government suggested was nearly inevitable. The Court's confusion on how to reconcile privacy interests of surveillance in public and private spaces was palpable during oral argument in *Jones*. During oral argument, the Court sought, but did not receive, guidance from the government on whether an alternative to the *Katz* test could be fashioned if warrantless GPS tracking were allowed under the Fourth Amendment.

The oral argument seemed to reveal that the Court was not ready to do more than signal a cybersurveillance nonintrusion test was possible.[393] The *Jones* decision does not adopt a cybersurveillance nonintrusion test. Instead, Justice Scalia's opinion returned to the physical trespass as an alternative to a *Katz* test for physical intrusions.[394] The Court did not outwardly weigh the advantages or disadvantages of an alternative to the

391. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 57.

392. *Id.* at 57–58.

393. *Id.*

394. United States v. Jones, 565 U.S. 400, 404–05 (2012).

Katz privacy test for non-physical intrusions.[395] *Jones* also failed to reach the issue central to the privacy question because it was able to find a narrower violation of the Fourth Amendment on the basis of a physical trespass.[396] Despite the majority's failure to acknowledge the need for a new test in the text of the opinion, the oral argument seemed to reveal that the current structure of the *Katz* privacy test would yield the wrong constitutional outcome. Invocation to *1984* and the Justices' lines of reasoning implied that the society's objective expectation of privacy should trump the individual's subjective expectation of privacy in the particular facts before the Court in *Jones*.

Table 2 describes how certain Justices of the Court implied a cybersurveillance nonintrusion test may be more appropriate than the *Katz* test during oral argument in *Jones.*

Table 2:
***Katz* Privacy Test v. Cybersurveillance Nonintrusion Test Implied by *Jones*'s Oral Argument**

Privacy Test	**Cybersurveillance Nonintrusion Test**
Box A In *Katz v. United States*,[397] Fourth Amendment Violation: (1) *Subjective Inquiry*: Would a reasonable person expect that the information (e.g., data, electronic communication) should be kept from others? Yes. (2) *Objective Inquiry*: Would society ratify that the information should be kept private? Yes.	**Box B** In *United States v. Jones*,[398] Potential New Test Implied by Concurrences and at Oral Argument: (1) *Objective Inquiry*: Would society expect that the government intrusion was unreasonable (or construed government action to be a search and seizure) under commonly held understandings of the Fourth Amendment (based upon culturally ingrained expectations or privacy customs of society)? Yes. (2) *Subjective Inquiry*: Would a reasonable person have considered the government intrusion to be a search and seizure, and unexpected and unjustified? Yes.

395. *Id.*

396. *Id.*

397. 389 U.S. 347 (1967).

398. 565 U.S. 400 (2012).

In other words, the Court implied that the *Katz* subjective-objective test could effectively be flipped to become an objective-subjective test. Rather than leading with the inquiry of whether an individual may subjectively enjoy a reasonable expectation of privacy and then proceeding to an objective analysis of whether society would ratify that viewpoint, the Court seemed to imply at oral argument that the more important inquiry was to consider society's viewpoint at large first. As such, it is this author's belief that a more promising approach would be to begin with a baseline societal standard—a commonly understood version of Fourth Amendment protections—from a societal point of view, which could be drawn from customary law traditions. Customary international law, for example, provides a basis for understanding human rights traditions and can be translated into human rights laws, conventions, and treaties.[399]

C. A Cybersurveillance Nonintrusion Test Under the Fourth Amendment

To address the growing challenges of cybersurveillance technologies, and the harms emanating from the protocols and programs of bureaucratized cybersurveillance, a new cybersurveillance nonintrusion test rather than a privacy test could be implemented. A cybersurveillance nonintrusion test would start with a consideration of privacy customs and the norms and values of democratic society. The secondary inquiry would be whether a subjective expectation of protection from government intrusion is reasonable. The subjective inquiry would not focus on an individualized privacy expectation, but rather on the question of whether or not an intrusion has occurred. Unlike the *Katz* test, the burden on the cybersurveillance nonintrusion test would be on the government to justify whether the surveillance technique is reasonable in light of the values of a democratic society.[400] Requiring the government to justify its surveillance is consistent with the arguments raised by Justice Harlan in *White* and Justice Brennan in *Riley*.[401]

---

399. *See, e.g.*, Bradley & Gulati, *supra* note 20, at 209:

> Treaties also address numerous issues that were not historically regulated (at least extensively) by international law, including environmental conservation, the protection of human rights, and the prosecution of international crimes. Customary International Law nevertheless continues to play an important role in international law and adjudication, regulating both within the gaps of treaties as well as the conduct of nonparties to the treaties.

Id.

400. United States v. White, 401 U.S. 745, 793 (1971) (Harlan, J., dissenting).

401. *See supra* notes 279–298 and accompanying text.

Furthermore, a cybersurveillance nonintrusion test would offer a more flexible and suitable method to evaluate whether a government action involving cybersurveillance violated the spirit of the Fourth Amendment, in addition to the letter. Such a test would shift the calculation away from what level of privacy is reasonable or whether certain types of information should be kept from others under the perspective of a hypothetical reasonable person. This move is critical given the nature of modern big-data technologies, which necessitate the sharing of private information with a wide range of third parties.[402] Once the calculation is shifted away from the axis of privacy, the courts would be empowered to develop a new conceptualization of the Fourth Amendment that rotates around intrusion as a legal concept. As we move toward ever-diminishing degrees of personal privacy as a result of a confluence of technologically and geo-political factors, a new axis of cybersurveillance nonintrusion as the lynchpin for protecting Fourth Amendment rights should prove fruitful in securing society's and citizens' constitutionally protected privacy interests.

Justice Sotomayor's concurrence from *Jones* hinted at this need to shift from privacy to cybersurveillance nonintrusion, and to lead with an inquiry that first addresses broad-based societal concerns and interests, rather than individual rights concerns, in contemplating the potential Fourth Amendment harms at play within the realm of cybersurveillance:

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity . . . may "alter the relationship between citizen and government in a way that is inimical to democratic society."[403]

This cybersurveillance nonintrusion test suggested by the concurring opinions in *Jones* appears preferable to the mosaic theory as we enter more completely into the realm of big data cybersurveillance.

Despite this precedent, the concurring justices in *Jones*, however, did not expressly adopt the mosaic theory reasoning of the D.C. Circuit. In fact, the broad brushstrokes of their concurrences instead suggest that a preference for a new direction is potentially forthcoming. Justice Alito and the three additional Justices who joined him (Justice Breyer, Justice Ginsburg, and Justice Kagan), as well as Justice Sotomayor in a separate concurrence, all appeared to signal their beliefs that a shift in doctrine might be needed in light of increasingly comprehensive and invasive cybersurveillance technologies. This seems to indicate that a majority of

402. United States v. Jones, 565 U.S. 400, 417 (Sotomayor, J., concurring).

403. *Id.* at 416 (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011)).

the justices are clearly open to a new Fourth Amendment approach in the face of rapidly evolving surveillance technologies.

Table 3 explains the differences between a cybersurveillance nonintrusion test and the *Katz* privacy test, and why a cybersurveillance nonintrusion test that is grounded in customary law is now more appropriate in light of the new and unprecedented challenges posed by big data cybersurveillance, including the metaphysical harms of cybersurveillance and the threat of "precrime."

Table 3: The Distinctions Between the *Katz* Test and a Cybersurveillance Nonintrusion Test[404]

Cybersurveillance Nonintrusion Test	***Katz* Privacy Test**
When the tests are used	
Under Fourth Amendment (Pertaining to Emerging Mass Surveillance and Cybersurveillance Methods)[405]	Under Fourth Amendment[406]
Government Action in Question: Unreasonable Search and Seizure of Digitally Constructed Identity and Personally Identifiable Digital Data?[407]	Government Action in Question: Unreasonable Search and Seizure of Person and Property? [408]

404. This chart originally appeared in the *American Criminal Law Review*. *See* Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, *supra* note 36.

405. *See* United States v. Jones, 565 U.S. 400 (2012).

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

407. *Jones*, 565 U.S. at 402.

408. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

Paradigmatic Case: Mass analytics and predictive analytics to anticipate guilt or predict future wrongdoing; "Precrime:" Government searching and seizing personally identifiable data of mass populations or subpopulations and locating suspects based on data searches; and determine one's probabilistic likelihood or statistical predisposition to commit crime or terrorism[409]	Paradigmatic Case: Government searching and seizing contents of one's diary or letters[410]
Unlikely to be used by police (unless, for example, a traffic stop was generated by an algorithm)	Commonly used by police
Expectations under the tests	
Expectation of Cybersurveillance Nonintrusion under Fourth Amendment: Reasonable Expectation to be Free of Unreasonable Cybersurveillance and Government Intrusion[411]	Expectation of Privacy under Fourth Amendment: Reasonable Expectation of Privacy and Expectation to be Free of Unreasonable Government Searches and Seizures of Physical Person and Physical Possessions[412]
No Third Party Doctrine: Expectation of cybersurveillance nonintrusion does not pivot on whether information was shared with others[413]	Third Party Doctrine: No expectation of privacy if information shared with third party[414]

409. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (presenting prima facie challenges to a provision of the Foreign Intelligence Surveillance Amendments Act of 2008, which empowers the FISA Court to authorize surveillance without a showing of probable cause that the target of surveillance is an agent of a foreign power).

410. *Katz*, 389 U.S. at 365.

411. *Jones*, 565 U.S. at 410–12.

412. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

413. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (questioning the applicability of the Third Party doctrine to modern technology and Fourth Amendment analysis).

414. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 742 (1979) (articulating the Third Party Doctrine).

Grounded in the positive right perspective (or hybrid) of the Fourth Amendment: "The Right of the People to be Secure in their Persons, Papers, and Effects"[415]	Grounded in the negative right perspective of the Fourth Amendment: Free from Unreasonable Searches and Seizures[416]
Focus of judicial inquiry under the tests	
Objective inquiry is leading question: Objectively, does society have a reasonable expectation to be protected from government intrusion (e.g., big data cybersurveillance) in this particular instance?[417]	Subjective inquiry is currently the leading question in *Katz* privacy test: Subjectively, does the individual have a reasonable expectation of privacy (e.g., expected personal information would be kept private) in this particular instance?[418]
Vantage Point of Inquiry: Societal Interest in Open Democratic Society (e.g., to be free from "*1984*"-type surveillance)[419]	Vantage Point of Inquiry: Personal Interest in Maintaining Information Private[420]

415. *See, e.g.*, U.S. CONST. amend. IV; Bivens v. Six Unknown Named Agents, 403 U.S. 388, 392 (1971) ("It guarantees to citizens of the United States the absolute right to be free from unreasonable searches and seizures . . . ."); Erwin Chemerinsky, *Making the Right Case for a Constitutional Right to Minimum Entitlements*, 44 MERCER L. REV. 525, 534 (1993) (noting that the Constitution creates affirmative duties); Gray, *Dangerous Dicta*, *supra* note 5, at 1181 (quoting the Fourth Amendment protections); Gray, *A Collective Right*, *supra* note 41 (arguing that the Fourth Amendment unambiguously refers to collective rights).

416. *See, e.g.*, U.S. CONST. amend. IV; Dist. of Columbia v. Heller, 554 U.S. 570, 646 (2008) ("[T]he Fourth Amendment describes a right *against* governmental interference rather than an affirmative right *to* engage in protected conduct . . . ."); *Katz*, 389 U.S. 347; Tracey Maclin, *Justice Thurgood Marshall: Taking the Fourth Amendment Seriously*, 77 CORNELL L. REV. 723, 772 (1992) ("Thus, Fourth Amendment rights are seldom considered positive rights. Rather, the Court generally views them as restraints on law enforcement to be acknowledged, but not taken seriously.").

417. *See* United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring).

418. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

419. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13, 25, 27, 33, 35, 57 (referring to George Orwell's *1984*).

420. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

Government Must First Demonstrate Mass Surveillance or Cybersurveillance Method is Necessary and Efficacious (e.g., Fourth Amendment Special Needs Doctrine or Special Needs Exception to Fourth Amendment Applies)[421]	Individual Must First Demonstrate Individual-Based Subjective Privacy Interest is Protected Under Fourth Amendment[422] and provide evidence of unreliability[423]
Need for the tests	
Big Data Cybersurveillance: Era of digital-based and database-driven information	Small Data Surveillance: Era of analog-based information
Intangible Harms: Realm of virtual reality, virtual cybersurveillance, and artificial intelligence and/or algorithmic intelligence	Tangible Harms: Physical or property-based harms, realm of traditional notion of reality and human intelligence and sensory-based surveillance
Protection from Big Data Inferences of Guilt or Suspicion from Correlative Data-Driven Evidence and Statistical Algorithms (e.g., Protection from "Guilty Until Proven Innocent" Status)[424]	Protection from Unwanted Revelatory Information; Physical Trespass; and Reputational or Privacy Tort Harms[425]

421. *See* United States v. Jones, 565 U.S. 400 (2012); United States v. White, 401 U.S. 745, 792–93 (1971) (Harlan, J., dissenting) ("[T]he burden of guarding privacy in a free society should not be on its citizens; it is the Government that must justify its need to electronically eavesdrop.").

422. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

423. *See, e.g.*, United States v. Esquivel-Rios, 725 F.3d 1231, 1239 (10th Cir. 2013) (contending that the interaction between the reasonable suspicion standard and the use of law enforcement databases that are imperfect and prevalent should get the full vetting it deserves so the court can confidently render a decision); United States v. Cortez-Galaviz, 495 F.3d 1203, 1209 (10th Cir. 2007) (questioning the validity of database information).

424. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013) (presenting prima facie challenges to a provision of the Foreign Intelligence Surveillance Amendments Act of 2008 that permitted FISC to authorize surveillance of a target without a showing of probable cause).

425. *Katz*, 389 U.S. at 352–53.

Where the tests originated	
Concurrences and oral argument in *Jones*: Suggestion that societal-based rights may now center the normative commitment of the Fourth Amendment[426]	Before *Jones*: Conceptualization that individual-based rights center the normative commitment of the Fourth Amendment[427]
Constitutional implications of mass cybersurveillance and warrantless, suspicionless tracking play out on public, society-wide level[428]	Constitutional implications of warrantless tracking or suspicionless surveillance of individual suspect unfold on personal, individual-rights level[429]
Grounded in Customary Law[430]	Grounded in Property Law and Tort Law[431]
Future direction of the tests	
Cybersurveillance nonintrusion appears to be transforming into the potential new axis for doctrinal analysis under Fourth Amendment inquiry after *Jones*[432]	Privacy is current axis for doctrinal analysis under Fourth Amendment inquiry after *Katz*[433]

CONCLUSION

The Court has signaled an understanding that the Fourth Amendment doctrine must now evolve to accommodate limitations on government intrusiveness in light of increasingly comprehensive and invasive

426. Transcript of Oral Argument, United States v. Jones, *supra* note 16, at 13, 25, 27, 33, 35, 57 (discussing George Orwell's *1984* in relation to broad surveillance).

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

428. *See, e.g.*, Balkin, *supra* note 209; Balkin & Levinson, *supra* note 209; *see also supra* notes 216–29 and accompanying text; *supra* Part II.

429. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

430. *See, e.g.*, *supra* notes 14, 19–27, 322.

431. *See, e.g.*, *supra* notes 36–37, 244–45 and accompanying text.

432. United States v. Jones, 565 U.S. 400, 418–20 (2012) (Alito, J., concurring) (citation omitted).

433. *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

cybersurveillance technologies. The Court has implied that this evolution is appropriate and necessary to impose meaningful limitations on the depth and scope of the potential government intrusion. With the emergence of big data cybersurveillance and the search and seizure of digitally constructed identity, a different Fourth Amendment framework is required. The *Katz* privacy test must be abandoned because the underlying fundamental principles of the Fourth Amendment are at risk of being undermined by it. In the coming years, the government will likely continue to expand big data cybersurveillance programs under the justification of immigration and crime control objectives, as well as counterterrorism policies. Thus, the need for a revision of the doctrine is urgent. This new type of constitutional harm is facilitated by an axial age of technology that has put the tools of big data, data surveillance or dataveillance, and cybersurveillance at the disposal of the government.

The *Jones* Court held that GPS tracking devices are subject to the tort doctrine of trespass and may not be surreptitiously placed on a person's effects without his or her consent, at least without a warrant. Thus, the Court's holding in *Jones* has only temporarily avoided the thornier question of whether the Court's "reasonable expectation of privacy" doctrine under *Katz* will impose any meaningful restraints on the government's growing virtual cybersurveillance and dataveillance capacities. In short, *Jones* made clear that Fourth Amendment jurisprudence has not yet developed a limiting principle to curtail the effects of rapidly advancing technology in the realm of cybersurveillance and dataveillance. During oral argument and in the concurrences filed by Justice Alito and Justice Sotomayor, the Court signaled the potential to shift the inquiry away from emphasizing a privacy interest to recognizing a right against unreasonable government intrusion. The anti-surveillance norms of democratic society were on full display through references to *1984* during the oral argument of *Jones.* In essence, a close observation of the line of reasoning at oral argument and in the concurring opinions in *Jones* reveals that the societal interest should be predominant as a first line of inquiry.

The Court's invocation to *1984* during oral argument in *Jones* reflects that these limitations are culturally ingrained and, therefore, must be part of an assessment of whether the surveillance is considered objectively or subjectively reasonable. The Court has suggested that an inquiry that pivots around a concept of cybersurveillance nonintrusion rather than privacy might be more appropriate in the digital age. The cybersurveillance nonintrusion test implicitly suggested by the Court first shifts the vantage point of the Fourth Amendment analysis from an individual-based tangible harm inquiry to an inquiry of a society-wide

intangible harm. Next, the cybersurveillance nonintrusion test shifts the burden from an individual citizen to the government. Under the current privacy test, an individual must first establish a subjective reasonable expectation of privacy. The cybersurveillance nonintrusion test instead requires the government to justify the intrusion of the surveillance on society. The Supreme Court and post-Snowden federal courts appear to be using the Orwellian trope both to establish the society-wide intangible harm: *1984*-type scenarios that violate established privacy customs in a democratic society; and to engage the cybersurveillance nonintrusion test to ask the government to overcome the *1984* problem presented by contemporary surveillance methods.

The oral argument during *Jones* signaled an emerging cybersurveillance nonintrusion test under the Fourth Amendment. This Article concludes that such a test could be grounded in customary law, and could replace the Fourth Amendment privacy test currently grounded in property and tort law. To preserve the integrity of the Fourth Amendment and the normative values it was intended to protect, a dramatic revision of the Fourth Amendment doctrine, including the adoption of a cybersurveillance nonintrusion test and the abandonment of the current Fourth Amendment privacy test, is now required.