2018

Cybersurveillance Intrusions and an Evolving *Katz* Privacy Test

Margaret Hu
Washington and Lee University School of Law, hum@wlu.edu

CYBERSURVEILLANCE INTRUSIONS AND AN EVOLVING *KATZ* PRIVACY TEST

Margaret Hu*

INTRODUCTION

Cybersurveilllance intrusions necessitate a different Fourth Amendment test than the privacy test set forth by the Supreme Court in *Katz v. United States*[1] 50 years ago. As part of the Symposium, Katz *at 50: The Fourth Amendment in the Digital Age*, this Article aims to illustrate why the transformation of Fourth Amendment doctrine is not only necessary with the increasing adoption of cybersurveillance technologies, but has already begun.[2] Courts are increasingly confronted with the constitutional implications of mass surveillance made possible by big data governance.[3] For example, suspicionless mass data collection, predic-

---

* Associate Professor of Law, Washington and Lee University School of Law. I would like to extend my deep gratitude to those who graciously offered comments on this draft, or who offered perspectives and expertise on this research through our thoughtful discussions: Alvaro Bedoya, Andrew Christensen, Jennifer Daskal, Laura Donohue, Josh Fairfield, David Gray, Stephen Henderson, Rachel Levinson-Waldman, Erik Luna, Tim MacDonnell, Russ Miller, Steve Miskinis, Paul Ohm, Christopher Slobogin, and apologies to anyone whom I might have omitted. In addition, this research benefited greatly from the discussions generated from the *American Criminal Law Review* 2017 Symposium: Katz *at 50: The Fourth Amendment in the Digital Age*. Many thanks to the research assistance of Alexandra Klein, Kirby Kreider, and Bo Mahr. All errors and omissions are my own. This work is a companion piece to Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test,* 92 WASH. L. REV. 1819 (2018).

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

2. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014); United States v. Jones, 565 U.S. 400 (2012); Susan W. Brenner, *The Fourth Amendment in an Era of Ubiquitous Technology*, 75 MISS. L.J. 1 (2005); Laura K. Donohue, *The Original Fourth Amendment*, 83 U. CHI. L. REV. 1181 (2016); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805 (2016); Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547 (2017); David Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. 1181 (2015); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); Adam Gershowitz, *The Post-*Riley *Search Warrant*, 69 VAND. L. REV. 585 (2016); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012); Orin S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISS. L.J. 85 (2005); Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?*, 2011–2012 CATO SUP. CT. REV. 15 (2011); Rachel Levinson-Waldman, *Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public*, 66 EMORY L.J. 527 (2017); Christopher Slobogin, *The World Without a Fourth Amendment*, 38 UCLA L. REV. 1 (1991); Christopher Slobogin, *Peeping Techno-Toms and the Fourth Amendment: Seeing Through* Kyllo*'s Rules Governing Technological Surveillance*, 86 MINN. L. REV. 1393 (2002); Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511 (2010); *see infra* Part III.

3. *See, e.g.*, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated*, Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015); Klayman v. Obama, 142 F. Supp. 3d 172 (D.D.C. 2015); *see also* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014); Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015); Margaret Hu, *Small Data Cybersurveillance v. Big Data Cybersurveillance*, 42 PEPP. L. REV.

tive analysis, and *ex ante* policing all present emerging and unresolved constitutional issues.[4]

To contextualize why a new approach to the Fourth Amendment is essential, this Article describes two emerging cybersurveillance tools. The first cybersurveillance tool, Geofeedia,[5] has been deployed by state and local law enforcement.[6] Geofeedia uses a process known as "geofencing" to draw a virtual barrier around a particular geographic region, and then identifies and tracks public social media posts within that region for predictive policing purposes.[7] The second tool, Future

---

773 (2015); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013); Stephen Rushin, *The Judicial Response to Mass Police Surveillance*, 2011 U. ILL. J.L. TECH. & POL'Y 281 [hereinafter Rushin, *The Judicial Response*]; Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008); Orin S. Kerr, *Foreword: The Future of Internet Surveillance Law*, 72 GEO. WASH. L. REV. 1139 (2004).

4. *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 10–11 (2008) ("Governance in the National Surveillance State is increasingly statistically oriented, *ex ante* and preventative, rather than focused on deterrence and *ex post* prosecution of individual wrongdoing."); Jack M. Balkin & Sanford Levinson, *The Processes of Constitutional Change: From Partisan Entrenchment to the National Surveillance State*, 75 FORDHAM L. REV. 489 (2006). "Like preventive measures, policing measures can be either ex ante or ex post, according to whether they function before—or only after—the wrong occurs." Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687, 706 (1997). Ex ante policing has been defined as a "form of continuous monitoring . . . [that] can deter misconduct by increasing the likelihood that it will be detected and sanctioned." *Id.* Although this definition refers to the corporate context, the principles remain the same regarding criminal policing applications. *See, e.g.*, David Cole, *The Difference Prevention Makes: Regulating Preventive Justice*, 9 CRIM. L. & PHIL. 501 (2015); Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014); *see also* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN. L. REV. 407 (2012); Laura K. Donohue, *The Dawn of Social Intelligence (SOCINT)*, 63 DRAKE L. REV. 1061 (2015); Collins T. Fitzpatrick, *Protecting the Fourth Amendment So We Do Not Sacrifice Freedom for Security*, 2015 WIS. L. REV. 1; David Gray, *A Collective Right to Be Secure from Unreasonable Tracking*, 48 TEX. TECH. L. REV. 189 (2015) [hereinafter Gray, *A Collective Right*]; Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633 (2017); Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray & Stephen E. Henderson eds., 2017); Paul Ohm, *Electronic Surveillance Law and the Intra-Agency Separation of Powers*, 47 U.S.F. L. REV. 269 (2012); Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91 (2016); Nadine Strossen, *Beyond the Fourth Amendment: Additional Constitutional Guarantees that Mass Surveillance Violates*, 63 DRAKE L. REV. 1143 (2015); Russell L. Weaver, *The Fourth Amendment and Technologically Based Surveillance*, 48 TEX. TECH. L. REV. 231 (2015).

5. *See* GEOFEEDIA, https://geofeedia.com/ (last visited Nov. 6, 2017).

6. *See, e.g.*, Jonah Engel Bromwich, Daniel Victor & Mike Isaac, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html?_r=0; Craig Timberg & Elizabeth Dwoskin, *Facebook, Twitter and Instagram Sent Feeds that Helped Police Track Minorities in Ferguson and Baltimore, Report Says*, WASH. POST (Oct. 11, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/10/11/facebook-twitter-and-instagram-sent-feeds-that-helped-police-track-minorities-in-ferguson-and-baltimore-aclu-says/?utm_term=.c74a5bc5eb08; Matthew Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU (Oct. 11, 2016, 11:15 AM), https://www.aclu.org/blog/free-future/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed; Nicole Ozer, *Police Use of Social Media Surveillance Software is Escalating, and Activists are in the Digital Crosshairs*, ACLU (Sep. 22, 2016, 2:45 PM), https://www.aclu.org/blog/free-future/police-use-social-media-surveillance-software-escalating-and-activists-are-digital; *infra* notes 42–58.

7. *See infra* notes 44–45 and accompanying text.

Attribute Screening Technology (FAST), is under development by the United States Department of Homeland Security (DHS).[8] FAST is another predictive policing tool that analyzes physiological and behavioral signals with the goal of identifying "malintent": an individual's predilection for disruptive or violent behavior.[9] Both Geofeedia and FAST seem to fall outside the scope of protections afforded by existing Fourth Amendment jurisprudence.[10]

Under the Fourth Amendment, unreasonable searches and seizures are prohibited—but reasonable searches may be permissible. For 50 years, *Katz v. United States*[11] has defined the federal courts' approach to evaluating what is a "reasonable" law enforcement action under the Fourth Amendment. The *Katz* test assesses whether law enforcement has violated an individual's "constitutionally protected reasonable expectation of privacy."[12] This test is traditionally used to determine whether a search has occurred within the meaning of the Fourth Amendment.[13] *Katz* focuses on whether an individual intended to keep information private[14] and whether information had been previously disclosed.[15] Technological developments, however, may change which expectations of privacy are "reasonable," calling the continued viability of the *Katz* "reasonable expectation of privacy" test into question.[16]

Thus far, the Supreme Court has begun to discern implications of big data governance structures and policies. In the 2012 case of *United States v. Jones*,[17] the Court considered the constitutionality of warrantless GPS tracking.[18] During oral argument, several Justices signaled a concern that GPS geolocational data collection could extend beyond one GPS device attached to a single vehicle in the course

---

8. *See* Sharon Weinberger, *Intent to Deceive?*, 465 NATURE 412, 414–15 (2010); *infra* notes 61–77 and accompanying text.

9. *See infra* notes 65–69 and accompanying text.

10. *See* U.S. CONST. amend. IV.

> 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.

11. 389 U.S. 347 (1967).

12. *Id.* at 360 (Harlan, J., concurring).

13. *See* United States v. Jones, 565 U.S. 400, 406 (2012) ("Our later cases have applied the analysis of Justice Harlan's concurrence in [*Katz*], which said that a violation occurs when government officers violate a person's 'reasonable expectation of privacy.'"); United States v. Jacobsen, 466 U.S. 109, 120 (1984) (explaining that law enforcement action that does not infringe on a "legitimate expectation of privacy . . . [is] not a 'search' within the meaning of the Fourth Amendment."); *see also* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

14. *See, e.g.*, *Katz*, 389 U.S. at 361 ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited.").

15. *See, e.g.*, *Smith*, 442 U.S. at 742; United States v. Miller, 425 U.S. 435, 440–41 (1976).

16. *See, e.g.*, *Jones*, 565 U.S. at 427 (Alito, J., concurring); *see also supra* notes 2–4.

17. *Jones*, 565 U.S. 400.

18. *Id.* at 402.

of a small data investigation.[19] Specifically, members of the Court expressed concern that GPS devices could be attached to all vehicles,[20] and speculated, for example, Departments of Motor Vehicles could include GPS devices on license plates.[21] The Court discussed the potential for universal GPS tracking of every vehicle to be mandated under state or federal law[22] or standardized in vehicle manufacturing.[23]

The government attempted to assuage the Court's concern over the specter of mass surveillance by pointing out that "[t]his case does not involve universal surveillance of every member of this Court or every member of the society. It involves limited surveillance of somebody who was suspected of drug activity."[24] Ultimately, the Court refrained from engaging in a full analysis of whether *Katz*'s reasonable expectation of privacy was applicable in a warrantless GPS tracking context. Instead, it resorted to an approach to the Fourth Amendment analysis that relied on trespass theory, which, as the Court explained, is an alternative to *Katz*.[25] Taking a narrow approach, the Court held that "the Government's installation of a GPS device on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a [Fourth Amendment] 'search.'"[26]

Similarly, in the 2014 case of *Riley v. California*,[27] the Court considered whether a warrantless search of a cell phone incident to arrest violates the Fourth Amendment.[28] During oral argument, the Court grappled with the difference between a search of a cell phone and a search of an individual's other effects in a search incident to arrest.[29] Digital data, as the Court pointed out, is different because "a person can only carry so much on their person . . . [but] with digital cameras people take endless photos and it spans their entire life."[30] The Court also noted the potential for abuse if it approved a warrantless search of a phone incident to arrest, positing that a person could be arrested for a minor traffic infraction, and

---

19. Transcript of Oral Argument at 29–30, 36, 46, 57–58, *Jones*, 565 U.S. 400 (No. 10-1259).

20. Justice Kagan asked about the constitutionality of a future in which "all cars are going to have GPS tracking systems, and the police could essentially hack into such a system without committing the trespass." *Id.* at 46.

21. Chief Justice Roberts noted that because license plates are state property, the possibility existed that the state could put a GPS device "the size of a credit card . . . behind the license plate" on any individual's vehicle. *Id.* at 29–30.

22. *Id.* at 46. Stephen Leckar, the attorney for Jones, pointedly explained that if GPS systems were installed in all vehicles, "that's because of manufacturers doing it, or because Congress has legislated it . . . ." *Id.*

23. *Id.*

24. *Id.* at 58.

25. United States v. Jones, 565 U.S. 400, 411 (2012) ("For unlike the concurrence, which would make *Katz* the *exclusive* test, we do not make trespass the exclusive test. Situations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis.").

26. *Id.* at 404.

27. 134 S. Ct. 2473 (2014).

28. *Id.* at 2480.

29. Transcript of Oral Argument at 8–11, 27–29, *Riley*, 134 S. Ct. 2473 (No. 13-132).

30. *Id.* at 28.

then officers could search the individual's phone to learn virtually every detail of the arrestee's life.[31] In a unanimous opinion, Chief Justice Roberts refused to extend search incident to arrest precedent to cell phones, holding that a warrant is required before a search of an arrestee's cell phone.[32] Despite being hailed as victories for privacy advocates,[33] neither *Jones* nor *Riley* identify a limiting principle for government intrusion through comprehensive dataveillance and cybersurveillance means.[34]

The Court, however, was not blind to the need for a dramatic revision of Fourth Amendment protections. During oral argument in *Jones*, and in concurrences by Justices Alito and Sotomayor, the Court suggested that a nonintrusion test may be more appropriate given the scope of developing technology. A nonintrusion test is grounded in customary law, replacing an interpretation of the Fourth Amendment that is currently grounded in property and tort law, and presents a way to untether concepts of privacy from nondisclosure.[35]

This Article proceeds in three parts. Part I explores how precrime rationales justify preventive policing through big data cybersurveillance systems. This

---

31. Justice Kagan stated:

> And the police could take that phone and could look at every single e-mail that person has written, including work e-mails, including e-mails to family members, very intimate communications, could look at all that person's bank records, could look at all that person's medical data, could look at that person's calendar, could look at that person's GPS and find out every place that person had been recently because that person was arrested for driving without a seat belt.

Id. at 29–30.

32. *Riley*, 134 S. Ct. at 2485.

33. *See, e.g.*, Andy Greenberg, *Why the Supreme Court May Finally Protect Your Privacy in the Cloud*, WIRED (June 26, 2014), https://www.wired.com/2014/06/why-the-supreme-court-may-finally-protect-your-privacy-in-the-cloud/; Adam Liptak, *Major Ruling Shields Privacy of Cellphones*, N.Y. TIMES (June 25, 2014), https://www.nytimes.com/2014/06/26/us/supreme-court-cellphones-search-privacy.html?_r=0; Ateqah Khaki, *Supreme Court Rules Government Violated Privacy Rights in GPS Tracking Case*, ACLU (Jan. 23, 2012, 12:29 PM), https://www.aclu.org/blog/supreme-court-rules-government-violated-privacy-rights-gps-tracking-case; US v. Jones, ELEC. FRONTIER FOUND., https://www.eff.org/cases/us-v-jones (last visited June 14, 2017).

34. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2493 (2014) (explaining the Court's holding, which required a warrant before a search of a cell phone incident to arrest); United States v. Jones, 565 U.S. 400, 412 (2012) (explaining that "the present case does not require [the Court] to answer [the] question" of whether constant electronic surveillance "without an accompanying trespass" is an "unconstitutional invasion of privacy"). Multiple scholars have explored in depth the constitutional implications of mass surveillance and cybersurveillance technologies. *See, e.g.*, SIMON CHESTERMAN, ONE NATION UNDER SURVEILLANCE (2011); DAVID COLE & JULES LOBEL, LESS SAFE, LESS FREE (2007); DAVID COLE & JAMES X. DEMPSEY, TERRORISM AND THE CONSTITUTION (2002); CONSTITUTION 3.0: FREEDOM AND TECHNOLOGICAL CHANGE (Jeffrey Rosen & Benjamin Wittes eds., 2011); JON L. MILLS, PRIVACY: THE LOST RIGHT (2008); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476 (2011).

35. In a sister article, the discussion focuses more intensely on the origins of the *Katz* test and how current Fourth Amendment jurisprudence has fared in the face of Fourth Amendment challenges to modern cybersurveillance. *See* Margaret Hu, *Orwell's* 1984 *and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819 (2018). In this Article, the discussion focuses more on the cybyersurveillance techniques. The goal is to discuss how representative cybersurveillance technologies function, and why they appear to circumvent the protections offered by *Katz* and its progeny.

discussion helps to lay a foundation for why a nonintrusion test provides a method to address Fourth Amendment concerns in the context of large-scale suspicionless data surveillance and seizures. Part II discusses why suspicionless data screening programs fall outside Fourth Amendment protections against unreasonable searches and seizures under *Katz*. *Katz*'s reasonable expectation of privacy test may not protect the data relied upon by contemporary cybersurveillance programs. Nonetheless, these programs implicate Fourth Amendment concerns, as well as other constitutional rights. Part III argues that a nonintrusion test is more appropriate in these arenas than is *Katz* because of the nature of big data technology, cybersurveillance, and bulk data collection practices. This Article concludes by arguing that, due to rapid technological changes, the evolution of the Fourth Amendment is now necessary, and the adoption of a non-intrusion test may provide greater protections to constitutional freedoms than the *Katz* privacy test.

I. BIG DATA CYBERSURVEILLANCE AS PRECRIME

Jones, *Riley*, and other recent Fourth Amendment cases illuminate the limitations of the *Katz* privacy test in the face of developing big data law enforcement capabilities. Historically, under *Katz*, courts have analyzed Fourth Amendment challenges by considering targeted law enforcement action, rather than suspicionless mass data tracking programs that encompass all individuals, and investigate their data for indicia of suspicion.[36] Automated and semi-automated data search and seizure cases often appear in administrative and bureaucratized circumstances different from typical law enforcement actions involving investigation of specific individuals.[37]

For instance, the use of biometric databases and mass suspicionless surveillance tools has become increasingly common by state and local law enforcement. Geofeedia and other similar technologies demonstrate law enforcement's transition from small data policing to big data cybersurveillance.[38] The spread of suspicionless surveillance tools to law enforcement forecasts the future of modern policing[39] and highlights the growing gaps in existing Fourth Amendment doctrine. Government tools like FAST are embedded in the Administrative State and are not typically seen as law enforcement tools, despite serving precrime governance ambitions. While FAST is still being tested by the Department of Homeland

---

36. *See* Christopher Slobogin, *Policing as Administration*, 165 U. PA. L. REV. 91, 93–94 (2016) (explaining that panvasive investigative techniques may not be considered searches and seizures and listing numerous techniques that the Supreme Court has upheld against Fourth Amendment challenges).

37. *See id.* at 96 ("Because . . . panvasive searches and seizures are policy-driven, group-based, and suspicionless, they are legislative in nature.").

38. For a discussion of some of these tools, *see* Margaret Hu, *Biometric Surveillance and Big Data Governance*, *in* THE CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW (David Gray & Stephen E. Henderson eds., 2017).

39. For a discussion of law enforcement use of mass surveillance tools, *see* Rushin, *The Judicial Response*, *supra* note 3; Stephen Rushin, *The Legislative Response to Mass Police Surveillance*, 79 BROOK. L. REV. 1 (2013).

Security, the No-Fly List, compiled by the Federal Bureau of Investigation's (FBI) Terrorist Screening Center (TSC), is already in effect.[40] The No-Fly List can fairly be described as a precrime program because it is intended to prevent "individuals [who] are known or suspected terrorists," from boarding planes.[41] Although predictive mass surveillance systems have yet to be prominently deployed, Geofeedia and FAST are representative technologies that signal it is likely that the use of such precrime technology will spread.

A. Geofeedia and Social Media Surveillance

Geofeedia, a social media surveillance software, combines social media posts and geographic data into one platform.[42] The software aggregates data from social media sites such as Facebook, Twitter, YouTube, Instagram, and Periscope. At the time it was revealed by media reports and civil rights organizations, Geofeedia collected posts, identified them by username and other tags, and filtered them into locational groups.[43] Geofeedia uses a process known as "geofencing." Geofencing builds a "virtual fence" around a designated physical location[44] and permits social media posts from that defined area to be identified and stored.[45] Although social media surveillance software companies like Geofeedia claim to be little more than "aggregator[s] of public information,"[46] media reports based on access to police records claim that Geofeedia attempted to access private social media posts rather than only the information users posted publicly.[47]

Geofeedia was initially funded by In-Q-Tel, a venture capital firm sponsored by the CIA.[48] Geofeedia had provided its services and technology to numerous police

---

40. *See* Latif v. Holder, 28 F. Supp. 3d 1134, 1141 (D. Or. 2014).

41. *Id.* ("TSC defines its reasonable-suspicion standard as requiring 'articulable facts which, taken together with rational inferences, reasonably warrant the determination that an individual is known or suspected to be, or has been engaged in conduct constituting, in preparation for, in aid of or related to, terrorism or terrorist activities.'") (internal quotation marks omitted). For a discussion of pre-crime programs, *see* Jennifer C. Daskal, *Pre-Crime Restraints: The Explosion of Targeted, Noncustodial Prevention*, 99 CORNELL L. REV. 327 (2014).

42. Ally Marotti, *Chicago Police Used Geofeedia, the TweetDeck for Cops Under Fire from ACLU*, CHI. TRIB. (Oct. 13, 2016), http://www.chicagotribune.com/bluesky/originals/ct-geofeedia-police-surveillance-reports-bsi-20161013-story.html.

43. Dell Cameron, *Denver Police Spent $30K on Social Media Surveillance Tools in May*, DAILY DOT (Sept. 19, 2017, 5:19 PM), https://www.dailydot.com/layer8/denver-police-geofeedia-social-media-monitoring/.

44. Jamie Wong, Daisy Sang & Chang-Shyh Peng, *An Android Geofencing App for Autonomous Remote Switch Control*, 11 INT'L J. COMPUTER ELECTRICAL AUTOMATION CONTROL & INFO. ENGINEERING 319, 319 (2017).

45. Cameron, *supra* note 43.

46. Richard Byrne Reilly, *All Your Social Media Posts Now Sorted by Location and Up for Sale*, VENTUREBEAT (Oct. 15, 2014, 4:30 PM), https://venturebeat.com/2014/10/15/all-your-social-media-posts-are-now-in-the-public-domain-forever/.

47. Dell Cameron, *Dozens of Police-Spying Tools Remain After Facebook, Twitter Crack Down on Geofeedia*, DAILY DOT (Feb. 24, 2017, 7:15 AM), https://www.dailydot.com/layer8/geofeedia-twitter-facebook-instagram-social-media-surveillance/.

48. Lee Fang, *The CIA Is Investing in Firms that Mine Your Tweets and Instagram Photos*, INTERCEPT (Apr. 14, 2016, 1:57 PM), https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/.

forces,[49] private companies, and schools.[50] The Chicago police, for instance, claimed to have used Geofeedia along with "publicly available tools . . . to monitor open source social media for special events and functions (sporting games, marathons, etc.) . . . ."[51] Critics argue, however, that the software can be used for discriminatory purposes and claim that Geofeedia's promotional materials "suggest the product can be used in ways that target activists . . . ."[52] For example, Geofeedia's documents explicitly identify unions and activist groups as "overt threats."[53] The ACLU of Northern California reports that Geofeedia "invite[d] the Los Angeles District Attorney to learn how Baltimore used the software to monitor and 'stay one step ahead of the rioters' after the police killing of Freddie Gray."[54] In addition to substantial constitutional concerns, the use of social media surveillance and geofencing raises significant concerns about transparency and individual accountability.[55] After the ACLU disclosed information regarding law enforcement's use of Geofeedia during protests, Facebook, Twitter, and Instagram denied Geofeedia access to their data in 2016.[56] Geofeedia, however, is among many other companies that provide geofencing and social media surveillance services.[57] Law enforcement, therefore, may access a number of tools that permit officers to draw inferences of suspicion about individuals based primarily on digital data.[58]

Because Geofeedia relies principally on publicly available social media information, as well as people's presence in public places, law enforcement's use of geofencing tools likely evades Fourth Amendment protection under established

---

49. Ozer, *supra* note 6.

50. Dell Cameron, *CIA-Backed Surveillance Software Was Marketed to Public Schools*, DAILY DOT (Oct. 18, 2016, 12:12 PM), https://www.dailydot.com/layer8/geofeedia-surveillance-software-high-school-chicago-social-media-monitoring/.

51. Marotti, *supra* note 42 (quoting Chicago Police Department spokesman Anthony Guglielmi).

52. Ozer, *supra* note 6.

53. *Id.* (providing access to Geofeedia materials obtained by the ACLU).

54. *Id.*

55. *Id.*

56. Amina Elahi, *Geofeedia Cuts Half of Staff After Losing Access to Twitter, Facebook*, CHI. TRIB. (Nov. 21, 2016), http://www.chicagotribune.com/bluesky/originals/ct-geofeedia-cuts-jobs-surveillance-bsi-20161121-story.html.

57. *See, e.g.*, Kalev Leetaru, *Geofeedia Is Just the Tip of the Iceberg: The Era of Social Surveillance*, FORBES (Oct. 12, 2016), https://www.forbes.com/sites/kalevleetaru/2016/10/12/geofeedia-is-just-the-tip-of-the-iceberg-the-era-of-social-surveillence/#2883a6f55b90; Press Release, Att'y Gen. of Mass., AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities (Apr. 4, 2017), http://www.mass.gov/ago/news-and-updates/press-releases/2017/2017-04-04-copley-advertising-geofencing.html.

58. Justin Jouvenal, *The New Way Police Are Surveilling You: Calculating Your Threat 'Score'*, WASH. POST (Jan. 10, 2016), https://www.washingtonpost.com/local/public-safety/the-new-way-police-are-surveilling-you-calculating-your-threat-score/2016/01/10/e42bccac-8e15-11e5-baf4-bdf37355da0c_story.html?utm_term=.b87984ddb5d4 (describing a software program in use by law enforcement that "scoured billions of data points, including arrest reports, property records, commercial databases, deep Web searches and [a suspect's] social-media postings" to calculate a "threat level").

jurisprudence.[59] Individuals who present themselves in public or post information that is fully accessible to the public through social media could not reasonably claim a legitimate expectation of privacy over such information under the *Katz* privacy test.[60]

B. Future Attribute Screening Technology and Precrime Programs

Another developing technology that seems to fall outside the *Katz* test is FAST, a DHS predictive policing tool intended to "equip security officials with quantitative tools to rapidly assess potential and unknown threats."[61] Predictive analytic systems intended to predict and prevent future crimes, and acts of terrorism, have been utilized with increasing frequency in the years following the terrorist attacks of September 11, 2001.[62] FAST, a post-9/11 program that is under development by DHS, analyzes "specific psychophysiological signals and behavioral attributes, e.g., respiration, cardiovascular response, eye movement, thermal measures, and gross body movement of a screened individual"[63] to "evaluat[e] suspicious behaviors and judg[e] the implications of those behaviors."[64]

The goal of FAST is to detect "malintent," a term that DHS defines as "the mental state of an individual intending to cause harm to our citizens or infrastructure."[65] FAST's technology is intended to identify individuals displaying characteristics associated with malintent.[66] The malintent analysis captures a broad range of potential harms, including "the extent of planned harm, the future time horizon of the event, and the consequences to the individual who is planning the event."[67] The FAST project also incorporates "passive stimuli" as a means for improving

---

59. *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (explaining that an individual in public has no reasonable expectation of privacy in movements from one place to another); Smith v. Maryland, 442 U.S. 735, 742 (1979) (finding no legitimate expectation of privacy in information disclosed to others).

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

61. *DHS/S&T/PIA-012 Future Attribute Screening Technology (FAST)/ Passive Methods for Precision Behavioral Screening*, U.S. DEP'T OF HOMELAND SEC. (May 26, 2016), https://www.dhs.gov/publication/dhsstpia-012-future-attribute-screening-technology-fast-passive-methods-precision.

62. WALTER L. PERRY ET AL. PREDICTIVE POLICING: THE ROLE OF CRIME FORECASTING IN LAW ENFORCEMENT OPERATIONS 3–5 (2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf (discussing the origins of predictive policing).

63. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT UPDATE FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST)/PASSIVE METHODS FOR PRECISION BEHAVIORAL SCREENING 3 (2011), https://www.dhs.gov/sites/default/files/publications/privacy_pia_012a-s%26t_fast.pdf [hereinafter 2011 FAST PASSIVE METHODS PRIVACY IMPACT ASSESSMENT].

64. *Id.* at 2.

65. U.S. DEP'T OF HOMELAND SEC. SCI. & TECH. DIRECTORATE, FUTURE ATTRIBUTE SCREENING TECHNOLOGY (2014), https://www.dhs.gov/sites/default/files/publications/Future%20Attribute%20Screening%20Technology-FAST-508_0.pdf.

66. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008), https://www.dhs.gov/sites/default/files/publications/privacy_pia_012-s%26t_fast-2008.pdf [hereinafter 2008 FAST PRIVACY IMPACT ASSESSMENT].

67. *Id.*

accurate identification of malintent.[68] Passive stimuli is defined as "the activation by the environment of an individual's mental representations of malintent and associated behavioral and physiological responses, without the need for an active conversant response by the individual."[69] In other words, it appears that FAST attempts to detect an individual's future actions using, among other data, analysis of an individual's physiological characteristics and responses to environmental stimuli.

Although FAST does not collect personally identifiable information,[70] substantial concerns remain about government screening and data collection of personal bodily functions.[71] The efficacy of technologies such as FAST has been called into question as well.[72] Trials for FAST reported by DHS purport to demonstrate a 70% success rate for identifying malintent.[73] The field accuracy of FAST remains unclear, as malintent detection is applied to volunteers who have been told to engage in disruptive behavior—although the individuals conducting the screening are unaware of which volunteers have malintent.[74] Arguably, individuals who are participating in a trial may have different physiological and emotional reactions than individuals who really are intending to engage in misconduct. Real conditions and simulated conditions may vary significantly, and some experts challenge whether the accuracy of precrime technologies can be tested in advance or tested at all.[75]

Programs such as FAST potentially risk mass misidentification of innocent individuals through false positives.[76] Experts have questioned whether FAST sensors will be able to accurately distinguish the attributes of malintent from the physiological traits of flight anxiety, for instance.[77] A reasonable suspicion determination under FAST would be difficult to challenge.[78] First, a defendant would carry the burden of proving FAST's inaccuracy in challenging the lawful-

68. 2011 FAST PASSIVE METHODS PRIVACY IMPACT ASSESSMENT, *supra* note 63, at 3.

69. *Id.*

70. *Id.*

71. *See, e.g.*, Pam Benson, *Will Airports Screen for Body Signals? Researchers Hope So*, CNN (Oct. 7, 2009), http://edition.cnn.com/2009/TECH/10/06/security.screening/index.html?iref=nextin.

72. *See, e.g.*, Sharon Weinberger, *Terrorist 'Pre-Crime' Detector Field Tested in United States*, NATURE (May 27, 2011), http://www.nature.com/news/2011/110527/full/news.2011.323.html.

73. Viktor Mayer-Schönberger & Kenneth Cukier, *Should We Use Big Data to Punish Crimes Before They're Committed?*, POPULAR SCI. (Mar. 6, 2013), http://www.popsci.com/science/article/2013-03/should-we-use-big-data-to-punish-crimes-before-theyre-committed#page-2.

74. 2008 FAST PRIVACY IMPACT ASSESSMENT, *supra* note 66, at 3.

75. *See, e.g.*, Alexander Furnas, *Homeland Security's 'Pre-Crime' Screening Will Never Work*, ATLANTIC (Apr. 17, 2012), https://www.theatlantic.com/technology/archive/2012/04/homeland-securitys-pre-crime-screening-will-never-work/255971/.

76. *See id.*

77. Weinberger, *supra* note 72.

78. *See, e.g.*, Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15 (2016).

ness of a detention under FAST.[79] Second, an experienced officer alerted by a system like FAST could easily identify a host of reasons why an individual was targeted that are unrelated to the screening system. Third, it is difficult to imagine how to litigate a case in which the defendant had not yet committed a crime, but nonetheless faces administrative or criminal-like consequences.[80] The use of a system like FAST raises concerns about changes in individual and social expectations of privacy if the technology ever comes into widespread public use. The use of geofencing tools like Geofeedia or other similar technologies presents similar concerns. Yet, under the *Katz* test, these tools might not offend an individual expectation of privacy because they rely on information that is not considered "private," such as publicly available social media posts or an individual's biometric identifiers and physiological public presentment.

II. LIMITATIONS OF THE *KATZ* PRIVACY TEST

In two recent cases, *United States v. Jones* and *Riley v. California,* the Supreme Court has indicated that the Fourth Amendment doctrine must evolve to limit government intrusiveness in light of increasingly comprehensive and invasive cybersurveillance technologies. The Court has yet to develop a new legal privacy doctrine that replaces the "reasonable expectation of privacy" test established in *Katz.*[81] The increasingly comprehensive nature of big data cybersurveillance presents unprecedented types of society-wide intangible harms that could not have been anticipated at the time *Katz* was decided. A dramatic revision of Fourth Amendment doctrine is therefore necessary.

Katz's departure from existing Fourth Amendment precedent was motivated by the Court's belief that the Fourth Amendment must be modified to address modern government surveillance techniques.[82] These techniques were unrestrained by previous Fourth Amendment cases such as *Goldman v. United States*[83] and *Olmstead v. United States*[84] that focused on "searches and seizures of tangible property" as a prerequisite to finding a Fourth Amendment violation.[85] In *Katz*, the Court expanded the protection of the Fourth Amendment beyond constitutionally protected areas,[86] and instead focused its inquiry on individual expectations of privacy.[87]

---

79. United States v. Esquivel-Rios, 725 F.3d 1231, 1239 (10th Cir. 2013) (explaining that a defendant carries the burden of proof of a Fourth Amendment violation in a motion to suppress).

80. *See supra* notes 40–41 (discussing the No-Fly List and the Administrative State).

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

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

83. 316 U.S. 129 (1942).

84. 277 U.S. 438 (1928).

85. *Katz*, 389 U.S. at 352–53.

86. *Id.* at 351 ("[T]he Fourth Amendment protects people, not places.").

87. *Id.* at 351–52.

The Court explained that what a "person knowingly exposes to the public, even in his home or office" is not protected by the Fourth Amendment, "[b]ut what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[88] The Court rejected the notion that a person placing a phone call in a glass phone booth surrenders constitutional protection from intrusion simply because he is visible while making the call.[89] Instead, the relevant fact was the individual's expectation that, by using a phone booth, he would prevent third parties from hearing his conversation.[90] The Court acknowledged the need to adapt the protections provided by the Fourth Amendment to match technological and social developments: "To read the Constitution more narrowly is to ignore the vital role that the public telephone has come to play in private communication."[91]

Justice Harlan's concurrence in *Katz* sets forth the two-part test now used to determine whether a Fourth Amendment violation has occurred. The first step requires determining whether "a person ha[s] exhibited an actual (subjective) expectation of privacy."[92] The second step requires determining whether "the expectation [is] one that society is prepared to recognize as 'reasonable.'"[93] Harlan explained that while a telephone booth may be a public place, closing the door transforms the booth into "a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[94] Harlan noted that modern technology had limited the usefulness of the trespass doctrine because surveillance could be accomplished without intrusion: "Its 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."[95]

In place of the trespass doctrine, *Katz* left a more flexible reasonable expectation of privacy test that protected against government intrusion, physical or otherwise, so long as the targeted individual intended to keep his affairs private.[96] Modern technology has, however, created tension in applying the second step of *Katz*.[97] Under the application of the *Smith v. Maryland*[98] third party doctrine, "an individual has no legitimate expectation of privacy in information provided to

88. *Id.*
89. *Id.* at 352.
90. *Id.*
91. *Id.*
92. *Id.*
93. *Id.*
94. *Id.*
95. *Id.* at 362.
96. *Id.*
97. *See* United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (arguing that the third party doctrine is problematic in the digital age).
98. 442 U.S. 735 (1979).

third parties."[99] As Justice Sotomayor pointed out in her *Jones* concurrence, "[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[100] This aspect is particularly problematic for suspicionless data collection practices, which rely on information that is publicly available, provided to third parties, or does not qualify as content (metadata)—or individual presence in public spaces.

In recent Fourth Amendment cases, the Court has examined the utility of the *Katz* test in light of modern surveillance techniques.[101] This examination is essential if the Fourth Amendment is to maintain any bite, as the "reasonable expectation" standard of *Katz* may lead to patently unreasonable results. The Court has identified some discomfort with the scope of modern surveillance, but it has struggled to articulate the point at which surveillance goes too far. Essentially, the Justices know it when they see it,[102] even if they are unable to clearly articulate why surveillance that seems to fit within *Katz*'s ambit potentially violates the Fourth Amendment. The heart of this problem is that the *Katz* test does not appear to be offended by cybersurveillance tools like geofencing and FAST that can subject both citizens and noncitizens to mass, suspicionless, criminal, and national security profiling through the collection and analysis of comprehensive databases of personally identifiable information.[103] And as such, the *Katz* standard appears inadequate for protecting Fourth Amendment values in the context of suspicionless seizures of data and subsequent analysis of that data. Much like the *Katz* Court, the current Court appears to be grappling with the impact of technology on Fourth Amendment doctrine, and the Justices have noted the need for an evolution of that doctrine.[104]

In *United States v. Jones*, the Supreme Court considered whether warrantless tracking of a criminal suspect through a GPS device attached to the suspect's

---

99. ACLU v. Clapper, 959 F. Supp. 2d 724, 749 (S.D.N.Y. 2013), *aff'd in part, vacated in part*, ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015).

100. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

101. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014); *Jones*, 565 U.S. 400.

102. In *Jacobellis v. Ohio*, Justice Stewart famously noted that, although he cannot define pornography, he "know[s] it when [he] see[s] it." 378 U.S. 184, 197 (1964) (Stewart, J., concurring). In oral argument in *United States v. Jones*, the Justices appeared to share a similar struggle with defining when surveillance had crossed the boundaries of the Fourth Amendment and came into tension with *Katz*. *See* Transcript of Oral Argument, *supra* note 19, at 23–25.

103. 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 cybersurveillance, including the consequences of big data "pre-crime" systems, *see* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 6–12 (2013); Richards, *supra* note 3; Julie E. Cohen, *What Privacy Is for*, 126 HARV. L. REV. 1904, 1913 (2013).

104. *See, e.g.*, *Jones*, 565 U.S. at 416–17 (Sotomayor, J., concurring).

vehicle was constitutional.[105] Law enforcement agents attached a GPS device to Jones's vehicle, where it remained for 28 days to allow for the tracking of the vehicle's movements.[106] During that time, the device calculated and transmitted the vehicle's precise location to law enforcement at ten-second intervals.[107] Officers used the GPS tracking data to discover a stash house containing large amounts of narcotics.[108] The GPS device did not provide information about the contents of Jones's Jeep or any conversations he had in the car—it only transmitted his locational data on a constant basis.[109] The technology itself was similar to the "beeper" cases technology,[110] but the real difference was that it made long-term, comprehensive surveillance feasible and automatically recorded the data that law enforcement officers could review at their convenience.[111]

During oral argument, several Justices conceded that the expectation of privacy test, as currently formulated, would not restrain the use of increasingly comprehensive and invasive data-driven surveillance techniques.[112] The tenor of the Justices' questions suggested that the evolution of these technologies required a parallel evolution of Fourth Amendment doctrine to be consistent with modern cyber developments.[113] The government argued that the intrusiveness of increasingly comprehensive surveillance methods is mediated by a public that has become accustomed to being monitored by new forms of technology.[114] Nonetheless, several of the Justices explored the option of modifying the Fourth Amendment doctrine.[115] The Court's discussion of potential modification of Fourth Amendment jurisprudence seemed to suggest that the *Katz* test should lead with the social

---

105. *Id.* at 402 (majority opinion). Officers had obtained a warrant to install the device on a vehicle registered to Jones's wife, which required them to install the GPS within ten days and in the District of Columbia. *Id.* at 402–03. Officers installed the device in Maryland after the ten-day period had expired. *Id.* at 403.

106. *Id.* at 403.

107. *Id.;* Brief for Respondent at 4, *Jones*, 565 U.S. 400 (No. 10-1259).

108. *Jones*, 565 U.S. at 403–04.

109. Brief for Petitioner at 49–50, *Jones*, 565 U.S. 400 (No. 10-1259) (explaining that the GPS device "does not conduct either a visual or aural search of the item to which it is attached . . . . [I]t provides information only about the vehicle's location").

110. *See id.* at 38 ("The GPS device used in this case conveyed the same type of information that the beeper conveyed in *Knotts*—the approximate location of the object to which it was attached."); *see also* United States v. Jones, 625 F.3d 766, 768 (D.C. Cir. 2010) (Sentelle, C.J., dissenting) ("There is no material difference between tracking the movements of the *Knotts* defendant with a beeper and tracking the *Jones* appellant with a GPS.").

111. *See* United States v. Maynard, 615 F.3d 544, 556 (D.C. Cir. 2010); Brief for Respondent at 24–28, *Jones*, 565 U.S. 400 (No. 10-1259); *see also* Transcript of Oral Argument, *supra* note 19, at 57–58.

112. *See* Transcript of Oral Argument, *supra* note 19, at 24–25.

113. *See id.* at 3–4, 10–11.

114. *See id.* at 57 ("Today perhaps GPS can be portrayed as a *1984*-type invasion, but as people use GPS in their lives and for other purposes, our expectations of privacy surrounding our location may also change."). Justice Kagan was immediately skeptical of this claim, posing the hypothetical that "a little robotic device follow[s] 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 . . . ." *Id.* at 57–58. She noted that she was "not sure how one can say that" a reasonable expectation of privacy would not be violated by such tracking. *Id.* at 58.

115. *See id.* at 50–51 (suggesting society may tolerate monitoring of someone police think may set off a huge bomb, even if no probable cause exists).

inquiry first.[116] Under such a suggested approach, the *Katz* subjective-objective test would instead become an objective-subjective test.[117]

Ultimately, the Court decided *Jones* on narrow grounds,[118] avoiding the opportunity to modify the reasonable expectation of privacy standard in the cyber arena.[119] Justice Scalia explained that either a trespass or a *Katz* invasion may be a Fourth Amendment search:

> *Katz* . . . established that property rights are not the sole measure of Fourth Amendment violations, but did not snuf[f] out the previously recognized protection for property . . .. *Katz* did not erode the principle that, when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment.[120]

The two concurring opinions by Justices Alito and Sotomayor both attempted to examine the broader issues at the heart of *Jones*. Justice Alito recognized that the *Katz* test had the potential to accommodate increasing levels of government intrusiveness. He explained that the "hypothetical reasonable person" is presumed to have a "well-developed and stable set of privacy expectations."[121] He noted that technology can change expectations of privacy, a concern reflected in other Fourth Amendment cases.[122] Justice Alito explained that individuals accept diminished privacy as a "tradeoff" for "increased convenience or security" of new technology, and may ultimately accept the tradeoff as inevitable.[123] He recognized that the *Katz* test is grounded in changing social norms that the Court must give effect to as a form of customary law—the general social expectation about what can be kept private.

Although Justice Alito did not fully explain how he would have resolved the issue, his opinion offers a shift away from a privacy standard towards an intrusion standard. He acknowledged the struggle the Court faced: "The best that we can do in this case is to 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

---

116. *See id.* at 12–13, 44, 51.

117. *See id.* at 22, 24, 57–58 (discussing objective perspectives on privacy); *see also* Hu, *supra* note 35.

118. *See* United States v. Jones, 565 U.S. 400, 408–13 (2012).

119. *Id.* at 412–13. The role of cybersurveillance in governance, security goals, and database rights has formed the basis for significant academic discourse in recent years. *See, e.g.*, JEFFREY ROSEN, THE NAKED CROWD (2004); BENJAMIN WITTES, BROOKINGS INST., DATABUSE: DIGITAL PRIVACY AND THE MOSAIC (2011), http://www.brookings./research/papers/2011/04/01-databuse-wittes; James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177 (1997); Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264 (2004).

120. *Jones*, 565 U.S. at 407 (internal quotation marks omitted).

121. *Id.* at 427 (Alito, J., concurring).

122. *Id.*

123. *Id.*

reasonable person would not have anticipated."[124] Alito's concurrence appears to suggest a revision of existing Fourth Amendment doctrine because "intrusiveness" is not precisely consistent with the reasonable expectation of privacy test.[125]

Justice Sotomayor's *Jones* concurrence also hinted at the need to shift from a privacy standard to a nonintrusion standard. In addition, she stressed the need to lead with an inquiry focusing on broad social concerns rather than individual rights, when considering the potential Fourth Amendment harms from cybersurveillance.[126]

In *Riley v. California*, the Supreme Court considered a pair of cases with a common issue: "whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested."[127] In both cases, officers discovered a cell phone in a search incident to an arrest.[128] The officers then looked through the phones and discovered evidence that was used to prosecute the arrestees.[129] Each arrestee—David Riley and Brima Wurie—moved to suppress the evidence obtained from the phone searches, arguing that the search violated their Fourth Amendment rights.[130] In Riley's case, the California Court of Appeals affirmed his conviction based on California precedent.[131] Wurie, however, fared better in the First Circuit on appeal. There, the court held that cell phones "are distinct from other physical possessions that may be searched incident to arrest without a warrant, because of the amount of personal data cell phones contain and the negligible threat they pose to law enforcement interests."[132]

Finding for the arrestees, Chief Justice Roberts's opinion focused on the relationship between technological developments and privacy and hearkened back to fundamental constitutional principles. According to the Chief Justice, cell phones raise both qualitative and quantitative privacy concerns that differ from other items of personal property found during a search incident to an arrest. Specifically, cell phones contain "vast quantities of personal information"[133]

---

124. *Id.* at 430.

125. Justice Alito's concurrence appears to focus primarily on identifying the flaws in Justice Scalia's majority opinion. *See id.* at 424–31 (discussing the flaws in the *Katz* test in relation to technological and social changes and suggesting that a legislative solution may be the best option). *Compare id.* at 430 (asking if the GPS "involved a degree of intrusion that a reasonable person would not have anticipated"), *with* Smith v. Maryland, 442 U.S. 735, 740 (1979) (explaining that the first inquiry under *Katz* is "whether the individual, by his conduct, has 'exhibited an actual (subjective) expectation of privacy'—whether . . . the individual has shown that 'he seeks to preserve [something] as private.'" (citation omitted) (quoting Katz v. United States, 389 U.S. 347, 361, 351 (1967))).

126. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring).

127. Riley v. California, 134 S. Ct. 2473, 2480 (2014).

128. *Id.* at 2480–81.

129. *Id.*

130. *Id.* at 2481–82.

131. *Id.* at 2481 ("The court relied on the California Supreme Court's decision in *People v. Diaz*, which held that the Fourth Amendment permits a warrantless search of cell phone data incident to an arrest, so long as the cell phone was immediately associated with the arrestee's person." (citing People v. Diaz, 244 P.3d 501 (Cal. 2011))).

132. *Id.* at 2482.

133. *Id.* at 2485.

available by storage capacity, functionality, and the possibility of remote cloud access.[134] Chief Justice Roberts cited Justice Sotomayor's concurring opinion in *Jones*, pointing out that the data on a phone and apps can provide extraordinary quantities of information about a person's private life.[135] A cell phone "contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is."[136] The Chief Justice explained that the nature of technology did not alter the fundamental principles upon which American democracy was founded.[137] Analogizing the scope of a warrantless search of a cell phone to the "reviled" general warrant, Chief Justice Roberts concluded: "The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought."[138]

In his concurring opinion, Justice Alito disagreed with Chief Justice Roberts's resort to "predigital" rules. Reiterating points made in his *Jones* concurrence, Alito argued that the transformation of technology "calls for a new balancing of law enforcement and privacy interests."[139] Justice Alito added, however, that such transformation should be done by the legislature, rather than "the federal courts using the blunt instrument of the Fourth Amendment."[140]

Both *Jones* and *Riley* marked a victory for those seeking robust Fourth Amendment protections in the face of technological advancement. In *Jones*, the Court's resolution of the case rejected the government's main contention that warrantless installation of a GPS device was not a search under the Fourth Amendment.[141] In *Riley*, the Court highlighted the importance of privacy in the digital age and its relationship to changing technology. In both cases, however, the Court avoided the larger question of how to address emerging cybersurveillance and dataveillance technologies. These cases represent the most recent collisions between cybersurveillance technology and the limits of Fourth Amendment doctrine in the Supreme Court,[142] and the Court still has not fully come to grips

---

134. *Id.* at 2491.

135. *Id.* at 2490 (noting that a GPS can generate precise records of "familial, political, professional, religious, and sexual associations") (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

136. *Id.* at 2491.

137. *Id.* at 2494–95 (discussing the founding generation's motivations for creating the Fourth Amendment and arguing that technological developments in how private information is stored does not alter the protections accorded that information).

138. *Id.* at 2495.

139. *Id.* at 2496–97 (Alito, J., concurring).

140. *Id.* at 2497.

141. *Jones*, 565 U.S. at 404.

142. At the time this Article was written, the Court had recently granted certiorari in *United States v. Carpenter*, 819 F.3d 880 (6th Cir. 2016), which addressed the constitutionality of the warrantless seizure and search of cell site tower location information. *See* Carpenter v. United States, 137 S. Ct. 2211 (2017) (granting certiorari).

with the implications modern cybersurveillance has for individual privacy.[143] Although Justice Alito's concurrences in *Riley* and *Jones* point to legislatures as the solution to the "diminution of privacy,"[144] any test that revolves around an increasingly fleeting concept of privacy will likely become insufficient to protect Fourth Amendment freedoms threatened by mass surveillance. Such surveillance threatens more than just the Fourth Amendment.[145] For that reason, a new theory of the Fourth Amendment is essential.

III. TOWARDS A THEORY OF A FOURTH AMENDMENT NONINTRUSION TEST

In a small data world, physical intrusions[146] and bodily intrusions[147] were primarily at the forefront of the Fourth Amendment inquiry.[148] Increasingly, the

---

143. *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 (2004); William Funk, *Electronic Surveillance of Terrorism in the United States*, 80 MISS. L.J. 1491 (2011); Renée McDonald Hutchins, *Tied Up in* Knotts*? GPS Technology and the Fourth Amendment*, 55 UCLA L. REV. 409 (2007). Other scholars examine statutory frameworks for governing surveillance technologies and for structuring domestic and foreign intelligence surveillance law. They recommend the enactment of congressional legislation to resolve any potential harms emanating from modern cybersurveillance, rather than reliance upon the Fourth Amendment. *See, e.g.*, Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607 (2003); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857–60 (2004); Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1308 (2004) (explaining that Supreme Court drew distinction between domestic and "foreign intelligence" surveillance and what procedures were required under the Fourth Amendment). Swire writes:

> 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.

Swire, *supra*, at 1308.

144. *See* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (Alito, J., concurring); United States v. Jones, 565 U.S. 400, 427–28 (2012) (Alito, J., concurring).

145. *See* Strossen, *supra* note 4, at 1145–46.

146. The term physical intrusions, as used here, refers to seizures of individuals. *See* Safford Unified Sch. Dist. No. 1 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").

147. The term bodily intrusions refers to actions that intrude into an individual's body. *See* Birchfield v. North Dakota, 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, 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).

148. *See Riley*, 134 S. Ct. at 2483–84 (describing case precedent addressing searches incident to arrest).

Court appears to now recognize, however, that the physicality of the intrusion is no longer the primary threat in a big data world.[149] In *Jones*, which was resolved on the physical intrusion, the concurrences of Justice Alito and Justice Sotomayor demonstrate a growing awareness by the Court that cybersurveillance intrusions were now at the forefront of the Fourth Amendment inquiry. Justices Alito and Sotomayor reasoned that cybersurveillance presents exactly the type of non-physical intrusive harm that is proscribed under the *Katz* privacy test.[150]

Technologies such as Geofeedia and FAST, and other emerging cybersurveillance tools, present especially difficult challenges to the Fourth Amendment. This is in part because cybersurveillance intrusions have not been explicitly defined by the Court. Federal courts, however, increasingly show a recognition of factors relevant to a determination as to whether a cybersurveillance intrusion has occurred: cost, duration of tracking or storage duration of information collected, mass ubiquity and suspicionless nature of the surveillance, automation- and data-oriented tools, surreptitious and virtual methods, comprehensive profiling capacity, and potential for facilitating digitized analysis and algorithmic decision-making.

Justice Sotomayor observes that because cybersurveillance, like the GPS monitoring at issue in *Jones*, "is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices."[151] Cybersurveillance monitoring may be short-term or long-term, and it may be suspicionless or targeted. Additionally, cybersurveillance may or may not result in any law enforcement or other consequence beyond the act of data collection, database screening, and digitized analysis.[152] In *Jones*, Justice Alito pointed out the surveillance dangers of long-term monitoring that is possible through extended gathering of geo-locational data through warrantless GPS tracking.[153] Justice Sotomayor reasoned that the potential Fourth Amendment harms were not contingent upon duration or enforcement action—these issues may not be relevant to the constitutional inquiry.[154] Therefore, Justice Sotomayor explained, "[i]n cases involving even short-term monitoring, some unique attributes of [cybersurveillance] relevant to the *Katz*

149. *See, e.g.*, *id.* at 2488–89 (pointing out that the scope of privacy intrusions is far greater with access to digital data); *Jones*, 565 U.S. at 405 ("Our later cases, of course, have deviated from that exclusively property-based approach [to the Fourth Amendment]."); *Jones*, 565 U.S. 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.'" (quoting Katz v. United States, 389 U.S. 347, 353 (1967))).

150. United States v. Jones, 565 U.S. 400, 414 (2012) (Sotomayor, J., concurring) ("[A]s Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance.").

151. *Id.* at 415–16.

152. *Id.* at 415 ("The government can store such [digitized] records and efficiently mine them for years into the future.").

153. *Id.* at 428–30 (Alito, J., concurring).

154. *Id.* at 415 (Sotomayor, J., concurring).

analysis will require particular attention."[155] Both Justice Alito and Justice Sotomayor expressed concern regarding broader constitutional harms of cybersurveillance,[156] including the chilling of expressive and associational freedoms.[157]

A test centered on societal nonintrusion, rather than personal privacy, is more appropriate to address the growing challenges of cybersurveillance technology and the harms emanating from the protocols and programs of bureaucratized cybersurveillance. To explore what the contours of a nonintrusion test might be, it is first necessary to examine the shortcomings of the *Katz* privacy test. Under the *Katz* test, a court first analyzes whether the individual's subjective expectation of privacy has been offended.[158] The second step of *Katz* requires a court to consider whether society objectively ratifies the individual's subjective expectation of privacy.[159] In both steps, however, the focus is on the individual's harm. The nonintrusion test implicitly suggested by the concurrences in *United States v. Jones* shifts the Fourth Amendment analysis from an individual's harm to a society-wide harm. Instead of requiring the individual to show a subjective reasonable expectation of privacy, the nonintrusion test instead first requires the government to justify the intrusion of the surveillance.[160] The significant question would be whether a societal-wide, objective expectation of governmental nonintrusion has been offended.

In other words, a court would need to understand not just how a surveillance program intrudes upon an individual's life but how that program intrudes upon everyone's life, across society.[161] Cybersurveillance often requires amassing a database of information across certain sectors of society in order to be effective, or indeed, all of society.[162] That would be the context from which a court should properly understand the implications of ratifying such surveillance as free of any

---

155. *Id.*

156. *Id.* at 430 (Alito, J., concurring) ("[S]ociety's expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalogue every single movement of an individual[] . . . .").

157. *Id.* at 416 (Sotomayor, J., concurring) ("Awareness that the government may be watching chills associational and expressive freedoms.").

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

159. *Id.*

160. Justices on the Supreme Court have previously considered shifting the burden to the government. United States v. White, 401 U.S. 745, 793 (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.").

161. *See, e.g.*, Gray & Citron, *supra* note 2, at 71–72 (arguing that the threshold question in a Fourth Amendment inquiry should be "whether a technology has the capacity to facilitate broad and indiscriminate surveillance that intrudes upon reasonable expectations of quantitative privacy by raising the specter of a surveillance state . . . ."); *see also* Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013), *vacated*, Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015) ("Thus, plaintiffs have a substantial likelihood of showing that their privacy interests outweigh the Government's interest in collecting and analyzing bulk telephony metadata and therefore the NSA's bulk collection program is indeed an unreasonable search under the Fourth Amendment.").

162. *See Klayman*, 957 F. Supp. 2d at 39 ("To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.").

Fourth Amendment restrictions. Next, a court would consider whether the subjective expectation of protection from government intrusion was reasonable. This inquiry would focus on whether an intrusion had occurred, rather than individualized expectations of privacy.

Adoption of a nonintrusion test potentially resolves many of the problems posed by cybersurveillance technological developments under the third party doctrine. Because the primary inquiry would no longer center on an individualized "expectation of privacy," whether an individual had voluntarily shared digital data with third parties like internet service providers or telecommunications companies would no longer control the Fourth Amendment analysis.

It is undisputed that the Court continues to struggle with how best to preserve the integrity of the Fourth Amendment in the face of changing technology and the different harms threatened by that technology.[163] Property and tort law, the traditional anchors of Fourth Amendment doctrine, cannot protect against the types of harms caused by this advancing technology.[164] Technology increasingly implicates the search and seizure of data of entire populations of individuals, particularly surveillance methods that turn on the accumulation and storage of information in databases. In such cases, the invasion of privacy suffered by an individual has as its starting point a much broader harvesting of social information across entire sectors of society. A socially-oriented framework of a kind of customary law[165] is now more appropriate to preserve the first principles of the Fourth Amendment because the dangers are presented to autonomy and freedom that make up an open democratic society.[166] The oral argument in *Jones* made clear an almost visceral objection to ratifying the government surveillance at issue there, even without an articulate legal rationale for why the Fourth Amendment was offended. Modern surveillance technologies have the capacity to threaten democratic norms and customs. These fundamental democratic principles must be articulated and preserved as society negotiates the tolerable boundaries of ongoing, pervasive cybersurveillance.

A nonintrusion test offers a more flexible and suitable method to evaluate whether the spirit of the Fourth Amendment has been violated. This test shifts the

---

163. *See* 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).

164. *Id.* at 405 (majority opinion) ("The text of the Fourth Amendment reflects its close connection to property, since otherwise it would have referred simply to 'the right of the people to be secure against unreasonable searches and seizures'; the phrase 'in their persons, houses, papers, and effects' would have been superfluous.").

165. We can identify the standard as customary because it requires considering if society would ratify an individual expectation of privacy "under the circumstances" in which the individual held it. *See* Katharine T. Bartlett, *Tradition as Past and Present in Substantive Due Process Analysis*, 62 DUKE L.J. 535, 540 (2012); Curtis A. Bradley & Mitu Gulati, *Withdrawing from International Custom*, 120 YALE L.J. 202 (2010); Curtis A. Bradley & Neil Siegel, *Historical Gloss, Constitutional Conventions, and the Judicial Separation of Powers*, 105 GEO. L.J. 255 (2017); Jack L. Goldsmith & Eric A. Posner, *A Theory of Customary International Law*, 66 U. CHI. L. REV. 1113, 1117 (1999); Hu, *supra* note 35.

166. *See* United States v. White, 401 U.S. 745, 792–93 (1971) (Harlan, J., dissenting).

calculation away from determining which levels of privacy are reasonable, or whether a hypothetical reasonable person would shield such information. This shift is critical because modern big data technologies necessitate sharing private information with a wide range of third parties. Indeed, vast numbers of standard consumer-oriented technologies require sharing data with third parties and are often interconnected. As our society orients towards ever-diminishing degrees of personal privacy through the confluence of technological and geopolitical factors, nonintrusion as the basis for Fourth Amendment safeguards is important to protect society's and citizens' constitutionally-protected democratic rights. Otherwise, citizens confront a choice between availing themselves of the conveniences and necessities of contemporary technology and surrendering individual privacy that has been historically protected.

At this juncture, a nonintrusion test may raise more questions than it answers. Still, it appears the Court is cautiously moving in this direction.[167] Legal scholarship has recognized that much current Fourth Amendment doctrine is threatened with obsolescence in the current context.[168] The Table below sets forth some observations for discussion of what might be construed as the most salient differences between a non-intrusion test and the *Katz* privacy test.

Table 1: Distinctions Between the *Jones* Nonintrusion Test v. *Katz* Privacy Test

Key	Nonintrusion Test	*Katz* Privacy Test
	Under Fourth Amendment (Pertaining to emerging mass surveillance and cybersurveillance methods)[169]	Under Fourth Amendment[170]
	Government Action in Question: Unreasonable search and seizure of digitally constructed identity and personally identifiable digital data[171]	Government Action in Question: Unreasonable search and seizure of person and property[172]

167. *See Jones*, 565 U.S. at 430 (Alito, J., concurring); *id.* at 417–18 (Sotomayor, J., concurring); Transcript of Oral Argument, *supra* note 19, at 22, 24, 57–58.

168. *See supra* note 2.

169. *See Jones*, 565 U.S. 400.

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

171. *See Jones*, 565 U.S. at 402.

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

Key	Nonintrusion Test	*Katz* Privacy Test
When the tests are used	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[173]	Paradigmatic Case: Government searching and seizing contents of one's diary or letters[174]
	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 Nonintrusion under Fourth Amendment: Reasonable expectation to be free of unreasonable cybersurveillance and government intrusion[175]	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[176]
	No third-party doctrine: Expectation of nonintrusion does not pivot on whether information was shared with others[177]	Third party doctrine: No expectation of privacy if information shared with third party[178]

173. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013) (presenting prima facie challenges to a provision of the Foreign Intelligence Surveillance Amendments Act of 2008, which empowers the FISC to authorize surveillance without a showing of probable cause that the target of surveillance is an agent of a foreign power).

174. *See id.*

175. *Jones*, 565 U.S. at 410–12.

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

177. *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring) (questioning the validity of the third party doctrine, as applied to modern technology).

178. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (articulating the third party doctrine).

Key	Nonintrusion Test	*Katz* Privacy Test
	Grounded in the positive right perspective (or hybrid) of the Fourth Amendment: "The right of the people to be secure in their persons, houses, papers, and effects"[179]	Grounded in the negative right perspective of the Fourth Amendment: Free from "unreasonable searches and seizures."[180]
	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?[181]	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?[182]
Focus of judicial inquiry under the tests	Vantage Point of Inquiry: Societal interest in open democratic society (e.g., to be free from "*1984*"-type surveillance).[183]	Vantage Point of Inquiry: Personal interest in maintaining information private[184]

179. U.S. CONST. amend. IV; *see also* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 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 Case for a Constitutional Right to Minimum Entitlements*, 44 MERCER L. REV. 525, 534 (1993) (noting that the Constitution creates affirmative duties), Gray, *A Collective Right*, *supra* note 4, at 199–200; Gray, *Dangerous Dicta*, *supra* note 3, at 1196.

180. U.S. CONST. amend. IV; *see also* Dist. of Columbia v. Heller, 554 U.S. 570, 646 (2008) (Stevens, J., dissenting) ("[T]he Fourth Amendment describes a right *against* governmental interference rather than an affirmative right *to* engage in protected conduct"); 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.").

181. *See Jones*, 565 U.S. at 407–08 (Sotomayor, J., concurring) (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1988)).

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

183. Transcript of Oral Argument, *supra* note 19, at 13, 25, 27, 33, 35, 57, (referring to George Orwell's *1984*).

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

Key	Nonintrusion Test	*Katz* Privacy Test
	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)[185]	Individual must first demonstrate individual-based subjective privacy interest is protected under Fourth Amendment[186] and provide evidence of unreliability.[187]
	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
Need for the tests	Protection from Big Data inferences of guilt or suspicion from correlative data-driven evidence and algorithms (e.g., Protection from "guilty until proven innocent" status)[188]	Protection from unwanted revelatory information; physical trespass; and reputational or privacy tort harms[189]
	Concurrences and oral argument in *Jones*: Suggestion that societal-based rights may now center the normative commitment of the Fourth Amendment[190]	Before *Jones*: Conceptualization that individual-based rights center the normative commitment of the Fourth Amendment[191]

185. *See Jones*, 565 U.S. 400; United States v. White, 401 U.S. 745, 792–93 (1971) (Harlan, J., dissenting).

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

187. *See,* United States v. Esquivel-Rios, 725 F.3d 1231, 1238–39 (10th Cir. 2013); United States v. Cortez-Galaviz, 495 F.3d 1203, 1208 (10th Cir. 2007).

188. *See* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 401 (2013).

189. *Katz*, 389 U.S. at 352–53.

190. *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Transcript of Oral Argument, *supra* note 19, at 13, 25, 27, 33, 35, 57 (discussing George Orwell's *1984* in relation to broad surveillance).

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

Key	Nonintrusion Test	*Katz* Privacy Test
Where the tests originated	Constitutional implications of mass cybersurveillance and warrantless, suspicionless tracking play out on public, society-wide level[192]	Constitutional implications of warrantless tracking or suspicionless surveillance of individual suspect unfold on personal, individual-rights level[193]
	Grounded in Customary Law[194]	Grounded in Property Law and Tort Law[195]
Future direction of the tests	Nonintrusion appears to be transforming into the potential new axis for doctrinal analysis under cybersurveillance-oriented Fourth Amendment inquiry after *Jones*[196]	Privacy is current axis for doctrinal analysis under Fourth Amendment inquiry after *Katz*[197]

CONCLUSION

Courts are increasingly confronted with the limitations of current Fourth Amendment doctrine when provided the opportunity to review big data cybersurveillance programs. The *Katz* test—although it is an evolving one, and one that must continue to evolve in light of new cybersurveillance methods—is an important starting point for a Fourth Amendment analysis of the types of harms posed by non-physical cybersurveillance intrusions. Yet the scope of protections afforded by the *Katz* privacy test fails to encompass the types of harms presented by new technologies such as Geofeedia and FAST. Under the two-part *Katz* test, first, it is unlikely that an individual can successfully establish a subjective reasonable expectation of privacy because modern cybersurveillance collects and captures data that has been disclosed over social media, the internet, and in public. Second, as big data cybersurveillance systems are normalized and integrated into preexisting bureaucratized settings, it will be increasingly difficult to find that a privacy expectation that rejects these types of mass surveillance systems is objectively reasonable.

In both *Jones* and *Riley*, the Justices acknowledged the limitations of privacy jurisprudence under the Fourth Amendment as a result of advancing technologies.

---

192. *See* Balkin, *supra* note 4; Balkin & Levinson, *supra* note 4.

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

194. The appropriate role of custom in law, and how and when custom transforms into something that is cognizable as embodying the force of law, is a topic central to a robust debate in the international law context. *See* Bradley & Gulati, *supra* note 165.

195. *See Katz*, 389 U.S. at 370 (Black, J., dissenting).

196. United States v. Jones, 565 U.S. 400, 418 (2012) (Alito, J., concurring).

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

The Court recognized that the relationship between an increasingly digitized society and an increasingly digitized law enforcement structure was changing the balance of power between citizen and State. The Court signaled, therefore, the scope of mass intrusions made possible by cybersurveillance demands an evolution of the Fourth Amendment inquiry. The Court's suggestion of a nonintrusion test to replace the *Katz* privacy test is intended to preserve core constitutional values by leading with an inquiry that centers on societal interests.