Oklahoma Law Review

Volume 66 | Number 4

Symposium: Law Enforcement Access to Third Party Records

2014

The ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology-Centered Approach to Quantitative Privacy

David C. Gray

University of Maryland School of Law, dgray@law.umaryland.edu

The ABA Standards for Criminal Justice: Law Enforcement Access to Third Party Records: Critical Perspectives from a Technology-Centered Approach to Quantitative Privacy

Cover Page Footnote

THE ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS: CRITICAL PERSPECTIVES FROM A TECHNOLOGY-CENTERED APPROACH TO QUANTITATIVE PRIVACY

DAVID GRAY*

I. Introduction

Long a topic of interest only to Fourth Amendment groupies and would-

* Professor of Law, University of Maryland Francis King Carey School of Law. First and foremost, thanks are due to Professor Stephen Henderson and his colleagues on the ABA Task Force who were prescient in pressing the initiative that led to these standards and have committed so much time and good will to their project. Although this essay advances some concerns about the results, the value of the Standards as they stand and as an ongoing project cannot be overstated. This essay is itself part of an ongoing project addressing Fourth Amendment rights and remedies in the twenty-first century. Among its most important components are: Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262 (2013); David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. 1 (2013); David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013); 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); David Gray, Danielle Keats Citron, & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745 (2013); and David Gray, Meagan Cooper, & David McAloon, *The Supreme Court's Contemporary Silver Platter Doctrine*, 91 TEX. L. REV. 7 (2012). For their support and feedback on these efforts, gratitude is due to those who listened and commented during presentations at Georgetown, Law and Society, Yale, the Annual Meeting of the ABA/AALS Criminal Law Section, the University of North Carolina, Northwestern University, the Privacy Law Scholars Conference, the Computers, Freedom, and Privacy Conference, and during conversations at the American Law Institute Meeting on Information Privacy Law and Harvard Law Review's Symposium on Informational Privacy. Particular thanks go to Ronald Allen, Julia Angwin, Jack Balkin, Kevin Bankston, Steve Bellovin, Marc Blitz, Richard Boldt, Becky Bolin, Mary Bowman, Al Brophy, Andrew Chin, Bryan Choi, Thomas Clancy, Julie Cohen, Thomas Crocker, Nick Doty, Lisa Marie Freitas, Susan Freiwald, Barry Friedman, Brandon Garrett, Bob Gellman, Don Gifford, Mark Graber, John Grant, James Grimmelmann, Deborah Hellman, Stephen Henderson, Leslie Meltzer Henry, Lance Hoffman, Renée Hutchins, Camilla Hrdy, Orin Kerr, Joseph Kennedy, Catherine Kim, Anne Klinefelter, Avner Levin, Michael Mannheimer, Dan Markel, Christina Mulligan, Richard Myers, Neil Richards, Kathryn Sabbeth, Laurent Sacharoff, Paul Schwartz, Christopher Slobogin, Robert Smith, Dan Solove, Max Stearns, David Super, Harry Surden, Peter Swire, Peter Quint, Jason Weinstein, Arthur Weisburd, and Jonathan Witmer-Rich. Finally, deepest thanks to the W.P. Carey Foundation for its support of Maryland-Carey School of Law and the scholarly efforts of its faculty.

be Supreme Court justices,[1] the third party doctrine is now a central concern for citizens of the United States and the world.[2] Much of the impetus for this global awakening is a series of leaked documents proving what many privacy scholars already suspected or knew[3]: the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), the National Security Administration (NSA), their foreign counterparts,[4] and a host of domestic agents,[5] are engaged in programs of expansive and invasive surveillance that many have credibly compared to the dark prophesies of George Orwell's *1984*.[6] Science fiction, it seems, is now reality.

---

1. *See* Michael Dolan, *The Bork Tapes*, CITY PAPER, Sept. 25, 1987, at 1.

2. *See, e.g.*, Louise Osborne, *Europeans Outraged over NSA Spying, Threaten Action*, USA TODAY, Oct. 29, 2013, http://www.usatoday.com/story/news/world/2013/10/28/report-nsa-spain/3284609/; Alissa Rubin, *French Condemn Surveillance by N.S.A.*, N.Y. TIMES, Oct. 22, 2013, at A4; Craig Timberg, *Google Encrypts to Defend Against Spying*, WASH. POST, Sept. 6, 2013, at A1.

3. James Bamford has been leading the reportage charge since well before the recent revelations. *See, e.g.*, JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA (2008) [hereinafter THE SHADOW FACTORY]; James Bamford, *The Black Box*, WIRED MAG., Apr. 2012, at 78 [hereinafter Bamford, *The Black Box*], *available at* http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

4. Among the most cooperative are parties to the United Kingdom-United States of America Agreement British, including the United Kingdom, the United States, Canada, New Zealand, and Australia, which are collectively referred to as the "Five Eyes." *See* THE SHADOW FACTORY, *supra* note 3, at 212-33. The U.K.'s General Communications Headquarters (GCHQ) has been particularly helpful, playing a key role in efforts by the NSA to surreptitiously tap data cables and switches located outside the United States in order to access user information from Google and Yahoo. *See id.* at 215-18; Charles Arthur, *Google Engineer Accuses NSA and GCHQ of Subverting 'Judicial Process'*, GUARDIAN, Nov. 6, 2013, http://www.theguardian.com/technology/2013/nov/06/google-nsa-gchq-spying-judicial-process.

5. For example, recently released orders of the Foreign Intelligence Surveillance Court document support provided by telecommunications companies like Verizon and AT&T to the NSA and FBI's telephonic surveillance programs. *See In re* Application of F.B.I. for an Order Requiring Prod. of Tangible Things from [Redacted], No. BR 13-80, at 4 (Foreign Intelligence Surveillance Ct., Apr. 25, 2013) *available at* http://apps.washingtonpost.com/g/ page/politics/ government-documents-related-to-nsa-collection-of-telephone-metadata-records/351/ (ordering the disclosure of "all call detail records or 'telephony metadata' created by [telephone companies] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."). Other companies gather and aggregate data for government agencies on a contract basis. *See* Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 595-96 (2004); Natasha Singer, *You for Sale*, N.Y. TIMES, June 17, 2012, at BU1.

6. Dan Roberts & Spencer Ackerman, *Anger Swells After NSA Phone Records Court Order Revelations*, GUARDIAN, June 6, 2013, http://www.theguardian.com/world/2013/

Among the more disturbing features of this burgeoning surveillance state is the increasing access that governments have to information about us and our activities—information that we entrust to third parties such as our telephone companies, financial institutions, internet service providers, social networks, and commercial partners. Take, for example, the revelation that the NSA, in conjunction with the FBI, has been gathering "all call detail records or 'telephony metadata' created by [telephone companies] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."[7] Although these agencies have so far denied gathering either the contents of telephonic communications[8] or the identities of the callers, telephony metadata, which usually includes telephone numbers, call location, call duration, and call frequency, "can provide authorities with vast knowledge about a caller's identity."[9] "[C]ross-checked against other public records, the metadata can reveal someone's name, address, driver's license, credit history, social security number and more."[10] A second program, referred to in leaked documents as "PRISM," reportedly allows NSA access to information held on the central servers of nine leading U.S. internet companies, "extracting audio and video chats, photographs, e-mails, documents, and connection logs."[11] In addition to, or as part of, this

---

jun/06/obama-administration-nsa-verizon-records ("From a civil liberties perspective, the program could hardly be any more alarming. It's a program in which some untold number of innocent people have been put under the constant surveillance of government agents. It is beyond Orwellian, and it provides further evidence of the extent to which basic democratic rights are being surrendered in secret to the demands of unaccountable intelligence agencies." (quoting Jameel Jaffer, Deputy Legal Director of the American Civil Liberties Union)).

7. *In re* Application of the F.B.I., No. BR 13-80, at 4.

8. Spencer Ackerman, *NSA Goes on 60 Minutes: The Definitive Facts Behind CBS' Flawed Report*, GUARDIAN, Dec. 16, 2013, http://www.theguardian.com/world/2013/dec/16/nsa-surveillance-60-minutes-cbs-facts. James Bamford has reported that government agencies are siphoning off content as well. *See* Bamford, *The Black Box*, *supra* note 3, at 84. Recent revelations of the NSA's unauthorized infiltration of server networks maintained by Google and Yahoo as part of the "clouds" in which they store customers' documents and communications support Bamford's reportage. Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide*, WASH. POST, Oct. 30, 2013, at A1, *available at* http://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d66 1e-4166-11e3-8b74-d89d714ca4dd_story.html.

9. Roberts & Ackerman, *supra* note 6.

10. *Id.*

11. Barton Gellman & Laura Poitras, *U.S. Mines Internet Firms' Data, Documents Show*, WASH. POST, June 7, 2013, at A1, *available at* http://www.washingtonpost.com/investiga

program, the NSA has also surreptitiously tapped into the physical components of these companies' cloud computing networks, gaining access to unencrypted user data transmitted between secure data centers.[12] A third program, dubbed XKeyscore, provides government analysts with the capacity to mine content and metadata generated by email, chat, and browsing activities through a global network of servers and internet access points operated by private entities.[13]

These leaked documents confirm previous reports about a comprehensive domestic surveillance program that has been underway at least since the terrorist attacks of September 11, 2001.[14] The current revelations go much farther, however, providing credible evidence that government agencies are collecting not only "metadata," but also the contents of all electronic communications that travel through infrastructure located in the United States or one of its partner nations.[15] Although seemingly fantastic, it is increasingly difficult to discount accounts of such programs. All the more so in light of the fact that the NSA is in the process of building massive data centers capable of storing petabytes of information.[16] Why, after all, would the federal government's premier signals spy agency need such facilities if it was not engaged in a commensurably massive data collection effort? Thus, it is a fairly safe bet that the government is already, or soon will be, collecting and retaining all of our electronic and telephonic communications, providing government agents with contemporary and perpetual access to details about everywhere we go and everything we do, say, or write when using or in the company of technology.[17]

---

tions/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html.

12. Gellman & Soltani, *supra* note 8, at A1.

13. Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* GUARDIAN, July 31, 2013, http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data.

14. *See* THE SHADOW FACTORY, *supra* note 3, at 177-96; Bamford, *The Black Box*, *supra* note 3; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1, *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all; Michael Isikoff, *The Fed Who Blew the Whistle*, NEWSWEEK (Dec. 12, 2008), *available at* http://www.thedailybeast.com/newsweek/2008/12/12/the-fed-who-blew-the-whistle.html.

15. *See* sources cited *supra* notes 11-13; THE SHADOW FACTORY, *supra* note 3, at 212-33.

16. *See* Bamford, *The Black Box*, *supra* note 3, at 80, 82-83.

17. *See id.* at 84; Isikoff, *supra* note 14; Risen & Lichtblau, *supra* note 14.

As unsettling as these massive electronic surveillance programs are, they are merely one branch of the rapidly expanding surveillance state in which we live. Our public spaces are being overtaken by a growing archipelago of observation systems deployed for public and private security, traffic control, environmental monitoring, and innumerable other purposes.[18] They are mounted to buildings, utility poles, cars, and sometimes people.[19] They are transported through the ether on unmanned drones.[20] Once kept in silos, the inputs from these sources increasingly are aggregated and analyzed by a nationwide network of fusion centers and local law enforcement efforts like New York City's Domain Awareness System, developed in collaboration with Microsoft,[21] or Virtual Alabama, which has been developed by Google with its state partner.[22] The inevitable end, if not the intent and purpose, seems to be constant and pervasive observation of everywhere we go, and everything we do, in public spaces.

Much of this expanding surveillance state intersects with or depends on private entities. The internet and portable electronic devices have become ubiquitous and play an increasingly central role in almost every aspect of our lives.[23] These technologies require us to share a vast amount of information with third parties.[24] We cannot buy things using credit cards without sharing vendor information.[25] Whether we are using landlines or

---

18. David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 63-72 (2013).

19. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1450-52 (2011) (noting that fusion centers, where federal and state analysts share intelligence data, routinely look at everything from traffic tickets and credit reports to video clips submitted by citizens).

20. *See* Lev Grossman, *Drone Home*, TIME MAG., Feb. 11, 2013, at 28, 31-33; Jennifer Lynch, *Are Drones Watching You?*, ELEC. FRONTIER FOUND. (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you. In the United States, "approximately 50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs." Lynch, *supra*. In 2010, expenditures on unmanned aircraft in the United States exceeded three billion dollars and are expected to surpass seven billion dollars over the next ten years. *Id.*

21. Gray & Citron, *supra* note 18, at 65-66.

22. *Id.* at 66-67.

23. *See* United States v. Jones, 132 S. Ct. 945, 963 (2012) (Alito, J., concurring).

24. *Id.* (Alito, J., concurring).

25. *Cf.* United States v. Miller, 425 U.S. 435, 440-43 (1976) (holding that bank customers cannot raise a Fourth Amendment bar against government subpoena for bank records documenting their transactions because banks and their customers are parties to the underlying transactions, and customers must share information about those transactions with their banks in order for the banks to perform their roles).

cellular phones, we cannot make or receive calls without sharing call details with our service providers,[26] including our locations.[27] Many of the apps and concierge services we use on our phones, tablets, and computers cannot function without knowing where we are.[28] We cannot search or surf the web without our search engines' and internet service providers' knowing what we look for and where we go. Email services search the content of our email in order to target us for the advertisements that subsidize their services.[29] Many web pages install cookies on our computers, or use other tracking mechanisms, and then auction visual space in our browsers to competing advertisers.[30] We post to social networking sites. We blog. We tweet. In short, there is an almost constant stream of data between us and the corporate world, most of which goes unrecognized[31] or unappreciated until we receive an eerily insightful solicitation.[32]

Although few, if any, of us really grasp how much information we share with institutional third parties, or know what they do with that information, our naïveté is periodically challenged. For example, in a frequently discussed article, the New York Times reported in 2012 that the retailer Target uses information purchased from third parties in combination with proprietary consumer data to identify newly pregnant women.[33] Target then, well, targets these women, sending coupons and offers for pregnancy

---

26. Smith v. Maryland, 442 U.S. 735, 744 (1979).

27. *See* 47 C.F.R. § 20.18(h)(1) (2014) (requiring cell phone carriers to use cell tower information or GPS technology to locate phones that make 9-1-1 calls on their networks).

28. One example is the popular social networking site Foursquare, which gives recommendations for services based on users' current location. *See About Foursquare*, FOURSQUARE, https://foursquare.com/about (last visited Apr. 10, 2014).

29. For example, this is the business model for Google's Gmail service. *See Ads in Gmail*, GOOGLE, https://support.google.com/mail/answer/6603?hl=en (last visited Apr. 10, 2014).

30. *See, e.g.*, *Ad Targeting*, GOOGLE, https://support.google.com/adsense/answer/160525?hl=en (last visited Apr. 10, 2014) (explaining the purpose and function of Google's Adwords).

31. For example, as Jennifer Golbeck reported recently, Facebook uses the content of draft and unpublished posts to target advertisements. Jennifer Gollacek, *On Second Thought . . .*, SLATE (Dec. 13, 2014), *available at* http://www.slate.com/articles/technology/future_Tense2013/12/facebook_self_censorship_what_happens_to_the_posts_you_don_t_publish.html.

32. *See* Charles Duhigg, *Psst, You in Aisle 5*, N.Y. TIMES, Feb. 19, 2012, at MM30, *available at* http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (recounting how Target uses publicly available databases and market analytics to identify women who are in the early stages of pregnancy).

33. *Id.*

and baby products.[34] In one of the cases reported by the Times, Target's marketing efforts notified a customer's family that she was pregnant before she did.[35] Many of us have similar, though more routine, moments of recognition when we see advertisements in our browsers pressing products we looked at days or weeks earlier; or we receive word from vendors thanking us for our interest in items we were linked to through an email earlier in the day.

Roger Clarke foresaw the rise of this practice, which he dubbed "dataveillance," in the late 1980s.[36] He would have categorized much of the contemporary use of data in commerce as "personal" in so far as it focuses on conduct that engages the attention of particular information consumers.[37] Clarke would categorize the more diffuse, and largely indiscriminate, data gathering engaged in by the NSA as "mass dataveillance."[38] These sorts of practices, often dubbed "Big Data" by contemporary scholars, seek to gather as much information as possible with the hope that subsequent analysis may reveal suspicious patterns of events or even persons of interest.[39] Here, the NSA is not alone. The National Counterterrorism Center recently secured authority to gather from third parties a broad range of information on every airline passenger entering the United States, including travel history, financial data, and even medical records.[40] Under authority granted by the Affordable Care Act, passed in 2012, the Department of Health and Homeland Security, along with its designees, can now require that agencies and healthcare providers collect and report a wide range of patient information, including "race, ethnicity, sex, primary language, and disability status."[41] Of course, government is not the only Big Data player. Private data aggregators like Acxiom, who have been dubbed "Big Brother's Little Helpers" by Chris Hoofnagle, buy

---

34. *Id.*

35. *Id.*

36. Roger A. Clarke, *Information Technology and Dataveillance*, 31 COMMC'NS OF ACM 498, 498 (1988).

37. *Id.* at 502-03.

38. *Id.* at 503-04.

39. *See* David Gray, Danielle Keats Citron & Liz Clark Rinehart, *Fighting Cybercrime After* United States v. Jones, 103 J. CRIM. L. & CRIMINOLOGY 745, 765-83 (2013).

40. Julia Angwin, *U.S. Terror Agency to Tap Citizen Files*, WALL ST. J., Dec. 13, 2012, at A1.

41. The Patient Protection and Affordable Care Act, Pub. L. No. 111-148, § 3101, 124 Stat. 119, 579 (2010) (codified at 42 U.S.C. § 300kk (2012)); *see also* Gray, Citron & Rinehart, *supra* note 39, at 765-70; Frank Pasquale, *Grand Bargains for Big Data: The Emerging Law of Health Information*, 72 MD. L. REV. 682, 683, 687 (2013).

and collect mass quantities of information from a range of private and public sources, which they then package and sell.[42]

There is no doubt that dataveillance, whether mass or personal, can serve important governmental and commercial purposes.[43] For example, Big Data in the healthcare arena has the potential to facilitate medical research,[44] epidemiological forecasting,[45] and efforts to combat fraud.[46] It also raises serious privacy concerns. As the breadth and scope of data gathering and aggregation grow, the potential for bad information to leak into the system increases.[47] Given the high degree of data sharing and largely uncritical interpenetration of databases,[48] these errors can be quite consequential for citizens, affecting their abilities to borrow, buy, or travel, and sometimes harming their job prospects.[49] Accurate and reliable dataveillance may be even more dangerous, however.[50] As Justice Sotomayor has pointed out, granting government "unfettered discretion"[51] to gather "comprehensive record[s]"[52] that disclose details of "familial, political, professional, religious, and sexual associations,"[53] "chills associational and expressive freedoms"[54] while "alter[ing] the relationship between citizen and government in a way that is inimical to a democratic society."[55] It also raises fearsome specters of a surveillance state, leading many commentators to draw vivid analogies to literary dystopias.[56]

---

42. Hoofnagle, *supra* note 5, at 595-96.

43. *See* Gray, Citron & Rinehart, *supra* note 39, at 765-800.

44. *See* Pasquale, *supra* note 41, at 683

45. Jody Ray Bennett, *The Big Data Contagion*, DATAVERSITY (June 21, 2012), http://www.dataversity.net/the-big-data-contagion/.

46. *See* Gray, Citron, & Rinehart, *supra* note 39, at 770-82.

47. Gray & Citron, *supra* note 18, at 80-81.

48. *Id.* at 119-20; Citron & Pasquale, *supra* note 19, at 1443.

49. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1273-77 (2008).

50. Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 2 (2008) ("Government's most important technique of control is no longer watching or threatening to watch. It is analyzing and drawing connections between data."); Gray & Citron, *supra* note 18, at 82.

51. United States v. Jones, 132 S. Ct. 945, 954-56 (2012) (Sotomayor, J., concurring).

52. *Id.* at 955 (Sotomayor, J., concurring).

53. *Id.* (Sotomayor, J., concurring).

54. *Id.* at 956 (Sotomayor, J., concurring).

55. *Id.* (Sotomayor, J., concurring) (quoting United States v. Cuevas-Perez, 640 F.3d 272, 285 (7th Cir. 2011) (Flaum, J., concurring)).

56. Gray & Citron, *supra* note 18, at 76 n.88 (quoting GEORGE ORWELL, NINETEEN EIGHTY-FOUR 4 (1949)); Roberts & Ackerman, *supra* note 6 (quoting the ACLU's Jameel Jaffer as characterizing the NSA's telephonic surveillance program as being "beyond

Given these privacy concerns, one might expect that the Fourth Amendment, which guards "reasonable expectation[s] of privacy,"[57] would impose some constraints on the government's ability to engage in dataveillance. Under present doctrine, however, it does not. This is due primarily to a long line of cases standing for the general proposition that, when you share information with others, you assume the risk that those whom you trust will pass it along to the government, whether on their own initiative or in response to a subpoena, warrant, or other "lawful process."[58] Although one member of the Court is ready to reconsider this "third party doctrine" in light of governmental efforts to engage in mass data collection and aggregation,[59] the Court has yet to take up the question.[60] In the meantime, government agents continue to exploit the third party doctrine to facilitate their expanding surveillance programs. It is precisely this lacuna

---

Orwellian"); *cf.* Florida v. Riley, 488 U.S. 445, 466 (1989) (Brennan, J., dissenting) ("The Fourth Amendment demands that we temper our efforts to apprehend criminals with a concern for the impact on our fundamental liberties of the methods we use. I hope it will be a matter of concern to my colleagues that the police surveillance methods they would sanction were among those described 40 years ago in George Orwell's dread vision of life in the 1980's."); Bill Keller, Op-Ed., *Living with the Surveillance State*, N.Y. TIMES, June 17, 2013, at A17, *available at* http://www.nytimes.com/2013/06/17/opinion/keller-living-with-the -surveillance-state.html (likening the Domain Awareness System, an interconnected system of CCTV cameras and law enforcement databases in Britain, to Orwell's "Big Brother" of *Nineteen Eighty-Four*).

57. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

58. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 741-42 (1979); United States v. Miller, 425 U.S. 435, 440-43 (1976); Cal. Bankers Ass'n v. Shultz, 416 U.S. 21, 55 (1974); United States v. White, 401 U.S. 745, 777 (1971); Hoffa v. United States, 385 U.S. 293, 302 (1966). As is common in this area of Fourth Amendment law, the Standards overstate the rule described by the third party doctrine, which surely does not provide that "one typically retains no federal constitutional reasonable expectation of privacy in information conveyed to a third party." *See* ABA STANDARDS FOR CRIMINAL JUSTICE: LAW ENFORCEMENT ACCESS TO THIRD PARTY RECORDS 6 (3d ed. 2013) [hereinafter LEATPR STANDARDS]. Individual standards will be referred to using the format 'STANDARD x.x.' Were this the rule then *Katz* would have been wrongly decided—after all, Katz did by definition share everything overheard by the government's electronic listening device with the parties to his phone calls. *Katz*, 389 U.S. at 348.

59. *Jones*, 132 S. Ct. at 957 (Sotomayor, J., concurring).

60. There are several lawsuits working their way through the courts that may present the Court with an opportunity to reconsider the third party doctrine. *See, e.g.*, ACLU v. Clapper, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013) (finding that the NSA's telephony metadata collection program is constitutional under the third- party doctrine); Klayman v. Obama, 957 F. Supp. 2d 1, 37 (D.D.C. 2013) (finding that the NSA's telephony metadata collection program is unconstitutional despite the third party doctrine).

that the ABA Standards for Criminal Justice on Law Enforcement Access to Third Party Records (LEATPR Standards) propose to span.

Recognizing the privacy implications of dataveillance, and even governmental access to discrete, but revelatory, bits of personal data, the LEATPR Standards propose super-constitutional constraints on law enforcement access to information held by institutional third parties. These efforts are neither unprecedented nor unwelcome.[61] Since its inception, the third party doctrine has been a point of considerable concern for citizens and scholars alike.[62] In the face of those worries, the political branches have taken action to guarantee some degree of privacy in certain shared information, even if the Constitution guarantees none. For example, in the face of concerns about the use of pen register devices, which were sanctioned by the Court in *Smith v. Maryland*,[63] Congress passed the Pen Register Act[64] as part of the Electronic Communications Privacy Act of 1986 (ECPA).[65] Among its more important provisions, the Pen Register Act limits telephone companies' use of these devices for their own purposes and imposes a requirement for a court order for any law enforcement use.[66] In the wake of concerns about the disclosure of video rental histories raised during the confirmation proceedings for Supreme Court nominee Robert Bork, Congress passed the Video Privacy Protection Act (VPPA).[67] The VPPA requires that video rental businesses maintain the privacy of their customers' viewing habits and interposes courts between law enforcement and video rental companies.[68]

In contrast to these past efforts, we have yet to see any significant legislative reactions to growing concerns about dataveillance and

---

61. For examples of extra-constitutional legislative constraints on law enforcement surveillance efforts, see *infra* notes 64-68. For prior examples of ABA model standards, see ABA STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE SECTION A: ELECTRONIC SURVEILLANCE OF PRIVATE COMMUNICATIONS (3d ed. 2001); ABA STANDARDS FOR CRIMINAL JUSTICE, ELECTRONIC SURVEILLANCE SECTION B: TECHNOLOGICALLY-ASSISTED PHYSICAL SURVEILLANCE (3d ed. 1999).

62. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the 'Legitimate Expectation of Privacy'*, 34 VAND. L. REV. 1289, 1314-15 (1981).

63. 442 U.S. at 745-46.

64. Pen/Trap Statute (Pen Register Act), Pub. L. No. 99-508, Title III, 100 Stat. 1868 (1986) (codified at 18 U.S.C. §§ 3121-3127 (2012)).

65. Pub. L. No. 99-508, 100 Stat. 1848 (codified in scattered sections of 18 U.S.C.).

66. 18 U.S.C. § 3121 (2012).

67. Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2012)).

68. 18 U.S.C. § 2710(b)(2)(C).

widespread government access to data shared with third parties. Although some judges and scholars hold out hope that Congress will step in,[69] it has yet to do so in any meaningful way. Even in the face of recent revelations about general warrants for telephonic metadata,[70] which were issued by the Foreign Intelligence Surveillance Court to the FBI and NSA under the auspices of the Foreign Surveillance Intelligence Act, there seems to be little interest in establishing new constraints, despite calls by a small minority of legislators.[71] Other commentators hope that the executive will restrain itself, but there is very little reason to think that it can or will given current efforts by the FBI and NSA to defend their widespread data gathering and to avoid any meaningful outside review.[72]

In the face of these legislative, executive, and judicial failures, the LEATPR Standards are agnostic as to which regime[73]—legislative, executive, or judicial—should bear the burden of action. They instead try to chart a regulatory structure that conceivably could be adopted and implemented as part of a judicial order, a legislative enactment, or an executive policy.[74] As a consequence, the Standards do not take a position on whether current data-sharing practices between institutional third parties and law enforcement raise any constitutional concerns. Rather, they start from the premise that there is something creepy going on and then take a

---

69. *E.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring); Orin Kerr, *Technology, Privacy, and the Courts: A Reply to Colb and Swire*, 102 MICH. L. REV. 933, 943 (2004).

70. Gray & Citron, *supra* note 18, at 119.

71. The exception is the Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013) & H.R. 1847, 113th Cong. (2013), which would require police to get a warrant for production of information and to provide notice to those whose records were sought. The Bill was reported out of the Senate Judiciary Committee on April 25, 2013, but has yet to clear the House Committee. None of the revelations about NSA and FBI surveillance and dataveillance in the intervening months seem to have moved the ball.

72. Not surprisingly, this is the approach advocated by the NSA. *See In re* Application of F.B.I. for an Order Requiring Prod. of Tangible Things from [Redacted], No. BR 13-80, at 3-6 (Foreign Intelligence Surveillance Ct. Apr. 25, 2013) (describing "minimization" procedures adopted within the NSA and FBI to limit access to and use of telephonic metadata). For a discussion of these procedures, see Gray & Citron, *supra* note 18, at 119-23.

73. I take this use of "regime" from Akhil Amar, who has long pressed for each of the three constitutional branches of government, or regimes, to do its part in protecting Fourth Amendment rights. AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 43-45 (1997).

74. STANDARD 25-3.4.

brave stab at both describing and addressing that creepiness without taking any position on whether or how the Constitution is implicated.

Although there is broad agreement that there is *something* creepy about the expanding scope of government's access to the products of data aggregation and discrete surveillance performed by third parties, that consensus quickly falls apart once one starts to focus on *why* it is creepy and *what can or should be done*. Some think that "creepy" is as far as it goes, and that contemporary norms, commerce, economics, and the realities of modern politics augur against any governmental intervention.[75] Others argue that programs of broad governmental surveillance, whether accomplished directly or through third parties, is socially destructive and constitutionally infirm.[76] While stopping well short of hysteria, the Standards take seriously the impact on privacy of expanding data-sharing relationships between the government and private parties.[77] Nothing that follows in this essay will attempt to dissuade contributors and consumers from this view. Rather, it will argue that the approach taken by the Standards is conceptually and practically fraught.

Although far too short to provide a conclusive case, this essay will argue that the LEATPR Standards adopt a strategy that is likely to fail and instead promote a regulatory framework that poses serious threats to core interests in individual liberty and functioning democracy that lie behind privacy claims. The strategic error is located in the Standards' refusal to find some constitutional ground that might demonstrate the necessity and sufficiency of its provisions. Part II provides a brief overview of some of the critical decisions reflected in the Standards. Parts III and IV explore the consequences of these choices. Part V turns to the regulatory framework proposed by the Standards and focuses in particular on the decision to govern access to information held by third parties according to a spectrum of privacy interests, which ranges from "highly private" to "not private."[78] Although this approach has a certain intuitive appeal, the project of describing these categories and assigning values to information poses a serious threat to individual autonomy, political neutrality, and democratic norms. In the end, these criticisms are self-defeating. After all, it is hard to get too spun up about the dangers of a regulatory framework that is doomed never to be adopted in the first place. They are offered here nevertheless in

75. Kerr, *supra* note 69, at 943.
76. Gray & Citron, *supra* note 18, at 101-24.
77. LEATPR STANDARDS, *supra* note 58, at 4-5.
78. *Id.* at 9-11.

the hope that they may be of some assistance to those seeking to step into the regulatory fray as they consider other alternatives.[79]

II. An Overview of the LEATPR Standards' Basic Approach

As a prelude to the discussion that follows, it is worth highlighting a few features of the LEATPR Standards that raise some concerns. The first of these is the Standards' agnosticism with respect to constitutional issues.[80] The Standards' Introduction emphasizes this posture, pointing out that "the Standards do not purport to interpret the federal constitution nor any state equivalent, nor the many statutes and administrative regulations that regulate law enforcement access to third party records."[81] Thus, the Standards do not challenge the third party doctrine or otherwise tether the project of general reform, or the specific provisions set forth by the Standards, to any constitutional theory. This agnosticism raises two very important issues and potential points of concern.

The first is the question of constitutional sufficiency. Standard 25-2.2 makes clear that any efforts to adopt and apply the Standards, in whole or in part, cannot "authorize a protection less than that required by the federal Constitution, nor less than that required by its respective state Constitution."[82] Although considerate,[83] this provision just highlights the possibility that the Standards are constitutionally infirm. As we shall see in a moment, this is a significant worry in present circumstances, where new technologies and expanding surveillance regimes have opened the third party doctrine, the public observation doctrine, and other seemingly well-established Fourth Amendment rules to new constitutional challenges.

---

79. Among these is a proposal that Danielle Citron and I have advanced, which would focus on regulating the technologies that are used to facilitate programs of dataveillance. Gray & Citron, *supra* note 18, at 101-24.

80. *See* LEATPR STANDARDS, *supra* note 58, at 9 ("Fortunately, it is not necessary for purposes of these Standards to answer these constitutional questions."). It appears that this agnosticism reflects a decision by the ABA rather than the drafters, at least some of whom sought to ground the Standards in claims of constitutional necessity. Stephen Henderson, Professor, University of Oklahoma College of Law, Remarks at the Oklahoma Law Review Symposium: Law Enforcement Access to Third Party Records (Nov. 15, 2013). Perhaps the points made here will be of some assistance in persuading the ABA to change its view when and if the Standards are considered for review and revision.

81. *Id.* at 9.

82. STANDARD 25-2.2.

83. Standard 25-2.2 is gratuitous, after all. By definition, the Standards could never hope to justify legislation or administrative practice that is constitutionally deficient.

The second concern derived from the Standards' constitutional agnosticism is the question of constitutional necessity. Returning to Standard 25-2.2, the Standards do not take a position on what protections are or should be demanded by federal or state constitutions. For example, the Standards do not challenge the third party doctrine or imply a constitutionally grounded expectation of privacy in information shared with third parties, whether that information is "highly private" or only "moderately private."[84] As a consequence, the Standards provide no constitutional impetus for either the project or its components, relying instead on the political process to carry the full mantle of motive and action. As is discussed below, there is very good reason to doubt that the Standards will have any effect if their fate is left to legislatures and executives. Although public responses to recent revelations about NSA surveillance raise some hope that the political will to adopt rules along the lines described by the Standards may be there, persistent linkages between surveillance and national security make it hard to be too sunny in the context of our perpetual war on terror. Those concerns are particularly salient given the Standards' specific refusal to regulate any governmental efforts to access third party records in the context of national security investigations.[85] That exclusion may well render the whole project academic in the most pejorative sense of the word.

These concerns are amplified by the fact that the Standards take no position on who should be the prime mover in promoting reform. Among those who think that the gathering and sharing of personal information by third parties should be regulated, there is considerable disagreement about who is best placed to develop and enforce regulations. Some think that the market should take the lead, with companies competing for consumers based in part on how much data they gather, how long they keep it, how they share it, and how vigorously they contest government attempts to gain access.[86] Others favor the political branches, and legislatures in

84. STANDARD 25-4.1.

85. STANDARD 25-2.1(a).

86. For example, this perspective is at the heart of the "do not track" movement in browser technology, which has been driven largely by consumer demand. *See* FED. TRADE COMM'N, PRELIMINARY STAFF REPORT: PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS 63-69 (2010), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-bureau-consumer-protection-preliminary-ftc-staff-report-protecting-consumer/101201privacyreport.pdf.

particular.[87] Some maintain that the privacy issues rise to a constitutional level, and therefore require court intervention—if only to force sluggish elected officials to action.[88] The Standards remain agnostic on these questions as well.[89] Thus, the Standards are offered as a framework that could be adopted by "legislatures, courts acting in their supervisory capacities, [or] administrative agencies."[90]

The final feature of the Standards that will guide the discussion here is their focus on the contents of third party records sought by government agents rather than other regulatory targets. Even among those who agree on the best forum for regulation, there is considerable disagreement on what approach to take. Some have focused on how much data is gathered or shared.[91] Others have focused on how long surveillance is conducted.[92] Among the more prominent proponents of these "quantitative" approaches are Christopher Slobogin[93] and the four justices who joined Justice Alito's concurring opinion in *United States v. Jones*.[94] A third group has made the case for focusing on how surveillance is accomplished. With my coauthor Danielle Citron, I have made the case for this method-centered approach, which would regulate both direct and indirect governmental access to and use of surveillance and data aggregation technologies capable of effecting broad programs of indiscriminate surveillance.[95] A fourth group of scholars

87. United States v. Jones, 132 S. Ct. 945, 964 (Alito, J., concurring); Kerr, *supra* note 69, at 943.

88. Gray & Citron, *supra* note 18, at 69-70, 112.

89. LEATPR STANDARDS, *supra* note 58, at 9 ("Fortunately, it is not necessary for purposes of these Standards to answer these constitutional questions. Although decision makers will of course be bound by constitutional decisions (see Standard 25-2.2), the Standards do not purport to interpret the federal constitution nor any state equivalent, nor the many statutes and administrative regulations that regulate law enforcement access to third party records. They instead carefully consider all of these, and other sources, in providing a framework via which decision makers, including legislatures, courts acting in their supervisory capacities, and administrative agencies, can answer such questions, thereby thoughtfully and consistently regulating government access to third party records.").

90. *Id.*

91. This "mosaic" theory is credited to Judge Ginsburg's opinion for the United States Court of Appeals for the District of Columbia Circuit in *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

92. 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).

93. *Id.*

94. United States v. Jones, 132 S. Ct. 945, 962-64 (2012) (Alito, J., concurring).

95. Gray & Citron, *supra* note 18.

and policy makers argues that regulations should focus on what kinds of data and information are gathered and shared.[96] For example, Neil Richards has argued that we should be most concerned with surveillance that gathers information implicating "intellectual privacy."[97] The Standards also favor this content-based approach. As we shall see, there are good reasons to worry that this choice may compromise core commitments to individual liberty, among other core democratic principles.[98]

III. The Consequences of Constitutional Agnosticism

Although there are many historical narratives explaining the current state and history of Fourth Amendment law and doctrine, one of the most compelling is the courts' deployments of Fourth Amendment principles and applications of founding-era analogies to address changes in law enforcement practice and advancing surveillance technology. Take, for examples, the exclusionary rule and the *Katz* doctrine. During the founding era, and well into the nineteenth century, there were no professionalized police forces.[99] Law enforcement was largely motivated by private action with minimal assistance provided by constables, who were more often criticized for their sloth than for their aggressive search and seizure practices.[100] Although colonials had experience with writs of assistance, these general warrants were used largely to facilitate tax enforcement and trade policy rather than to advance general law enforcement purposes or for government intelligence gathering.[101] As a consequence, the sorts of police conduct that concern us today—invasive home searches, routine searches and seizures on the street, ex parte custodial interrogations, widespread surveillance, and ubiquitous dataveillance—were not part of the American

96. *See* State v. Earls, 70 A.3d 630, 641-43 (N.J. 2013).

97. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1935-36 (2013); Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 403-04 (2008).

98. Danielle Citron and I have made this case against Professor Richards. *See* Danielle Keats Citron & David Gray, *Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards*, 126 HARV. L. REV. F. 262 (2013).

99. Thomas Y. Davies, *Recovering the Original Fourth Amendment*, 98 MICH. L. REV. 547, 620-21 (1999); Wesley MacNeil Oliver, *The Neglected History of Criminal Procedure*, 1850-1940, 62 RUTGERS L. REV. 447, 447-48 (2010); Carol S. Steiker, *Second Thoughts About First Principles*, 107 HARV. L. REV. 820, 824 (1994).

100. *See* Davies, *supra* note 99, at 641; Oliver, *supra* note 99, at 452, 456; Lawrence Rosenthal, *Pragmatism, Originalism, Race, and the Case Against* Terry v. Ohio, 43 TEX. TECH. L. REV. 299, 342 (2010) (quoting ROGER LANE, POLICING THE CITY: BOSTON 1822-1885, at 6-7 (1967)).

101. Oliver, *supra* note 99, at 450, 456-57.

imagination in 1791. It is therefore impossible to make the case that the Fourth Amendment originally was intended or understood to curb police excesses. There simply were no police forces of any consequence and therefore no serious excesses to curb. The landscape began to change in the mid-nineteenth century as urban centers like New York City began to incorporate professional, paramilitary-style police forces and to endow those forces with broad authority to use force and violence in the service of detecting, preventing, and prosecuting crime.[102] Police units quickly became institutions unto themselves, described by enterprise goals, populated by careerists, and vulnerable to political manipulation and corruption.[103] What followed was an era of expanding police departments, increasing police powers, and more invasive and oppressive police practices, including searches, detentions, and "third-degree" interrogations.[104]

Faced with these dramatic changes, courts started to take action. The primary result was a series of cases, beginning with *Boyd v. United States*[105] in 1886 and culminating in *Mapp v. Ohio*[106] in 1961, in which courts at both the federal and state levels began excluding from trial evidence that was found or seized in violation of the Fourth Amendment. Courts adopting this new exclusionary rule justified their actions on grounds of both constitutional principle and pragmatic necessity.[107]

There is little doubt that the exclusionary rule represented a significant doctrinal novation. Prior to 1886, there is no persuasive evidence that the prospect of excluding otherwise reliable evidence acquired as a result of an illegal search or seizure garnered any sympathy in American courts.[108]

---

102. *Id.* at 448, 459.

103. *Id.* at 459-60, 493.

104. The widely influential Wickersham Report, which the Court relied on in *Miranda v. Arizona*, 384 U.S. 436, 445-47 (1966), defines the "third degree" as "the use of physical brutality, or other forms of cruelty, to obtain involuntary confessions or admissions." 11 NAT'L COMM'N ON LAW OBSERVANCE & ENFORCEMENT, REPORT ON LAWLESSNESS IN LAW ENFORCEMENT 4 (1931).

105. 116 U.S. 616 (1886).

106. 367 U.S. 643 (1961).

107. David Gray, *A Spectacular Non Sequitur: The Supreme Court's Contemporary Fourth Amendment Exclusionary Rule Jurisprudence*, 50 AM. CRIM. L. REV. 1, 13-19 (2013).

108. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786-87 (1994) (quoting United States v. La Jeune Eugenie, 26 F. Cas. 832, 843-44 (C.C.D. Mass. 1822); Commonwealth v. Dana, 43 Mass. (2 Met.) 329, 337 (1841) ("If the search warrant were illegal, or if the officer serving the warrant exceeded his authority, the party on whose complaint the warrant issued, or the officer, would be responsible for the wrong done; but this is no good reason for excluding the papers seized as evidence, if they

Rather, it arrived on the scene only in response to changes in the nature of law enforcement, the scope of police powers, and the increasing invasiveness of police practices.[109] The exclusionary rule marks the courts' response to these changes and to the persistent inability of the political branches to regulate police conduct with any sustained effectiveness. As the Court reported in *Elkins v. United States*, "neither administrative, criminal nor civil remedies are effective in suppressing lawless searches and seizures."[110] By contrast, the exclusionary rule had almost immediate salutary effects when and where it was adopted, reducing Fourth Amendment violations, increasing training and therefore the professionalism of police officers, and expanding engagements between law enforcement and prosecutors.[111]

The exclusionary rule was and remains controversial, of course. It is also persistently targeted by several current justices on the Supreme Court.[112] We can leave these debates aside for the moment, however, and simply take note of the historical fact that the exclusionary rule marks a doctrinal adaptation to changes in the nature of law enforcement institutions, their powers, and their practices. Absent those changes, we likely would not have an exclusionary rule at all; and, absent the exclusionary rule, we likely would live in a world where illegal searches and other abuses of power were far more common. To see some of what that world might look like, we need look no further than fields of police-citizen engagements liberated from serious court scrutiny by those exceptions to the exclusionary rule that contribute to what I have described

---

were pertinent to the issue, as they unquestionably were.")). As Akhil Amar has pointed out, the exclusive remedies for illegal searches and seizures prior to 1886 were to be found in common law trespass. *Id.* at 774; *see also id.* at 787 ("As late as 1883, the leading evidence treatise clearly proclaimed illegally procured evidence admissible . . . ."); William C. Heffernan, Foreword, *The Fourth Amendment Exclusionary Rule as a Constitutional Remedy*, 88 GEO. L.J. 799, 808 (2000) (noting the Court's departure from the common law trespass as the exclusive remedy for illegal searches and seizures); Potter Stewart, *The Road to* Mapp v. Ohio *and Beyond: The Origins, Development and Future of the Exclusionary Rule in Search-and-Seizure Cases*, 83 COLUM. L. REV. 1365, 1372-77 (1983) (same). Roger Roots recently has disputed this common wisdom in *The Originalist Case for the Fourth Amendment Exclusionary Rule*, 45 GONZ. L. REV. 1 (2010). For a brief critique of his views, see Gray, *supra* note 107, at 14 n.82.

109. *See id.* at 13-26.

110. 364 U.S. 206, 220 (1960) (quoting People v. Cahan, 282 P.2d 905, 913 (Cal. 1955)).

111. *Id.* at 219-21.

112. *See* Gray, *supra* note 107, at 16-21.

elsewhere as the Court's contemporary silver platter doctrine.[113] These include grand jury investigations,[114] immigration enforcement,[115] civil tax proceedings,[116] and parole enforcement.[117] In each of these arenas, we can see both examples of unchecked Fourth Amendment violations and the threat and potential for more widespread abuses.

The rule announced in *Katz v. United States* reinforces this narrative of doctrinal adaptation to historical changes in police power and practice.[118] Although not specified in the text of the Fourth Amendment, for at least a century after ratification, "search" was understood in reference to concepts of common law trespass.[119] As a consequence, Fourth Amendment rights were tied to property rights.[120] On this point, *Olmstead v. United States* is most often cited.[121] There, the Court held that intercepting telephone conversations using wiretapping technology did not constitute a Fourth Amendment "search" because deploying and using that technology did not require a physical invasion of the home.[122]

The Court's views on wiretapping began to shift over the next several decades, both as telephones became a more common feature of daily life and as wiretapping took a more prominent place in the law enforcement toolbox.[123] That shift culminated with *Katz* in 1967.[124] There, the Court

---

113. David Gray, Meagan Cooper, & David McAloon, *The Supreme Court's Contemporary Silver Platter Doctrine*, 91 TEX. L. REV. 7 (2012).

114. *Id.* at 21-25.

115. *Id.* at 25-36.

116. *Id.* at 46.

117. *Id.* at 36-46.

118. 389 U.S. 347 (1967).

119. United States v. Jones, 132 S. Ct. 945, 949 (2012) ("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."); *see also* Slobogin, *supra* note 92, at 3-4. *But see* Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2012 SUP. CT. REV. 67, 68-69 (arguing that the trespass test of Fourth Amendment searches is a myth created by the Court in *Katz*).

120. Amar, *supra* note 108, at 786.

121. 277 U.S. 438 (1928), *overruled by Katz*, 389 U.S. 347.

122. *Id.* at 466. In a spirited dissent, Justice Brandeis argued that this property-based approach to the Fourth Amendment was anachronistic. *Id.* at 473-74 (Brandeis, J., dissenting). That dissent drew on work that Justice Brandeis did in his groundbreaking article *The Right to Privacy*, 4 HARV. L. REV. 193 (1890), which he co-wrote with Samuel D. Warren.

123. *Olmstead*, 277 U.S. at 471-79 (Brandeis, J., dissenting); Oliver, *supra* note 99, at 460-61; *see also* DAVID R. JOHNSON, POLICING THE URBAN UNDERWORLD: THE IMPACT OF CRIME ON THE DEVELOPMENT OF THE AMERICAN POLICE, 1800-1887, at 4-9, 29-40 (1979).

concluded that "the underpinnings of *Olmstead* . . . [had] been so eroded . . . that the 'trespass' doctrine there enunciated can no longer be regarded as controlling."[125] In its place, the Court adopted the view that the Fourth Amendment "protects people, not places,"[126] and formulated a new definition of "search" organized around reasonable expectations of privacy.[127] Under this standard, the Court held that surreptitiously listening to telephone conversations constitutes a "search" because citizens reasonably expect that those conversations are private.[128]

Like the exclusionary rule, the *Katz* doctrine marks an adaptation of constitutional doctrine to changes in law enforcement and society that has no doubt had significant salutary effects on the relationships between citizens and law enforcement. Just to cite one example, *Katz* impelled adoption of the Wiretap Act.[129] Absent *Katz*, the concept of the Fourth Amendment search likely would remain limited by the law of trespass,[130] and the use of wiretapping would be left to the unfettered discretion of law enforcement. As recent experiences show, efforts by law enforcement to self-regulate or efforts by legislatures to limit government access to surveillance technologies solely through extra-constitutional means would be very unlikely to have imposed any real restraint on the use of wiretapping technology. It took a shift in constitutional doctrine to impel legislative action

---

124. *Katz*, 389 U.S. 347. *Berger v. New York*, decided in the term prior to *Katz*, set the stage while also providing specific guidance to Congress as it considered its legislative options. 388 U.S. 41, 54-60 (1967). In *Berger*, the Court found that New York's regulatory regime governing wiretapping was constitutionally insufficient. *Id.* at 63-64.

125. *Katz*, 389 U.S. at 353.

126. *Id.* at 351.

127. *Id.* at 351-52.

128. *Id.* at 352 (noting that telephone booths function as spaces of aural repose in which citizens may reasonably expect that their communications will not be monitored by "uninvited ear[s]").

129. *See* HOWARD J. KAPLAN ET AL., THE HISTORY AND LAW OF WIRETAPPING 4 (2012), *available at* http://www.americanbar.org/content/dam/aba/administrative/litigation/materials/sac_2012/29-1_history_and_law_of_wiretapping.authcheckdam.pdf ("Congress therefore regarded *Katz* and *Berger* as instructive on how to draft a constitutionally sound wiretapping law and thereafter passed the Omnibus Crime Control Act of 1968. Title III of that Act addresses interception of communications and remains to this day the law that governs the federal use of wiretaps.").

130. As the Court recently has made clear, the trespass-based approach to defining Fourth Amendment "search" remains in force. *See* United States v. Jones, 132 S. Ct. 945, 949-51 (2012); *id.* at 954-55 (Sotomayor, J., concurring). The *Katz* doctrine marks a doctrinal addition that can enhance, but not degrade, rights and protections.

The LEATPR Standards break from this pattern. There can be no doubt that the rules and regulations promoted by the Standards are designed to contend with dramatic changes in society, surveillance technology, and law enforcement practice. In its current form, Fourth Amendment doctrine is unable to meet these challenges. If past is prologue, then we might expect a doctrinal reaction. The Court came close in *United States v. Jones*, with five justices expressing support for a "quantitative" approach to assessing Fourth Amendment rights and protections that would respond to enhanced surveillance and data aggregation technologies.[131] Justice Sotomayor went a step further, suggesting that law enforcement's increasing reliance on these technologies may make it "necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[132] Nevertheless, the LEATPR Standards explicitly decline to propose or promote a constitutional foundation for the overall project of reform or for the rules and regulations that comprise the core of its proposals. This raises serious concerns.

Foremost among these are questions of constitutional sufficiency and necessity. Although the Standards are not grounded by any proposed change in Fourth Amendment law or doctrine, there can be little doubt that such a change is coming. When it does, the Standards will face questions of constitutional sufficiency and necessity. At that point, the Standards might well turn out to be constitutionally infirm. They might also turn out to be largely gratuitous. Absent some kind of constitutional commitment on the part of the Standards that is linked to its regulatory proposals, there is simply no way to know.

This mystery marks a significant barrier against adoption. After all, the Standards propose significant changes in current practice and even require the development of new internal control structures within police agencies. It is hard to see why the political branches would make these changes without some idea that they are both necessary and sufficient to meet constitutional demands. Here, the Wiretap Act provides a helpful example. Although *Katz* did not squarely overrule *Olmstead*, combined with *Berger v. New York*, it described the Fourth Amendment theory and doctrine that would govern wiretapping going forward. Acting on this advice, Congress passed the Wiretap Act,[133] which limits law enforcement access to

131. *Jones*, 132 S. Ct. at 949-51; *id.* at 954 (Sotomayor, J., concurring); *id.* at 962-65 (Alito, J., concurring with Ginsburg, Breyer, and Kagan, JJ.).

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

133. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified in scattered sections of 5 U.S.C., 18 U.S.C., and 42 U.S.C.).

wiretapping technology by requiring warrants and court monitoring of all active wiretaps.[134] Those new rules and regulations clearly were tied to the doctrinal changes effected by *Katz*, and as a consequence have been largely immune to constitutional challenge. Although the Standards do not yet have the benefit of a *Katz* for the twenty-first century, they could go quite far in meeting concerns about their constitutional status if they were tied to a Fourth Amendment theory—novel though it might be.

The absence of an underlying Fourth Amendment theory that would buttress the Standards also raises serious questions about the Standards' effectiveness in practice. As the courts' experiences with alternatives to the exclusionary rule show, law enforcement agencies caught up in the "competitive enterprise of ferreting out crime"[135] largely are incapable of self-regulation and immune to meaningful legislative regulation. Although the Standards describe a role for the courts in reviewing some efforts to gain access to some information held by some third parties,[136] the overall scheme remains a free-flying balloon from a constitutional point of view. As a consequence, courts remain powerless to compel adoption of the Standards or to review law enforcement conduct governed by the Standards.[137] Here again, the Wiretap Act provides a useful model. Linked as it is to *Katz*, there can be no doubt that courts have the right and the duty both to limit government access to wiretapping technology and to enforce the overall regulatory scheme. Because of their studiously agnostic stance with respect to constitutional issues, the Standards can make no such claim.

Finally, in the absence of some kind of constitutional impetus, the Standards run full-force into the concerns described in the next section relating to the vagaries of the political process. Acting in the wake of *Berger* and *Katz*, Congress had little choice but to regulate wiretapping. Furthermore, had Congress failed to act, there can be no doubt that the courts would have. Absent that Fourth Amendment sword of Damocles, there is no reason to think that the Wiretap Act would have been adopted, stable, or effective in any sustained way. The challenges posed by contemporary surveillance and dataveillance technologies are greater by far than those posed by wiretapping in 1968. Thus, absent some kind of

134. 18 U.S.C. § 2518 (2012).

135. United States v. Johnson, 333 U.S. 10, 14 (1948).

136. *See* STANDARD 25-5.3.

137. The Standards suggest that its regulations could be imposed on law enforcement by courts exercising their "supervisory authority." STANDARD 25-3.4. As is discussed below, the project described by the Standards exceeds the scope of that authority absent some claim of constitutional necessity.

constitutional driver that can both compel action by the political branches and constrain the outcome of that action, there is serious doubt that the Standards will be either adopted or effective.

This may seem to put the LEATPR Standards and their drafters in a Catch-22: If the Standards adopt a constitutional theory under which the provisions described are constitutionally necessary, then there is really no reason for the Standards in the first place. Alternatively, if the Standards are not constitutionally necessary, then they will not be adopted and may not even meet constitutional demands. That is not where the foregoing critique leaves the Standards, however. Questions relating to what the Fourth Amendment allows law enforcement to do in their engagements with citizens' "persons, houses, papers, and effects" have been a constant since the rise of professionalized police forces in the mid-nineteenth century. The point pressed here is that they are constitutional questions. If the Standards were grounded in a prescribed doctrinal adaptation, as were the exclusionary rule and the Wiretap Act, then they could be quite useful in providing guidance to courts, legislatures, and law enforcement agencies. Absent a clear account of what that constitutional adaptation to contemporary surveillance technologies, techniques, and practices looks like, there is serious doubt that they will be very influential or useful.

There is a risk, of course, that, were the Standards to abandon their agnosticism, then the constitutional theory they adopt may turn out to be wrong. That possibility should not deter supporters from taking the constitutional plunge, however. Consider the possibilities: The Standards might get the constitutional question right, demonstrating both necessity and parsimony in the provisions proposed. That, of course, would be an ideal outcome. Alternatively, the Standards might undershoot on the constitutional front, with the consequence that the provisions would later turn out to be constitutionally insufficient. Of course, if that's the case, then the Standards are already a failed enterprise. That failure would not be lessened by the decision to offer a constitutional foundation from the outset. Finally, if the Standards turn out to be constitutionally sufficient, but in some ways also gratuitous, then they would be in no worse position than they are now. In other words, there really is nothing to lose by grounding the Standards in a constitutional theory. Quite to the contrary, there is everything to be gained.

IV. Consequences of Relying on the Political Process

Because the Standards are not grounded in any claim of constitutional necessity or sufficiency, responsibility for adopting and enforcing their

provisions is left to "legislatures, courts acting in their supervisory capacities, and administrative agencies."[138] This ultimately means that the fate of the Standards and their proscriptions is left entirely in the hands of the political process. Given past experience and recent revelations, this strategy is likely to fail. It may even be dangerous to the overall project of imposing reasonable constraints on law enforcement access to records held by third parties. The fact that the Standards do not reach post-arrest investigations or national security investigations only makes matters worse.[139] This section explores some of these concerns.

To start, we can set aside any real hope that the courts will impose the Standards or any of their constituent provisions absent a claim of constitutional necessity. Courts' supervisory authorities simply do not stretch that far.[140] Appellate courts have some supervisory authority over the procedures adopted by their inferior courts. Trial courts have limited authority to set the rules governing the conduct of parties that appear before them in particular cases.[141] But courts and litigants are not the main regulatory targets for the Standards, which concern themselves primarily with police procedure. The discretionary authority granted to courts simply does not extend to the conduct of police during the course of investigations—at least not without a specific legislative grant or a claim of constitutional necessity.[142] Thus, any attempt by a court to impose the

138. LEATPR STANDARDS, *supra* note 58, at 9.

139. *See* STANDARD 25-2.1(a)-(b).

140. *See* Sara Sun Beale, *Reconsidering Supervisory Power in Criminal Cases: Constitutional and Statutory Limits on the Authority of the Federal Courts*, 84 COLUM. L. REV. 1433, 1455, 1464-94 (1984) (pointing out that the Court's exercise of its supervisory powers has been limited to efforts to "promote the search for the truth, to protect the integrity of the courts, to remedy violations of individual rights, and to impose sanctions against government misconduct" and arguing that much of even these limited efforts constitute overreach).

141. *See, e.g.*, FED. R. CIV. P. 83(a).

142. The Supreme Court's limited claim of supervisory authority over law enforcement arises from its decision in *McNabb v. United States*, 318 U.S. 332 (1943), *superseded in part by* 18 U.S.C. § 3501 (2012). Even in that case, however, the Court limited the compass of its own power to review law enforcement practices to those circumstances where "courts themselves become instruments of law enforcement" by explicitly or implicitly endorsing illegal conduct. *Id.* at 347. Given the fact that any law enforcement efforts that would be regulated by the Standards are by definition legal under the Court's own third party doctrine, it is hard to see where the Court, or any court, could find authority to exercise supervisory powers over law enforcement without first holding that current practices are unconstitutional or otherwise illegal.

Standards or its provisions based solely on its supervisory authority would almost certainly run afoul of basic separation of powers principles.[143]

Take Miranda warnings as a point of comparison. The Miranda warnings comprise perhaps the most minimal imposition on police procedure one could imagine. Nevertheless, the Court has been quite clear that its ability to require Miranda warnings derives from its constitutional authority, not from some discretionary, supervisory power over law enforcement.[144] It is hard to see how the Court, or any court, could mandate prophylactic measures as complex as the Standards based solely on a claim of supervisory authority when something as simple as Miranda warnings must be grounded in a claim of constitutional necessity.

Nothing would seem to change if the Standards were recast as rules of evidence. The Standards do not attach themselves to traditional common law rules of evidence such as relevance, reliability, prejudice, or hearsay, and it is hard to see how they could. Furthermore, few courts have sole authority over the rules of evidence they apply, instead sharing that power with legislatures.[145] Thus, if a court were to create a new category of evidentiary rules based solely on supervisory powers, without any footing in either the common law or the Constitution, that effort would be patent overreach.[146] At any rate, the courts' sole remedy for violations of the Standards if they are treated as rules of evidence is exclusion of evidence acquired from third party records. Even at its most expansive, the Court has never deployed exclusion as a remedy in the absence of some claim of illegality.[147] It is hard to see how a violation of the Standards could constitute illegal conduct unless they are adopted as law by the political branches or backed by a finding of constitutional necessity from the courts.

---

143. Beale, *supra* note 140, at 1473-74 ("Although the term 'procedure' may properly be defined more broadly for other purposes, separation of power principles provide strong support for the application of the narrow definition when the issue is the scope of the federal courts' implied constitutional authority."); *id.* at 1506 ("Although judicial integrity and separation-of-power principles are important considerations in formulating an appropriate remedy for a violation of federal law, they provide no independent source of authority for the exercise of supervisory power when there has been no violation of any constitutional provision or federal statute. The federal courts' authority to create federal common law may provide an additional basis for some supervisory power decisions, but it cannot be expanded to control matters left by the Constitution either to the states or to a coordinate federal branch.").

144. Dickerson v. United States, 530 U.S. 428, 437 (2000).

145. *See, e.g.*, Palermo v. United States, 360 U.S. 343, 352-53 (1959).

146. *See* Beale, *supra* note 140, at 1509, 1515-16, 1521.

147. *See McNabb*, 318 U.S. at 345-46; Beale, *supra* note 140, at 1507.

The consequence is that responsibility for adopting the Standards or any of its measures will fall inevitably and ultimately to the political branches.

Because the Standards rely on the political branches for their adoption, they are dependent upon the political will of legislators and executives to act on their own initiatives without any threat of court intervention that would accompany a claim of constitutional necessity. In the present environment, at least, it is hard to see whence that initiative would come. Supporters might draw some hope from prior legislative efforts to regulate law enforcement access to information held by third parties. For example, they might point to the Penn Register Act,[148] which was passed in the wake of *Smith vs. Maryland*,[149] or the Video Privacy Protection Act,[150] passed in response to disclosures of Robert Bork's video rental history after he was nominated by Ronald Reagan to a position on the Supreme Court.[151] It is surely true that these laws provide constitutionally gratuitous protections, and therefore demonstrate the potential for recruiting political will sufficient to limit the third party doctrine in specific cases. To extrapolate from these specific examples more general support for the broader regulations proposed by the Standards would, however, be akin to the fallacy of generalizing from the particular. Far more likely are piecemeal initiatives such as recent efforts led by Senator Patrick Leahy to amend the Stored Communications Act to reflect changes in expansion of online storage of electronic mail.[152] But, given the glacial progress of this narrow, and relatively uncontroversial measure, this looks more like an exception that proves the rule of legislative inaction rather than an example of political will building around a broader, more expansive set of regulations on the scale of the Standards.

---

148. Pen/Trap Statute (Pen Register Act), Pub. L. No. 99-508, Title III, § 301(a), 100 Stat. 1848, 1868.

149. 442 U.S. 735 (1979).

150. Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (2012)).

151. S. REP. NO. 100-599, at 5 (1988). One might add to this list other components of the Electronic Communications Privacy Act, including the Wiretap Act and the Stored Communications Act, but that would be a mistake. Both of these provisions trace directly to the threat of constitutional regulation posed by *Katz* and its progeny. That the SCA limited its extension of warrant protection to electronic communications stored for fewer than 180 days proves the point. In 1986, when the law was passed, that line described what legislators imagined to be the outlying boundary for how long service providers could physically and economically store communications committed to their custody for purposes of transport.

152. Electronic Communications Privacy Act Amendments Act of 2013, S. 607, 113th Cong. (2013).

To see clear evidence of the lack of political will that is available to advance broad and general regulations along the lines described by the Standards, we need look no further than the remarkable absence of coherent public outcry in the wake of recent revelations about broad, pervasive, and indiscriminate surveillance efforts. Take, for example, New York's Domain Awareness System. When confronted with comparisons of the technology to the dystopian surveillance state described by George Orwell in *1984*, Mayor Bloomberg boasted that the NYPD was no longer a "mom and pop police department."[153] In the intervening months there have been no serious public or legislative efforts to challenge either the technology or its implementation. Public docility in the face of revelations that the NSA, FBI, and CIA are engaged in policies of broad and indiscriminate searches, such as the telephony metadata program,[154] and surreptitious infiltration of networks owned and operated by major internet companies, provides yet more evidence that there is insufficient political will to compel serious regulation.[155]

This is not to suggest that there has been no pushback. There are a few legislators who have taken to the floor of their respective chambers to condemn the executive agencies involved and the lack of substantive court oversight.[156] Several internet companies have also offered strident public critiques.[157] Others have made it corporate policy to fight back. For example, Twitter has committed itself to protecting user information to any

153. Rocco Parascandola & Tina Moore, *NYPD Unveils New $40 Million Super Computer System That Uses Data from Network of Cameras, License Plate Readers, and Crime Reports*, N.Y. DAILY NEWS, Aug. 8, 2012, http://www.nydailynews.com/new-york/nypd-unveils-new-40-million-super-computer-system-data-network-cameras-license-plate-readers-crime-reports-article-1.1132135.

154. *See, e.g.*, Roberts & Ackerman, *supra* note 6.

155. On this front, at least, there may be some movement. As this essay goes to press, the House of Representatives passed the USA FREEDOM Act, H.R. 3361, 113th Cong. (2014) (as passed by House, May 22, 2014), which would amend the Foreign Intelligence Surveillance Act to change the process by which the FBI and NSA would gain access to business records, including telephonic metadata. The text of the bill can be found at H.R. 3361 – USA FREEDOM Act, CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/house-bill/3361 (last visited May 27, 2014).

156. Ashley Parker, *Republicans, Led by Rand Paul, Finally End Filibuster*, N.Y. TIMES (Mar. 6, 2013), http://thecaucus.blogs.nytimes.com/2013/03/06/rand-paul-does-not-go-quietly-into-the-night/?ref=politics.

157. Gellman & Soltani, *supra* note 12 (quoting David Drummond, Chief Legal Officer at Google, as stating, "We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform").

extent it can, including efforts to quash subpoenas and other requests for user information.[158] Some companies have also made it a practice to publish the number of subpoenas they have received and to which they have responded.[159] Most recently, Google and its employees have reacted with outrage and profanity to news that their secure networks were penetrated by the NSA, allowing the government broad access to the contents of customer communications and the cloud storage facilities where user content is stored.[160] None of this reaction has matured into action, however—and it is hard to imagine that it ever will. That is because there is a 500-pound gorilla in the room, which has time and again proved capable of crushing any serious efforts to secure privacy against government dataveillance: national security.

The LEATPR Standards specifically decline to address governments' accessing third party records for the purposes of national security.[161] This omission dooms the Standards' prospects for two reasons. First, the Standards simply cannot hope to generate any political will for their own adoption in the face of countervailing complaints that such procedures as the Standards describe would compromise national security. Attempting to carve off national security investigations just makes matters worse by adding validity to irrationally overblown claims of existential threats that

158. *See, e.g.*, People v. Harris, 949 N.Y.S. 2d 590 (N.Y. Crim. Ct. 2012).

159. *See, e.g.*, *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/ (last visited Apr. 11, 2014).

160. *Google Employees on NSA: 'F*ck These Guys'*, HUFFINGTON POST, Nov. 6, 2013, http://www.huffingtonpost.com/2013/11/06/google-nsa_n_4227596.html; *Google Statement on NSA Infiltration of Links Between Data Centers*, WASH. POST, Oct. 30, 2013, http://www.washingtonpost.com/world/national-security/google-statement-on-nsa-infiltration-of-links-between-data-centers/2013/10/30/75f3314a-41b3-11e3-a624-41d661b0bb78_story.html.

161. STANDARD 25-2.1(a). There is a chance that some of the concerns that follow are mooted by the Standards' definition of "national security acquisitions" as "those intended to acquire information concerning a foreign power or an agent thereof." STANDARD 25-2.1(a) commentary. For example, taken literally, this definition of "national security" would exclude investigations of terrorism, border security, and the NSA's telephonic dataveillance program because none of these necessarily involves a "foreign power" or its agents. The Standards themselves do not suggest this narrow, literal reading, however. That is evident in the commentaries, which contemplate information gathering that might have prevented the terrorist attacks of September 11, 2001, as outside the scope of the Standards. *Id.* Footnote 14 in the introduction is even more explicit, appearing to embrace the broader definition of "national security" set forth in the USA PATRIOT Act, and explicitly encompassing "telephone records of a person who is *not* an agent of a foreign power, so long as those records are relevant to a national security investigation of such an agent." LEATPR STANDARDS, *supra* note 58, at 5 n.14.

have been used to grant largely unchecked license for law enforcement to engage in all sorts of invasive surveillance and dataveillance. Second, even if the Standards were to provide sufficient reassurance to nervous legislators that national security would in no way be compromised by implementing significant access controls in the context of criminal investigations, the exception represented by the carve-out would swallow the rule.

There can be no doubt that the primary use and abuse of the third party doctrine these days is in the national security arena. From New York's Domain Awareness System to the NSA's gathering of all telephonic metadata generated by every call serviced by every telephone company in the United States, the primary justification officials cite is national security and the war on terror. But these examples are little more than pebbles cast into still waters. Rippling outward from this center are hundreds and thousands of federal agencies, state law enforcement, and local police departments that have been recruited into the ever-sprawling project of national security. Every one of these agencies and agents is now deployed in the war on terror.

For example, by rhetoric and bureaucratic design, immigration enforcement is now a centerpiece of national security policy. Moreover, local law enforcement is now heavily involved through federal programs such as 529(g) and Secure Communities, which have successfully made immigration enforcement a primary law enforcement concern at every level—right down to local beat cops.[162] Even the previously secular war on drugs has now got national security religion. Some of this coming to the faith is understandable—the opiate trade traces straight back to terrorist centers in Afghanistan and Pakistan, after all[163]—but, with drug cartels and other organizations tied to cocaine and marijuana production in south and central America now designated "terrorist organizations" by the State Department,[164] every local narcotics enforcement agency is engaged in national security activities. If even the most quotidian of police actions—traffic stops and drug investigations—can now be linked to national security, then the Standards look like the saddest damsel at the dance.

None of this is a surprise. During the founding era, when anti-federalists attacked the Constitution and the central government it contemplated as a

---

162. Gray, Cooper, & McAloon, *supra* note 113, at 26-32.

163. *See* GRETCHEN PETERS, HOW OPIUM PROFITS THE TALIBAN 3-6 (2009), *available at* http://www.usip.org/sites/default/files/resources/taliban_opium_1.pdf.

164. *Foreign Terrorist Organizations*, STATE.GOV (Sept. 28, 2012), http://www.state.gov/j/ct/rls/other/des/123085.htm.

threat to individual liberty, critics knew the power of executive claims of emergency to justify invasive search and seizure. Consider, for example, the prophetic words of the Maryland Farmer, who wrote in 1788 about the inability of common law prohibitions on general warrants to resist executive overreaching in "cases which may strongly interest the passions of government."[165] His concerns were well grounded not only in the American experience with writs of assistance, but also in British experiences with general warrants used to target political and religious subversives. Reflecting on perhaps the most famous of these cases, *Wilkes v. Wood*,[166] the Canadian Freeholder noted that executive officers are too "fond of doctrines of reason of state, and state necessity, and the impossibility of providing for great emergencies and extraordinary cases," and that they therefore demanded "discretionary power in the Crown to proceed sometimes by uncommon methods not agreeable to the known forms of law."[167] What was true for our eighteenth century forebears is true for us today—and the same lesson applies: it is simply folly to hope that political will or self-restraint will be enough to keep government agents within the compass of powers proscribed for them by the liberty of their subjects. Our forefathers understood that this goal can only be accomplished by enforcement of constitutional precommitments.[168] There

165. A MARYLAND FARMER, NO. 1 (1788), *reprinted in* THE FOUNDERS' CONSTITUTION 462, 464 (Philip B. Kurland & Ralph Lerner, eds. 1987) ("[S]uppose for instance, that an officer of the United States should force the house, the asylum of a citizen, by virtue of a general warrant, I would ask, are general warrants illegal by the constitution of the United States? Would a court, or even a jury, but juries are no longer to exist, punish a man who acted by express authority, upon the bare recollection of what once was law and right? I fear not, especially in those cases which may strongly interest the passions of government, and in such only have general warrants been used.").

166. (1763) 98 Eng. Rep. 489 (C.P.).

167. 2 THE CANADIAN FREEHOLDER: IN THREE DIALOGUES BETWEEN AN ENGLISHMAN AND A FRENCHMAN SETTLED IN CANADA 243-44 (London, B. White 1779).

168. As Thomas Davies has shown, the Fourth Amendment was adopted as a constitutional Precommitment against not only executive overreach but legislative license as well. *See* Davies, *supra* note 99, at 578-81, 657-60, 663-64, 668. Specifically, although general warrants were prohibited under the common law well before 1791, anti-federalists were concerned that the federal government might be tempted to pass legislation licensing general warrants, particularly if faced with a claim of emergency or necessity. *Id.* at 668 ("[The framers] thought the important issue, and the only potential threat to the right to be secure, was whether *general* warrants could be authorized by *legislation*."). Recent amendments to the USA PATRIOT Act that have been exploited, with legislative acquiescence and approval, to allow the NSA to pursue broadening dataveillance programs under the auspices of general warrants issued by the Foreign Intelligence Surveillance Court

is no reason to think that the project of reform and regulation described by the Standards can escape this historically proven truth.[169]

V. Some Concerns with the Core Approach

In the wake of the Supreme Court's decision in *United States v. Jones*, and recent revelations about widespread and largely unchecked government surveillance and dataveillance, advocates, activists, technologists, and scholars have advanced a range of possible approaches to the challenge of preserving privacy in the twenty-first century. Although diverse in the details, most of these proposals fall into one of four categories.

The first is market-based and favors allowing the private sector to develop business models and technologies capable of protecting personal information.[170] The problem with these proposals, of course, is that they perpetuate an arms race between government and corporate engineers. Moreover, even when the corporate guardians win, they are still vulnerable to overt demands for information, which few have so far been able to resist.[171] As a consequence, pure market-based solutions seem to be doomed to failure without some kind of legislative or constitutional framework that can constrain government surveillance and limit legal access to third party records.

The second strategy focuses on the duration of a search or the quantity of information that is discovered or aggregated. In his concurring opinion in *Jones*, Justice Alito seemed to favor just this sort of approach.[172] Christopher Slobogin has picked up that mantle by elaborating model

---

provide a modern vision of our founders' bête noir. *See* Gray & Citron, *supra* note 18, at 119-23.

169. A similar case can be made based on the Standards' decision not to regulate grand jury investigations. *See* STANDARD 25-2.1(c). As I have argued elsewhere, the grand jury exception to the exclusionary rule has left largely unregulated a widening range of law enforcement-citizen engagements to the detriment of Fourth Amendment rights. *See* Gray, Cooper, & McAloon, *supra* note 113, at 21-25.

170. *See, e.g.*, DISCONNECT, https://Disconnect.me (last visited Apr. 11, 2014).

171. *See supra* note 158 and accompanying text. Yahoo reports rejecting only 8% of requests for user data from U.S. law enforcement agencies between July 1, 2013, and December 31, 2013. *Transparency Report: Government Data Requests*, YAHOO, https://transparency.yahoo.com/government-data-requests/US-JUL-DEC-2013.html (last visited May 13, 2014). Google reports providing data in response to 83% of requests in the same time frame. *Transparency Report: Requests for User Information*, GOOGLE, https://www.google.com/transparencyreport/userdatarequests/countries/https://www.google.com/transparencyreport/userdatarequests/countries/ (last visited May 13, 2014).

172. United States v. Jones, 132 S. Ct. 945, 962-63 (2012) (Alito, J., concurring).

legislation that would set boundaries on how long law enforcement officers can conduct surveillance and how much data they can aggregate.[173] Although far more promising than pure market-based approaches, proposals based on the duration of surveillance or raw quantity of data gathered inevitably will be under- and over-inclusive.[174] Professor Slobogin has acknowledged these difficulties, and his proposed statute does its best to address them by striking reasonable bright lines,[175] but even these efforts cannot avoid this inherent deficit of all purely quantitative approaches to regulating surveillance and data gathering.

A third strategy would focus regulatory attention on the technologies that are used to facilitate surveillance and dataveillance. Danielle Citron and I have argued for this strategy in a sustained way through a series of recent articles.[176] As we point out in this work, the Fourth Amendment was conceived and designed as a bulwark against the temptations that legislatures and executives inevitably feel to derogate from the common law prohibition on general warrants.[177] Our founders knew from their own experiences with writs of assistance that granting government agents broad powers to search anyone, anywhere, at any time, leaves all citizens insecure in their persons, homes, papers, and effects.[178] The Fourth Amendment guarantees a right to security by limiting the government's search powers within the compass of reasonableness. In our view, technologies that are capable of facilitating policies of broad and indiscriminate search pose the same threat to general security that general warrants did in the eighteenth century.[179] We therefore argue that law enforcement access to these technologies must be limited in order to effect a reasonable balance between government interests in preventing, detecting, and prosecuting crime and citizens' interests in security from pervasive surveillance.[180] As we point out, striking that balance will depend on the nature of the

173. Slobogin, *supra* note 92, at 16-37.

174. *See* 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, 427 (2013).

175. Slobogin, *supra* note 92, at 16-37.

176. *See, e.g.*, Citron & Gray, *supra* note 98; Gray & Citron, *supra* note 174; Gray & Citron, *supra* note 18; Gray, Citron & Rinehart, *supra* note 39.

177. Gray & Citron, *supra* note 18, at 92-100.

178. *Id.* at 70, 93-96.

179. *Id.* at 101-05.

180. *Id.* at 101-03.

technology in question and the competing interests at stake.[181] Sometimes warrants may be required.[182] For other technologies, administrative review subject to court oversight may suffice.[183] What the Fourth Amendment cannot abide, however, are efforts to revitalize general warrants such as those issued by the Foreign Intelligence Surveillance Court in support of the NSA's telephony metadata gathering program.[184]

The fourth major category of proposals focuses on the nature and significance of the information that is sought or secured. Neil Richards has perhaps done the most to advance this strategy on the academic side through a series of articles driven by First Amendment rather than Fourth Amendment concerns.[185] The LEATPR Standards also adopt this tack. Danielle Citron and I have argued elsewhere against this content-based approach on conceptual and practical grounds.[186] Although the Standards provide a distinct and much more specific set of proposals than has been previously offered, they suffer the same conceptual and practical deficits and are therefore vulnerable to the same objections. Before getting to those concerns, however, it is important to take notice of a failure that is unique to the Standards and is measured by its own metrics for progress.

The Standards fail to advance the cause of privacy even according to their own internally defined metric. "Privacy" for purposes of the Standards, is defined as the "ability to control what information about oneself is known to others and for what purposes that information is used."[187] The third party doctrine holds that, as a constitutional matter, there is only one way to control information and, in turn, only one way to control the purposes for which information is used: keep it secret. In her concurring opinion in *Jones*, Justice Sotomayor suggests that this conflation of secrecy and privacy is no longer tenable in the age of Big Data and ubiquitous surveillance,[188] and that we must therefore "reconsider" the third

---

181. *Id.* at 105-24 (discussing the Fourth Amendment status of drones, data aggregation technology, and human surveillance under a technology-centered approach to quantitative privacy).

182. *Id.* at 105-12 (arguing for a warrant requirement covering discrete surveillance technologies like drones).

183. *Id.* at 112-24 (arguing for administrative review structures modeled on consent decrees to cover data aggregation technologies).

184. *Id.* at 119.

185. *See, e.g.*, Richards, *Intellectual Privacy*, *supra* note 97.

186. Citron & Gray, *supra* note 98.

187. STANDARD 25-4.1(a) commentary.

188. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I for one doubt that people would accept without complaint the warrantless disclosure to the

party doctrine.[189] Without purporting to disrupt constitutional doctrine,[190] the Standards take a similar view of the relationship between secrecy and privacy. "[P]rivacy is not secrecy," we are told.[191] Rather, "secrecy is merely one form of privacy."[192] Thus, although it is true to the point of tautology that keeping information about oneself secret will serve to keep that information private as well, the Standards seek more bespoke measures that will allow us to share personal information while still preserving some level of control over the use and dissemination of that information. Unfortunately, the Standards fail in that effort. To see why, it is necessary to examine the regulatory strategy that the Standards adopt.

The Standards' strategy for offering greater privacy controls without requiring secrecy is organized around two overlapping spectrums. The first spectrum measures the privacy interests that individuals might hold in information they share with third parties. Some information is "highly private," some is "moderately private," some is "minimally private," and some is "not private" at all.[193] The second spectrum describes four ways that law enforcement might gain access to information held by third parties without the consent[194] of the person whose privacy interests are at stake: by

---

Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.").

189. *Id.*

190. LEATPR STANDARDS, *supra* note 58, at 6-9.

191. STANDARD 25-4.1(a) commentary.

192. *Id.*

193. STANDARD 25-4.2.

194. Consent gets separate treatment under the Standards:

> Law enforcement should be permitted to access by particularized request any record maintained by an institutional third party if:
>
> (a) the focus of the record has knowingly and voluntarily consented to that specific law enforcement access;
>
> (b) the focus of the record has knowingly and voluntarily given generalized consent to law enforcement access, and
>
> (i) the information in the record is unprotected or minimally protected;
>
> (ii) it was possible to decline the generalized consent and still obtain the desired service from the provider requesting consent, and the focus of the record had specifically acknowledged that it was possible; or
>
> (iii) a legislature has decided that in a particular context, such as certain government contracting, generalized consent should suffice for the information contained in the record; or
>
> (c) the record pertains to a joint account and any one joint account holder has given consent as provided in subdivision (a) or (b).

court order[195] based on a judicial determination of probable cause,[196] by court order based on a judicial determination of reasonable suspicion or a finding of investigative need,[197] by prosecutorial subpoena,[198] or by an official certification of a politically accountable official within a law enforcement agency.[199] Symmetry dictates what follows: in order for law enforcement to demand access to records held by third parties that contain highly private information, a court order based on a judicial finding of probable cause is required;[200] records containing moderately private information require a court order based on reasonable suspicion or a finding of investigative need;[201] access to records containing minimally protected information requires a subpoena;[202] and information that is not private at all requires only an official certification.[203]

There is no doubt that the framework proposed by the Standards marks an improvement over current practices operating under the third party doctrine. Foremost, the Standards recognize that sharing information does not, or at least should not, entail a complete abdication of all expectations of privacy.[204] Unfortunately, that is all that is offered. The Standards do not challenge in any fundamental way the structured assumptions about the

---

STANDARD 25-5.1.

195. The Standards describe a "court order" as:

> (i) a judicial determination that there is probable cause to believe the information in the record contains or will lead to evidence of crime;
>
> (ii) a judicial determination that there is reasonable suspicion to believe the information in the record contains or will lead to evidence of crime;
>
> (iii) a judicial determination that the record is relevant to an investigation; or
>
> (iv) a prosecutorial certification that the record is relevant to an investigation.

STANDARD 25-5.2(a).

196. STANDARD 25-5.2(a)(i).

197. *See* STANDARD 25-5.2(a)(ii)-(iv).

198. STANDARD 25-5.2(b) (requiring that subpoenas be "based upon a prosecutorial or agency determination that the record is relevant to an investigation").

199. STANDARD 25.52(c) (requiring that official certifications be "based upon a written determination by a politically accountable official that there is a reasonable possibility that the record is relevant to initiating or pursuing an investigation").

200. STANDARD 25-5.3(a)(i).

201. STANDARD 25-5.3(a)(ii).

202. STANDARD 25-5.3(a)(iii).

203. STANDARD 25-5.3(d) ("Law enforcement should be permitted to access unprotected information for any legitimate law enforcement purpose.").

204. *See* STANDARD 25-3.3 commentary.

nature of privacy and its relationship to secrecy that underlie the third party doctrine. This general approach is both problematic and worrisome.

Although often condensed as "the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,"[205] the third party doctrine is not so broad. Were it so, then there would be no constitutional barrier against wiretapping or any other interception of communications because all information imparted during a conversation is by definition "disclosed to third parties." Rather, the third party doctrine holds that the Fourth Amendment is not violated if the government obtains through lawful means information from a third party that an investigative target voluntarily shared with that third party.[206] Put differently, sharing information with a third party entails an assumption of risk that the third party might share that information with others, either voluntarily or if compelled to do so by "legal process."[207]

As the LEATPR Standards rightly recognize, this "assumption of risk" model of privacy conflates privacy and secrecy. The Standards are deeply critical of the third party doctrine on this score. "Privacy," according to the Standards, is more expansive than secrecy. It "is the more encompassing ability to control what information about oneself is known to others, and for what purposes that information is used."[208] Secrecy is certainly one method of preserving privacy, but it is not, and should not be, the only way. After all, it makes very little sense to talk about "control" if the only options are to quit, abdicate, withdraw, or simply not participate in the first place.[209] To draw the inevitable sports analogy, we certainly would not say that a basketball player has excellent ball control when all he does is hold the ball, never dribbling, passing, or shooting. Rather, "control" implies engagement, and describes the ability to restrain, direct, and influence the course and outcome of events once one has engaged. To the extent that

---

205. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

206. *See Miller*, 425 U.S. at 442-43; Hoffa v. United States, 385 U.S. 293, 302 (1966).

207. *Smith*, 442 U.S. at 744 (finding that a person who uses the phone "assume[s] the risk that the [telephone] company would reveal to police the numbers he dialed").

208. STANDARD 25-4.1(a) commentary.

209. DANIELLE KEATS CITRON, HATE 3.0: A CIVIL RIGHTS AGENDA TO COMBAT DISCRIMINATORY ONLINE HARASSMENT (forthcoming 2014) (on file with author) (arguing at length against the proposition that those who are subjected to online harassment should just stay off the internet); Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 105 (2009) (same).

privacy is a function of control, then, the Standards are perfectly right to hold that privacy is more than secrecy.

Given the Standards' critique of the third party doctrine's conflation of secrecy and privacy, one would expect some effort by the Standards to provide means short of secrecy by which one could exercise control over personal information. Unfortunately, they do not. To the contrary, they reinforce the basic digital dynamic that underlies the third party doctrine: keep it secret, and preserve your privacy, or share, and run the risk that what you share will end up in the hands of law enforcement through lawful means. It is certainly true that the Standards add dimension and specificity to the otherwise abstract notion of "lawful means," but doing so provides no additional measures by which a person might exercise control over the use and dissemination of personal information. Under the Standards, as under the status quo described by the third party doctrine, secrecy is the only game in town.

To see the point, consider the two spectrums at the core of the Standards. The first spectrum describes a range of privacy interests one might have in a particular bit of information extending from "highly private" to "not private."[210] Given the Standards' focus on control, one would expect to have a high degree of control over highly private information and very little control over information that is not private. The Standards provide no such means of control, however. Rather, the second spectrum describes a range of comparatively higher procedural hurdles for law enforcement to clear when seeking access to information.[211] Nothing about the process of clearing those hurdles suggests any control by the subject. It certainly does not provide for any additional tools that a person might use to limit the use and dissemination of private information. Rather, it seems that we are still caught in a world where secrecy is the only means available for someone who wants to preserve her privacy.

A defender of the Standards might respond to this point by shifting the conversation away from "control" in its colloquial sense to a more technical account that focuses on risk assessment. On this view, the fundamental question is that which was initiated by the Court in *Katz*: reasonable expectations of privacy. What the Standards really provide, then, is a more elaborate and specific risk profile that citizens can use when weighing whether to break the seal of secrecy by sharing personal information. Thus, we might reasonably expect that "highly protected" information is less

210. *See* STANDARD 25-4.1.
211. STANDARD 25-4.2.

likely to be shared with the government than "minimally protected" information. In a somewhat paradoxical sense, then, one need be less cautious in sharing "highly protected" information, but might well need to keep completely secret anything that warrants only "minimal protection."

Unfortunately, this response does nothing more than admit defeat according to the Standards' own, well, standards. Remember that "privacy" according to the Standards is about control, not prediction. As it stands, we all know that our telephone calls are being monitored for metadata and that the contents of our communications and data files transmitted through or held by Google are accessible by the NSA. It would tax the language, however, to claim that this knowledge is what we mean by "privacy," much less "control." To the contrary, if "privacy" is a function of control, then knowledge that one has no control means that one has no privacy.

Nothing changes if one can predict that information will only be accessible by provision of a judicial warrant. All that does is specify the process that law enforcement must go through to gain access to personal information. It does not inform the citizen of how likely that eventuality is. Neither do the LEATPR Standards suggest other means by which a citizen could negotiate, impose, or enforce any sort of constraints on the sharing of information, even if governed by a warrant process. Thus, shifting the ground from control to prediction simply highlights the fact that the Standards really do not offer any additional means to protect privacy by effecting "control [over] what information about oneself is known to others, and for what purposes that information is used."[212] The Standards instead put us back where we started: a practical, if not conceptual, collapsing of privacy into secrecy. Under the Standards, as under the status quo, once information is shared, it is out of your control.

The Standards' failure to expand subjects' control over the use and dissemination of private information beyond the nuclear option of secrecy is further reflected in the procedures law enforcement can use to access private information. Just as under the status quo, law enforcement's pathway to third party records under the regime described by the Standards is *ex parte*. That means that the holders of privacy interests, who have both the purest need and the dearest desire to exercise control over access to third party records, will continue to be denied the opportunity to participate in the adversarial processes where their interests are assessed and either protected or compromised. The Standards do impose certain notice

212. STANDARD 25-4.1(a) commentary.

requirements,[213] but these offer no real solace. That is because the notice contemplated is *post hoc*. So, once notice is received, the moment to exercise control has already passed.

Perhaps the Standards' most blinding failure to offer real control over information is found in the decision to give legislatures and courts sole authority to designate the level of privacy that will be afforded to information. It is hard to imagine a more profound denial of control over information than allowing someone else to decide how "private" one's private information is. That the decision is a generic one does not change anything, and may well make matters worse. That is because it emphasizes further the lack of real control that each of us has over our information. Not only is the degree of privacy interest not *your* decision, but the Standards will not even consider your unique claims or circumstances.[214] Furthermore, the general approach to assessing privacy interests submits this most critical decision to a political process. The inevitable result will be endless contests over which kinds of information deserve which level of protection.[215] Marking the boundaries between information that is highly private and only moderately private presents practical problems, of course, but more worrisome is the inevitable politicization of the process and its outputs.

By definition, decision makers designated by the Standards to categorize personal information will have to pick winners and losers among different persons and groups and among their competing conceptions of the good life.[216] That process will almost inevitably lead to decisions that further marginalize and oppress minorities and those who hold minority views.[217] All the more so given the outsized influence that national security interests are bound to have.[218] It is one thing to be told that government agents need access to the information you regard as most private in order to effectuate

---

213. STANDARD 25-5.7.

214. *See* LEATPR STANDARDS, *supra* note 58, at 12 ("It should be stressed that this determination will have been made by a legislature, administrative agency, or court" before law enforcement officers seek access.).

215. *Cf.* Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 330-53 (2012) (leveling this argument against the "mosaic theory" of quantitative privacy). For a critical discussion of Kerr's concerns, see Gray & Citron, *supra* note 174, at 422-28. The Standards foresee these debates, see STANDARD 25-4.1 commentary, but fail to address the oppressive potential of the contests and the decisions.

216. Citron & Gray, *supra* note 98, at 267-68.

217. *Id.*

218. Citron & Pasquale, *supra* note 19, at 1479-80 (exploring the Schmittian "state of emergency" exceptionalism embraced in the post-9/11 era).

the war on terror. It is quite another, however, to be told that the information is not private at all because, were it otherwise, it would be too difficult for law enforcement to obtain regular access.

The Standards appear to foresee this objection. Specifically, the commentary to Standard 25-4.1 emphasizes that the assignment of privacy interest must come first and be considered separately from the level of privacy protection.[219] In order to ensure that sequence, Standard 25-4.2(b) provides a safety valve of sorts for law enforcement, which would allow a legislature to lower the hurdles for accessing highly private information. There is no structural way to enforce this sequence, of course.[220] Furthermore, a quick look at the political costs of assigning relatively lower degrees of privacy interest to information versus granting law enforcement a broad exception suggests that passive aggression is the more likely course. Even where the Standards' preferred sequence is followed, the "out" offered by 25-4.2(b) seems like an exception that is very likely to swallow the rule given the outsized role played by national security interests in the current environment. We need look no further than the general warrant issued by the Foreign Intelligence Surveillance Court for the NSA's telephonic surveillance program to see both the pressures and the effects.[221]

Supporters of the Standards might try another response, arguing that the four factors offered as relevant for assessing the privacy interests held in third party records will provide sufficient breadth and constraint to meet, or at least mostly moot, these concerns.[222] Of course, that does nothing more than move the debate, and therefore the site of oppression, back one step. Moreover, the factors themselves seem to create more space for controversy and potential oppression than they provide guidance, predictability, or control. Let us take a moment to consider each of them in turn.

The first factor that legislatures, administrative agencies, or courts are tasked to consider when weighing the level of privacy interest held in information contained in third party records, is whether "the initial transfer of such information to an institutional third party is reasonably necessary to participate meaningfully in society or in commerce, or is socially beneficial,

---

219. STANDARD 25-4.1 commentary.

220. STANDARD 25-4.2(b) (allowing legislatures to alter the scheme if it "would render law enforcement unable to solve or prevent an unacceptable amount of otherwise solvable or preventable crime").

221. *See In re* Application of F.B.I. for an Order Requiring Prod. of Tangible Things from [Redacted], No. BR 13-80 (Foreign Intelligence Surveillance Ct. Apr. 25, 2013).

222. *See* STANDARD 25-4.1.

including to freedom of speech and association."[223] The main problems with this factor are, of course, that it is utterly ambiguous and requires the very selection among competing ethical views that Danielle Citron and I have warned against. Let us consider first the ambiguity.

Viewed one way, the first factor might cut in favor of assigning a higher privacy interest to information that comes under its wing. After all, if the information is forced out by necessity rather than freely shared, then it would seem wrong to penalize the privacy holder for simply participating in the world.[224] On the other hand, a functional requirement that information be shared in order to facilitate routine daily life may reflect a social discount such that it is no longer reasonable to preserve a strong privacy interest in that information. In short, the need to share may tell us very little about the privacy interests. We may be required to share very personal information, as when we tell our physicians about the uncomfortable rash we've developed "down there." Alternatively, we may be required to reveal information that is utterly banal, such as sharing preferences on brands of sneakers with an online vendor when searching their inventory. So, the fact that I am required to share information really says nothing about the implications of revelation for my privacy interests.[225]

The more compelling problem with the first factor is, however, that it requires legislatures, administrative agencies, or courts to select among competing conceptions of the good life. Neutrality as to ethical choice is a cornerstone of liberal democracies and is baked into the American consciousness.[226] Citizens of equal standing who have different views on what, for them, constitutes the pursuit of happiness inevitably will have different views on what sort of information must be easily accessible in order to facilitate the social good and what must be protected as private in order to secure sufficient space for projects of ethical self-development.

It is out of this respect for diversity of views on the nature and value of privacy that the Supreme Court has declined to make the kinds of assessments that the Standards demand. In *Kyllo v. United States*, the Court

---

223. STANDARD 25-4.1(a).

224. *See* Citron, *supra* note 209, at 104-05.

225. At most, it operates as a limitation on the quasi-abandonment rationale of the third party doctrine. So, the first factor shows that any assertion that sharing implies lack of privacy is false; but it does not show either that sharing requirements signal a diminishment of privacy interest or that sharing requirements indicate heightened privacy interests.

226. *See, e.g.*, THE DECLARATION OF INDEPENDENCE para. 2 (U.S. 1776) ("We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness.").

had the opportunity to link Fourth Amendment protections to the degree of intimacy entailed in the information gathered by law enforcement when using a heat detection device to peer into a home.[227] Writing for the Court, Justice Scalia declined this invitation because he thought the Court had neither the qualifications nor the authority to determine what is and is not "intimate."[228] Laying ground for the technology-centered approach that Danielle Citron and I have defended, Justice Scalia focused instead on the invasiveness of the technology itself and its potential to render a wide range of activities subject to government surveillance, whether "intimate" or not.[229]

The Standards, of course, go in precisely the opposite direction. Rather than preserving neutrality as to competing conceptions of intimacy, privacy, expression, and social benefit, they specifically charge legislatures, administrative agencies, and courts with the task of choosing among them. Elsewhere, Danielle Citron and I have warned about the dangers that inhere to these sorts of political contests, particularly for political and social outsiders, who more often than not make outsized contributions to society in the long term.[230] The fact that the Standards give specific license to challenge and perhaps violate this basic democratic commitment to neutrality should give us pause.

The second factor is neither more helpful nor less subject to contest. Here the Standards require that legislatures, agencies, and courts consider whether the information disclosed is "intimate and likely to cause embarrassment or stigma if disclosed, and whether outside of the initial transfer to an institutional third party it is typically disclosed only within one's close social network, if at all."[231] These are, of course, highly personal assessments. Some of us—this author included—tend to be very private people. We (I) would never share the sorts of information that others broadcast freely over blogs or social networking websites. Where this is the case, a legislative, administrative, or court decision to go with what seems to be the public practice would by definition deny protection to those of us who are less visible precisely because we value our privacy.

The third factor offered by the Standards to decision makers tasked to assess the privacy interests invested in particular kinds of information does little to add new opportunities for control or to temper threats posed by

227. *See* 533 U.S. 27, 37-38 (2001).
228. *Id.*
229. *Id.*; *see also* Gray & Citron, *supra* note 18, at 105, 127-28.
230. Citron & Gray, *supra* note 98, at 267-68.
231. STANDARD 25-4.1(b).

submitting these questions to a political process. Here, the Standards ask whether the information at issue "is accessible to and accessed by non-government persons outside the institutional third party."[232] Here again, no additional opportunities to effect control appear to be offered. Save the odd opportunity to decline a request from vendors to share our information with their commercial partners, we seldom have control over what institutional third parties do with the information we provide to them. Their contracts for services, including their privacy policies, are almost always contracts of adhesion. Moreover, even when we may be willing participants in information sharing among third parties, our reasons for being so are unlikely to translate directly into a lessened expectation of privacy with respect to sharing with law enforcement. For example, I might be quite happy about the potential for information-sharing among health providers because it can advance the cause of providing me with more consistent and cost-effective care. It does not follow, however, that this information is anything less than "highly private."

The fourth factor appears to hold a bit more promise, but also raises some confusion. Here the Standards suggest that whether "existing law, including the law of privilege, restricts or allows access to and dissemination of such information or of comparable information" is relevant to assessing the level of privacy interest invested in that information.[233] Although the promise of using collateral legislative efforts to effectuate constraints on law enforcement access is intriguing, the current landscape of such laws raises some eyebrows. For example, access to video rental records is restricted by law,[234] but access to location information is not. The Standards' reference to the laws of privilege is also a bit confusing. Privilege addresses the party with whom information is shared, not what information is shared[235]—and it is the information that is of concern to the Standards. Moreover, privilege covers a pretty wide range of information. Some privileged relationships are centered on a fairly narrow range of types of information. Patient-doctor relationships are a good example. But others are not nearly so limited. Take for example the range of information shared with lawyers, priests, and spouses. It is so broad that

232. STANDARD 25-4.1(c).

233. STANDARD 25-4.1(d).

234. 18 U.S.C. § 2710 (2012).

235. *See, e.g.*, 12 OKLA. STAT. § 2502(B) (2011) ("A client has a privilege to refuse to disclose and to prevent any other person from disclosing confidential communications made for the purpose of facilitating the rendition of professional legal services . . . .").

this fourth factor seems at risk of being overinclusive to the point of negation.

For these and other reasons, Danielle Citron and I have argued elsewhere that efforts to protect privacy in the face of twenty-first century threats should focus on regulating law enforcement's access to and use of surveillance and dataveillance technologies.[236] In our view, what is troubling about the dataveillance technologies that take advantage of the third party doctrine is not what information they gather, but, rather, the broad, indiscriminate, and continuous nature of the surveillance they facilitate, and the effects of that surveillance on general security in our persons, houses, papers, and effects.[237] If we want to preserve reasonable expectations of privacy against these technologies, then we should confront the threats that they pose directly. The Standards choose a collateral approach. For that reason, and for others set forth here, they are unlikely to succeed.

VI. Conclusion

There is, of course, much more to say and write about the LEATPR Standards. They reflect both serious thinking and, perhaps more importantly, serious engagement among representatives of the many constituencies that are concerned with the current state of affairs with respect to law enforcement access to third party records. Even though this essay is ultimately skeptical of the Standards on their own terms and on exogenous grounds, the merit of the enterprise and the value of the product cannot be denied and should not be dismissed. The Standards truly represent a Herculean effort. There is no doubt that they will serve as a valuable source of ideas and locus for important conversations going forward. I, for one, am grateful for the opportunity to be part of this early engagement.

---

236. *See* Gray & Citron, *supra* note 18.

237. *Id.* at 8, 8 n.45. We are inspired to use this formulation by Susan Freiwald. *See* Susan Freiwald, The Four Factor Test (Jan. 2013) (unpublished manuscript), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1012&context=susan_freiwald.