CONSTITUTIONAL LIMITS ON SURVEILLANCE: ASSOCIATIONAL FREEDOM IN THE AGE OF DATA HOARDING

*Deven R. Desai**

ABSTRACT

Protecting associational freedom is a core, independent yet unappreciated part of the Fourth Amendment. New surveillance techniques threaten that freedom. Surveillance is no longer primarily forward looking. Today, changing technology allows law enforcement and intelligence services to obtain the same, if not more, information about all of us by looking backward. This shift massively expands the government's ability to examine, investigate, and deter exercise of the freedom of association.

* Associate Professor of Law and Ethics, Georgia Institute of Technology, Scheller College of Business; J.D. Yale Law School; former Academic Research Counsel, Google, Inc. This Article has benefitted from the input of Derek Bambauer, Jane Bambauer, Ashutosh Bhagwat, Jack Chin, Julie Cohen, Brett Frischmann, Chris Hoofnagle, Orin Kerr, Paul Ohm, Christopher Slobogin, Daniel Solove, and Peter Swire. The attendees of Privacy Law Scholars Conference 2013 at U.C. Berkeley provided valuable feedback as well. Last, I'd be remiss if I did not thank the *Notre Dame Law Review* for its excellent editing and support for this Article. I thank all for their help, and, of course, all errors are mine.

Forward-looking surveillance has limits that don't apply to backward-looking surveillance. Some limits are practical such as the cost to place a person in a car to follow a suspect. Some are procedural, such as the requirement that surveillance relate to criminal activity. In addition, surveillance such as wiretapping and using a GPS tracker often requires a warrant, involving review by a neutral magistrate. The warrant sets limits on what information may be collected, how it is collected, and how it can be used. The surveillance is also time limited and requires continual justification to a judge, or the surveillance will be shut down. With backward-looking surveillance all of these protections are gone. Anyone conducting surveillance can now use low-cost technology to track us or need only ask a business for the record of where we went, whom we called, what we read, and more. Revelation of the NSA's vast PRISM surveillance project is but the most recent example of overreaching surveillance. The FBI has previously deployed programs to read mail, obtain lists of books read, demand member lists, and generate watch lists of people to round up in case of national emergency. The efforts vary; the harm is the same. With access to a myriad of our records, law enforcement or intelligence services have an almost perfect picture of our activities and associations regardless of whether they are criminal. With digital records these harms are more acute. Once the data about our activities is gathered, that data may be kept indefinitely. There is now a data hoard. Once created, the hoard can be continually rifled to investigate us but without any effective oversight. In short, data hoards present new ways to harm associational freedom.

Yet, in the face of these new surveillance threats, our current understanding of associational freedom is thin. We over-focus on speech and miss the importance of the precursors to speech—the ability to meet or network and to share, explore, accept, and reject ideas and then choose whether to speak. Recent work has shown, however, that the Constitution protects associational activities, because they enable self-governance and foster the potential for speech. That work has looked to the First Amendment. I show that these concerns also appear in Fourth Amendment jurisprudence and work to protect us from surveillance regardless of whether an act is speech or is shared with others including third parties.

The Article then examines the implications of the growing technology of backward-looking surveillance for Fourth Amendment jurisprudence. Notably, warrant procedures should be updated, building especially on the idea of return, which requires the government to return items taken as part of an investigation once they are not needed. In our new era of backward-looking surveillance, the idea of return requires deletion of data after an investigation. This shift will allow access to data but limit the ability to overreach and threaten associational freedom. When new surveillance techniques threaten associational freedom, they must be subject to proper constitutional limits. This Article explains why those limits are needed, when they must be in place, and how they operate.

INTRODUCTION

Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.

—Justice Sonia Sotomayor, United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

[I]n any normal sense of the word [privacy] . . . there would be an uneasiness, and I think a justified uneasiness, if those who patronized [a] bar felt that their names were being taken down and filed for future reference [by the government]. . . . [M]ost of

us would feel that . . . a dossier on every citizen ought not to be compiled even if manpower were available to do it . . . .

—William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 9–10 (1974).[1]

The Constitution demands that we limit law enforcement and domestic intelligence precisely when it has become too easy to conduct surveillance, because that power threatens core aspects of our democracy.[2] To date, we have treated forward-looking surveillance and backward-looking surveillance differently. Changes in technology call this distinction into question and in some cases makes it untenable. Surveillance can reveal our activities and associations, but forward-looking surveillance has limits. Surveillance such as wiretapping and using a GPS tracker often requires a warrant and must relate to criminal activity. Judges review surveillance procedures before they are deployed. The warrant will be specific about what information may be collected, how it is collected, and how it can be used. The surveillance is also time limited and requires continual justification to a judge, or the surveil-

1 The former Chief Justice was a Justice when he wrote this article.

2 *Accord* Swire, Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1310–15 (2004) [hereinafter Swire, *System of Foreign Intelligence*] (detailing the history and logic behind limits on law enforcement and domestic security use of surveillance). Although foreign intelligence operates under different and arguably more lenient rules than law enforcement and domestic security, the concern for safeguarding rights and democratic process can be seen in that realm too. *See, e.g.*, RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 154 (2013) ("The special protections [under FISA] for United States persons must therefore be understood as a crucial safeguard of democratic accountability and effective self-governance within the American political system. In light of that history and those concerns, there is good reason for every nation to enact *special* restrictions on government surveillance of those persons who participate directly in its own system of self-governance."). Orin Kerr has argued that the Supreme Court seeks equilibrium between law enforcement and criminals. Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 480–81 (2011). This Article agrees that the Court seeks balance but argues there are different equilibriums the Court seeks, that protecting associational freedom is part of that analysis, and that striking a balance between citizens' rights and surveillance is part of the balancing as well. *See infra* notes 170–82; *see also* Paul Ohm, *The Fourth Amendment in a World Without Privacy*, 81 MISS. L.J. 1309, 1341–45 (2012) (questioning Kerr's approach to equilibrium as a "balance sheet approach" that "does little more than justify the rules we have today"). This Article agrees with Swire's argument "that the reasonableness doctrine offers the best opportunity to [address] unconstrained discretion in high-tech searches" and that "'minimization' of intrusive surveillance and procedural checks against standardless or discriminatory surveillance" are the levers to fashion a solution. Peter Swire, *A Reasonableness Approach to Searches After the* Jones *GPS Tracking Case*, 64 STAN. L. REV. ONLINE 57, 58 (2012) [hereinafter Swire, *A Reasonableness Approach*]. I augment this point by showing how association animates the nature of the reasonableness inquiry.

lance will be shut down. With backward-looking surveillance all these protections are gone. Law enforcement or intelligence services[3] need only ask a business for the record of where we went, whom we called, what we read, and more.[4] They then have a near perfect picture of our activities and associa-

3 This Article focuses on law enforcement and domestic security, which are different from foreign intelligence. *See, e.g.*, Swire, *System of Foreign Intelligence*, *supra* note 2, at 1341–42. In simplest terms, law enforcement and domestic security operate under different and more restrictive rules than foreign intelligence. *Id.* at 1341 ("The 1967 *Katz* and *Berger* decisions overruled *Olmstead* and emphasized the strong constitutional limits on how electronic surveillance could be used for law enforcement purposes. The constitutional mandates for law enforcement wiretaps notably included notice to the target once a wiretap was concluded and the ability of defendants to confront the wiretap and other evidence against them." (footnote omitted)). The 1972 *Keith* case held that the Fourth Amendment requires a prior warrant for electronic surveillance in domestic security matters. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 319–21 (1972); *accord* Swire, *System of Foreign Intelligence*, *supra* note 2, at 1312–15 (explaining the "The Law and Logic of National Security Wiretaps"). The Court has nonetheless made a distinction between law enforcement pursuing "ordinary crime" and domestic security, because domestic security can involve a different set of circumstances. *See Keith*, 407 U.S. at 322; *see also* Swire, *System of Foreign Intelligence*, *supra* note 2, at 1315 (noting that the Court's concerns regarding limits on domestic security were similar to concerns raised about managing security after the September 11 attacks on the United States). Foreign intelligence is a separate realm focused on surveillance of "foreign powers." *See* 50 U.S.C. § 1801(a)(1) (2012). Foreign power is a broad term in this context. *See* Swire, *System of Foreign Intelligence*, *supra* note 2, at 1320–21 (explaining that the definition includes "any 'foreign government or any component thereof, whether or not recognized by the United States,' . . . a 'faction of a foreign nation,' or a 'foreign-based political organization, not substantially composed of United States persons,' [and] [e]ven in 1978, the definition also included 'a group engaged in international terrorism or activities in preparation therefor'" (quoting 50 U.S.C. § 1801(a) (2000))). A key concern in drawing the line between foreign intelligence and domestic security is to protect U.S. persons—U.S. citizens and permanent residents—from surveillance. *See* 50 U.S.C. § 1801(i). Thus revelations about the NSA's surveillance programs cause greatest concern when they touch on domestic security and surveillance of U.S. persons. That said, the techniques the NSA has used to gather and analyze data can be used by law enforcement and domestic security, and in that sense, this Article seeks to address the implications of those techniques for those arenas.

4 Section 215 of the PATRIOT Act changed FISA to allow for orders compelling third parties to produce business records and other tangible objects. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified as amended at 50 U.S.C. § 1861(a)(1)). To obtain such records the government must give "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant" to an authorized investigation intended to protect "against international terrorism or clandestine intelligence activities." USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192, 196 (codified as amended at 50 U.S.C. § 1861(b)(2)(A)). For an explanation of the expansion of government powers under FISA to include the use of trap and trace and the pen register as well as the changing views on compelling third party records, see CLARKE ET AL., *supra* note 2, at 79–86.

tions regardless of whether they are criminal.[5] There is thus an asymmetry that makes little sense.

Consider tracking. The FBI has stated a preference for using a warrant when using a GPS tracker.[6] If the FBI wishes to track someone for the next twenty days with a GPS tracker, it will go through warrant procedures and adhere to them.[7] If there is a misstep in obeying the warrant, the evidence gathered can be thrown out.[8] Yet, why go through the process of obtaining a warrant, placing a device on a car, retrieving the device, and adhering to all the steps a warrant requires? The FBI can instead identify a suspect, wait twenty days, and find the same information for those twenty days with almost no process.[9] It can even ask for records for more than the twenty days it wanted to start; and arguably as far back as third party records are kept. Worse, once the data is gathered, the gatherer may keep that data indefinitely. They have a data hoard. That hoard grows with each new data request.

Once created, the hoard can be continually rifled to investigate us but without any effective oversight.[10] But desire does not make the practice cor-

5 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring); Berger v. New York, 388 U.S. 41, 65–66 (1967) (Douglas, J., concurring); *accord* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. Rev. 112, 114 (2007) ("In the Information Age, a massive amount of data about our lives—data that may pertain to First Amendment activities—is maintained by third-party businesses and organizations.").

6 *See infra* notes 165–66. There is a debate about when tracking requires a warrant. And there is an open question whether other modes of tracking such as use of cell tower geolocation data that provide the same or similar information as GPS trackers requires a warrant. *Id.* This Article addresses the question as one of associational freedom. The Article offers that this approach is not technology specific and so overcomes some of the technology specific issues that arise in surveillance law.

7 Fed. R. Crim. P. 41(e)(2)(C).

8 That is what happened in *Jones*. *See Jones*, 132 S. Ct. at 948.

9 *See generally* Daniel J. Solove, The Digital Person: Technology and Privacy in the Information Age 165–75 (2004) (comparing subpoena procedures to obtain records from third parties and warrant procedures).

10 Oversight of surveillance matters for both forward- and backward-looking surveillance. As Peter Swire has argued, two cases, *Delaware v. Prouse*, 440 U.S. 648 (1979), and *Jones*, 132 S. Ct. at 945, show that the Court is concerned with the lack of oversight. *See* Swire, *A Reasonableness Approach*, *supra* note 2, at 58 ("The unanswered questions from the *Jones* argument thus suggest that the Court is seeking a new, as-yet unarticulated way to constrain police and government discretion to conduct unprecedented surveillance. The proposal here is that the answer lies in addressing what the Supreme Court in *Delaware v. Prouse* called 'standardless and unconstrained discretion,' and what Justice Sotomayor called 'unfettered discretion' in her concurrence in *Jones*." (quoting *Prouse*, 440 U.S. at 661; *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring)). The problem of being able to evade oversight procedures appears in the foreign intelligence arena as well. *See* Clarke et al., *supra* note 2, at 105, 118 (noting "several significant compliance issues" regarding the NSA's bulk collection of telephony metadata and recommending that such data not be stored by the government as a way to "reduce the risk, both actual and perceived, of government abuse").

rect. When a calamity occurs, the outcry about what the government could or should have done to prevent the event is fierce.[11] As President Obama has said, "if another 9/11 or massive cyber attack occurs, [executive actors] will be asked by Congress and the media why they failed to connect the dots."[12] Other crimes—child abductions, serial killing, shooting sprees—spur the same response.[13] It is the executive's job to police and protect us. It is society's job to set out the limits on that duty. Having access to data may make law enforcement and intelligence services more efficient. But efficiency and ease are not the touchstones of the Constitution's approach to surveillance.[14]

Fourth Amendment jurisprudence and the reasonable expectation of privacy test are supposed to calibrate the limits on law enforcement and domestic intelligence surveillance, but the analysis gets lost in asking whether something is private or public. Because of the obsession with privacy as secrecy, the inquiry does not protect public acts, even limited ones such as acts that have been disclosed to third parties.[15] Yet many acts are important even if they have not been kept secret. Freedom from surveillance is important, because surveillance undermines associational freedom.

I argue that protecting associational freedom is a core, independent, yet underappreciated part of the Fourth Amendment. If we recapture that function, we will see how to limit all manners of surveillance. Until we do that, government will be able to achieve a type of total surveillance that threatens associational freedom.[16]

---

11 This problem can be understood as the tradeoff between short-term and long-term privacy protection. *See, e.g.*, Swire, *System of Foreign Intelligence*, *supra* note 2, at 1350 ("In the short term, when asked whether they would support a specific measure to fight terrorism, many people would support the measure. Support for new security measures would be especially high in the midst of a crisis. On the other hand, especially as the crisis eases, many people would then support overall measures that reduce the risk of a 'Big Brother' society.").

12 Barack Obama, *Transcript of President Obama's Jan. 17 Speech on NSA Reforms*, WASH. POST (Jan. 17, 2014), http://www.washingtonpost.com/politics/full-text-of-president-obamas-jan-17-speech-on-nsa-reforms/2014/01/17/fa33590a-7f8c-11e3-9556-4a4bf7bcbd84_story.html [hereinafter *Transcript of NSA Reform Speech*].

13 *Cf.* Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 16 (2008) ("Once governments have access to powerful surveillance and data mining technologies, there will be enormous political pressure to use them in everyday law enforcement and for delivery of government services.").

14 *Cf.* Harold J. Krent, *Of Diaries and Data Banks: Use Restrictions Under the Fourth Amendment*, 74 TEX. L. REV. 49, 83 (1995) ("Pleas for governmental efficiency may too easily override concern for individual rights [as protected by the Privacy Act]."); Ohm, *supra* note 2, at 1341–47 (arguing that "excessive government power will justify creating artificial police inefficiency").

15 *See generally* SOLOVE, *supra* note 9, at 165–75 (comparing subpoena procedure to obtain records from third parties and warrant procedures).

16 Justice Sotomayor has expressed this concern. United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) ("I would also consider the appropriateness of entrusting to the Executive, in the absence of any oversight from a coordinate branch, a tool so amenable to misuse, especially in light of the Fourth Amendment's goal to curb

Associational freedom protects acts that support and foster speech, but that protection exists regardless of whether speech occurs. Associational freedom is about the acts—such as the right to petition, to assemble, to read, to coordinate activity, to use social networks, to march, and more—that are not speech and are often not private, but provide the foundation for public speech, dissent, and democracy.[17] Associational freedom is thus about something other than expressive speech[18] and something other than privacy as secrecy from everyone. In current terms, associational freedom is about the power of networking.[19] Diverse, challenging, and dissenting speech is core to our democracy.[20] But to have the possibility of that speech, we need to share and develop ideas free from government surveillance so we can choose whether to speak, and if we do speak, what to say.[21] Without associational freedom, our power for self-governance erodes.[22] Preventing the state from hidden, pervasive watching, recording, and tracking where we go enables associational freedom, because we need to be able to meet, share ideas, and choose whether to assemble, petition, vote, or take other action in public. Although those acts may not be fully private in that two or many more people may be involved, they still need to be private from government oversight.

Since the Founding, the executive branch, in multiple periods, has used aggressive methods to suppress speech and associations it does not like.[23] In some cases the attacks were on what was said or the ability to meet; in others

---

arbitrary exercises of police power to and prevent 'a too permeating police surveillance.'" (quoting United States v. Di Re, 332 U.S. 581, 595 (1948))).

17 Several scholars have done work on what might be called the First Amendment privacy project. *See infra* Section I.B. For example, Neil Richards has called many of these interests intellectual privacy. Neil M. Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387, 387 (2008). I agree with his claims and most of his ideas, but I diverge from Richards, who relies on the First Amendment and speech, especially as he sets aside association and distances it from his idea of freedom of thought in his analysis. *See id.* at 426. I argue that the Court has protected these "free thinking" interests as part of association, for reasons independent of speech or privacy. In that sense I hope to augment the First Amendment privacy project and provide further grounding protection for associational freedom from within Fourth Amendment jurisprudence.

18 *See generally* Ashutosh Bhagwat, *Associational Speech*, 120 YALE L.J. 978 (2011) (demonstrating that associational rights historically were independent of free speech and press rights).

19 *See* Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment*, 90 N.C. L. REV. 1371, 1374 (2012) (arguing there is a "profound connection between social networking and freedom of association" and exploring the tension between the need to share information to build networks and associate and the potential privacy harms when the state interferes with that sharing).

20 *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964) (noting that there is "a profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open, and that it may well include vehement, caustic, and sometimes unpleasantly sharp attacks on government and public officials").

21 *Cf.* Richards, *supra* note 17, at 391 ("If we are interested in a free and robust *public* debate we must safeguard its wellspring of *private* intellectual activity.").

22 *See* Bhagwat, *supra* note 18, at 989.

23 *See infra* Section I.A.

widespread surveillance was used to shut down dissent.[24] Regardless of the mode, the transgressions occurred as part of trying to preserve law and order or protect national security in the face of real threats, but the Court has still held those acts unconstitutional.[25]

Today we have new a problem. Two distinct but related types of surveillance raise associational concerns. One type of surveillance looks forward. It allows the government to track everywhere we go. The other looks backward and seems less harmful. But that backward-looking surveillance allows the government to threaten associational freedom as much, if not more than the real time spying with which we are familiar.

Unlike the past, we live in an explosion of data-generating devices and activities, and they tell much about what we do, our health, and our politics. According to the Pew Center, as of January 2014, 90% of Americans own cell phones and 58% of those are smart phones.[26] In addition, 42% of Americans use a tablet and 32% an e-reader.[27] People use these devices to check email, text, surf the web, post to social networks, and get directions, with 64% engaging in online use on their phones and 34% using phones for their main online activity.[28] Many users find these devices indispensible, with almost 30% saying they can't "imagine living without" their cell phone.[29] More than 100 billion apps were downloaded in 2013 and some project that number to reach more than 250 billion by 2017.[30] Teens send about sixty texts a day, and adults about half that depending on age.[31] One might think

24 The 1976 Church Committee Report, which investigated intelligence practices of the government, recognized that surveillance by means of bugs, wiretaps, and more, captured "vast amounts of information about the personal lives, views, and associations of American citizens." S. REP. NO. 94-755, bk. 2, at 5 (1976); *see* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1445 (2011) (stating that intergovernmental gathering and sharing of intelligence has been used to monitor and disparage political dissent); Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1937–38 (2013) (detailing international, domestic, dictatorial, and democratic regimes using similar tactics in recent years); Swire, *System of Foreign Intelligence*, *supra* note 2, at 1315 (noting the Supreme Court's recognition of the potential for abuse in domestic security wiretaps, such as the temptation to oversee political dissent).

25 *See infra* Sections I.A–B.

26 *See Mobile Technology Fact Sheet*, PEW RESEARCH INTERNET PROJECT (Jan. 2014), http://www.pewinternet.org/fact-sheets/mobile-technology-fact-sheet/.

27 *Id.*

28 *Id.*

29 *Id.*

30 *See* Ingrid Lunden, *Gartner: 102B App Store Downloads Globally in 2013, $26B in Sales, 17% from In-App Purchases*, TECHCRUNCH (Sept. 19, 2013), http://techcrunch.com/2013/09/19/gartner-102b-app-store-downloads-globally-in-2013-26b-in-sales-17-from-in-app-purchases.

31 *See* Alex Cocotas, *Chart of the Day: Kids Send a Mind Boggling Number of Texts Every Month*, BUSINESS INSIDER (Mar. 22, 2013), http://www.businessinsider.com/chart-of-the-day-number-of-texts-sent-2013-3. Monthly, 18–24 year olds send/receive around 3800 texts monthly; 25–34 year olds about 2200; 35–44 year olds about 1500; 45–54 year olds about 1000; and those over 55 about 500. *Id.*

much of the activity is frivolous, yet mobile computing is used for politics. The number of Americans who use cell phones to track political issues went from 13% in 2010 to 28% in 2014.[32] And 16% of Americans used social media to follow political figures and issues in 2014; that is up from 6% in 2010.[33] All these activities generate and log data in detail and volume like never before. Because of them, the government can easily gather data and learn about where someone has been or with whom someone spoke.

These technologies play a "vital role" in "private communication,"[34] and the laws of ten, fifteen, or thirty-five years ago could not contemplate these changes in behaviors and their implications.[35] As an example, consider metadata. Metadata is usually defined as time, date, from whom, and to whom a message is sent but can also include a URL for a website.[36] The analogy is to address or routing information on an envelope.[37] That view seems to indicate that metadata reveals little. Yet, metadata can be used to figure out someone's political interests, social network, interest in semiautomatic weapons, whether he called a suicide hotline, health conditions, and more.[38] To date, the fights over access to metadata turn on whether it is content or non-content and whether it is public or private. But metadata and other data that reveals our associational activity is not speech nor is it private.[39] Trying to force protection for that data into those rubrics fails to offer a coherent, constitutionally grounded explanation and solution as to why,

32 *See* Aaron Smith, *Cell Phones, Social Media, and Campaign 2014*, PEW RESEARCH INTERNET PROJECT (Nov. 3, 2014), http://www.pewinternet.org/2014/11/03/cell-phones-social-media-and-campaign-2014/.

33 *Id.*

34 Katz v. United States, 389 U.S. 347, 352 (1967).

35 *Accord* Julian Hattem, *NSA Phone Program Faces Key Test*, THE HILL (Nov. 2, 2014) (the "explosion of data" changes the facts from what they were in 1979 under *Smith v. Maryland* and changes the legal outcomes); *see also* Miller v. United States, 425 U.S. 435 (1976) (holding phone data exposed to third part phone company had no reasonable expectation of privacy).

36 *See* STEVEN M. BELLOVIN, SUBMISSION TO THE PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD: TECHNICAL ISSUES RAISED BY THE § 215 AND § 702 SURVEILLANCE PROGRAMS 5–7 (July 31, 2013), *available at* https://www.cs.columbia.edu/~smb/papers/PCLOB-statement.pdf.

37 *Id.*

38 Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014), http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/.

39 Swire, *supra* note 19, at 1404 ("U.S. courts have found no general constitutional right, however, for individuals in the realm of data privacy."); *accord* Brief Amici Curiae of the Elec. Frontier Found. et al. in Support of Appellees at 5, Klayman v. Obama, Nos. 14-5004, 14-5005, 14-5016, 14-5017 (consolidated) (D.C. Cir. Aug. 20, 2014) (arguing that the content/noncontent distinction is misleading and regardless of what one calls it, metadata "reveals highly personal information about the person and her life"); Dimitri Tokmetzis, *How Your Innocent Smart Phone Passes on Almost Your Entire Life to the Secret Service*, BITS OF FREEDOM (July 30, 2014, 4:46 PM), https://www.bof.nl/2014/07/30/how-your-innocent-smartphone-passes-on-almost-your-entire-life-to-the-secret-service/ (examining one week's metadata for one user and finding information about the subject's occupation, his girlfriend, sports interests, news reading habits, television and YouTube viewing habits, use of

when, and how data-gathering and use practices must be limited. I argue that associational freedom provides that ground and answers those questions.

One way to think of the change is the evolution of dossiers. Concern over the way government can keep dossiers on people and then misuse them is old. Popular culture nodded to that fear in the 1942 movie *Casablanca*. Major Strasser, a Nazi, tells Richard Blaine: "We have a complete dossier on you: Richard Blaine, American, age thirty-seven. Cannot return to his country. The reason is a little vague. We also know what you did in Paris, Mr. Blaine, and also we know why you left Paris." He hands the dossier to Blaine and says, "Don't worry, we are not going to broadcast it." To which Blaine quips as he reads the file, "Are my eyes really brown?"[40] Not all of us can be so glib.

The potential for dossier misuse is large. Dossier power has been a subject of scholarship and concern from the 1960s to the present.[41] Even with older analog dossiers, it is too easy to harvest, hoard, and analyze data and then step far beyond legitimate goals into acts that threaten civil liberties.[42] As no less than then-Justice Rehnquist said in the early 1970s, "most of us would feel that . . . a dossier on every citizen ought not to be compiled even if manpower were available to do it."[43] Digitization increased the problems. It still took time to generate dossiers, but instead of having to root through file cabinets, cross-reference, and connect dots, digitization allowed dossiers to be searched and easily shared. Data is the next big step in dossier production and analysis. In Rehnquist's terms, manpower and costs are no longer barriers to modern dossier building.

---

three email accounts to manage commercial, personal, and work correspondence, his different social networks, and more).

40 CASABLANCA (Warner Bros. 1942).

41 *See, e.g.*, KENNETH C. LAUDON, DOSSIER SOCIETY (Rob Kling & Kenneth L. Kraemer eds., 1986) (analyzing the use of computerized criminal history systems); HERBERT MITGANG, DANGEROUS DOSSIERS (1988) (documenting the government's maintenance of dossiers on writers and thinkers such as Ernest Hemingway, Dorothy Paker, Dashiell Hammett, Thornton Wilder, Edmund Wilson, Graham Greene, and methods of infiltrating groups to assemble the dossiers); ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE (Stanton Wheeler ed., 1969) (examining the way educational, economic, governmental, and welfare institutions generated dossiers and the law about access to those dossiers); SOLOVE, *supra* note 9, at 1–26 (investigating the problems of digital dossiers).

42 *See, e.g.*, CLARKE ET AL., *supra* note 2, at 154; Citron & Pasquale, *supra* note 24, at 1458–63 (detailing ways that data gathering and analysis programs for domestic intelligence programs have enabled "surveillance of political, racial, ethnic, and religious groups" and inclusion of a journalist and blogger on a threat list based on his writings); *cf.* Randy Barnett, *Knowledge Is Power: How the NSA Bulk Data Seizure Program Is Like Gun Registration*, WASH. POST, Jan. 21, 2014, http://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/01/21/knowledge-is-power-how-the-nsa-bulk-data-seizure-program-is-like-gun-registration/ (arguing that even if bulk data collection were legal it provides too much power in one place).

43 William H. Rehnquist, *Is an Expanded Right of Privacy Consistent with Fair and Effective Law Enforcement? Or: Privacy, You've Come a Long Way, Baby*, 23 U. KAN. L. REV. 1, 10 (1974).

Dossiers of where we go and with whom we meet are created automatically as we go through our daily lives. They reside with cell phone, Internet, search, email, e-commerce, credit, and almost any service we use. The tremendous power of the state to compel production of this information combined with what the state can do with technology and data creates a moral hazard. As Justice Sotomayor put it, "the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[44] Once the government has obtained data, it is easy and inexpensive to store and search. Thus, the data is not deleted or destroyed; it is hoarded.[45] That vat of temptation never goes away.[46] The lack of rules on the government's use of the data explains why it has an incentive to gather data, keep it, and increase its stores. After the government has its data hoard, the barriers to dragnet and general searches—ordinarily unconstitutional—are gone. If someone wishes to dive into the data and see whether embarrassing, or even blackmail-worthy, data is available, they can do so.[47] These temptations are precisely why we must rethink how we protect associational freedom in the age of data hoarding. By understanding what associational freedom is, what threatens it, and how we have protected it in the past, we will find that there is a way to protect it now and in the future.

Part I of this Article establishes the role and history of associational freedom. Most analysis of the First Amendment and privacy draws on the speech and expressive aspects of the First Amendment. That move misses the way in

44 United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

45 Although the Privacy Act of 1974, 5 U.S.C. § 552 (2012), is supposed to address the problems of government data storage and use, the limits on the Act's reach and the carve outs for law enforcement blunt its power for the issues this Article addresses. *See* Krent, *supra* note 14, at 83 ("[T]he Privacy Act places no restrictions whatsoever on criminal law enforcement use, regardless of how the government obtained the information. And the definition of routine use has evidently expanded exponentially."). The PRISM program appears to have some limits on storage, but these are still long (five to ten years) and seem to be self-imposed. *See* James Risen & Laura Poitras, *N.S.A. Gathers Data on Social Connections of U.S. Citizens*, N.Y. TIMES, Sept. 28, 2013, http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html?pagewanted=all ("[A]n internal briefing paper from the N.S.A. Office of Legal Counsel showed that the agency was allowed to collect and retain raw traffic, which includes both metadata and content, about 'U.S. persons' for up to five years online and for an additional 10 years offline for 'historical searches.'").

46 *See* Citron & Pasquale, *supra* note 24, at 1463–64 (noting the potential for "[m]ission [c]reep" as data gathered for one purpose such as anti-terror actions can be used to address almost "all threats" but without the oversight and grounding that was in place when a project began).

47 The history of United States abuse of surveillance includes use of information against political opponents, attempts to undermine disfavored groups and movements, and use of the fear that all mail is being opened. *See* MORTON H. HALPERIN ET AL., THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES (1976); Swire, *System of Foreign Intelligence*, *supra* note 2, at 1317–19. For the extreme possible outcome of surveillance as practiced outside the United States, see Richards, *supra* note 24, at 1953–54 (detailing instances of blackmail and rules against using communist secret police files because of the threat of blackmail).

which the First Amendment protects non-speech activity. I draw on recent First Amendment scholarship to show that associational freedom has its own logic. It is an independent interest that reaches many activities and things—such as the data we generate as we engage in associational activities—that do not qualify as expressive speech and that we nonetheless protect. Just as First Amendment analysis can be myopic and look only to speech, Fourth Amendment analysis can miss interests other than privacy as secrecy. I examine Fourth Amendment jurisprudence and show that it too protects associational freedom as an independent interest. For example, in both *Berger v. New York*[48] and *United States v. Jones*,[49] associational freedom was an underlying rationale for questioning and limiting surveillance. Drawing on these two strains of thought, I show that the Constitution demands strong, but not absolute, limits on the government's ability to interfere with associational freedom.

Part II explains the way we balance law enforcement's need for surveillance and society's need for associational freedom. I show how associational freedom informs and shapes warrant procedures for forward-looking surveillance, especially when technology allows the government to watch and track us easily and at low cost. I then argue that the potential harms of forward-looking surveillance reappear in backward-looking surveillance. Because our lives now create precise records with extreme detail of what we do, those records enable backward-looking surveillance. They also create a large temptation to engage in overreaching surveillance. Much of the data that raises concerns, however, is not covered by warrants and is easily accessible. This Part concludes by explaining how historical and recent government surveillance chills associational freedom and by showing how data aggravates that problem.

Data hoards are not going away, but that does not mean there should be unfettered access to them. Part III applies associational freedom as I have developed it to surveillance and data hoards. I set out what discipline for data hoards should look like. I also address distinctions between different types of data gathering and show how to distinguish amongst different data hoards and their threats to associational freedom.

In short, we have lost our way. We apply rules based on tangible, high-cost analog things to a world of ever-changing, digital surveillance and to data that is inexpensive to gather and store, easy to analyze, and that can be put to many uses.[50] Many of these uses threaten associational freedom but

48 388 U.S. 41, 64–66 (1967) (Douglas, J., concurring).

49 132 S. Ct. at 956 (Sotomayor, J., concurring).

50 *Cf.* Riley v. California, 134 S. Ct. 2473, 2489 (2014) (requiring a warrant before searching an arrestee's cellular phone because of the quantitative and qualitative difference between searching notes in one's pockets and the material stored on a cell phone); *id.* ("A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom."). The Court explicitly stated that the ruling did not reach Fourth Amendment

are unregulated. There is, however, hope. Returning to insights from Fourth Amendment jurisprudence addressing technology and surveillance explains the associational problems in both forward- and backward-looking surveillance and reinvigorates our standard for protecting that freedom. This approach thus offers a foundation for calls to protect us from law enforcement's ability to probe our reading, meeting, and gathering habits—our associational freedom—even though those acts are not private or speech, and it explains what the constitutional limits on surveillance in the age of data hoarding must be.

I. The Constitution Favors Enabling and Making Associations

Protecting associational freedom as an independent, core right is an underappreciated aspect of the Constitution.[51] From the Founding to the present, Americans have assembled to share ideas, debate, organize, demonstrate, plan petitions, engage in philanthropy, and more. The way those activities occur has changed over time. Early groups relied on word of mouth, letters, newspapers, and pamphlets to build associations and in some cases take action. Then came the telephone, and the ability to organize expanded and was less public. Today, blogs, social networks, email, mobile phones, and the Internet in general have increased associational activities.[52] At each stage, government has sought to watch these activities and sometimes prevent them. Just as the advent of wiretaps, bugs, and other novel government surveillance methods spawned landmark cases in Fourth Amendment law and legislation to govern the surveillance of the day, the government's ability to track us with GPS technology and to grab vast amounts of data about where we go, what we read, who we meet, and more demand a new approach to managing modern surveillance.[53] Without such action our asso-

issues related to "the collection or inspection of aggregated digital information"—the issue this Article addresses. *Id.* at 2489 n.1. "Because the United States and California agree that these cases involve *searches* incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.*

51 Underappreciated does not mean no work has been done. Work by Tabatha Abu El-Haj, Ashutosh Bhagwat, John Inazu, and Jason Mazzone has laid the foundation to recapture association as an independent right. *See, e.g.*, Tabatha Abu El-Haj, *The Neglected Right of Assembly*, 56 UCLA L. Rev. 543, 589 (2009) ("[T]he right of assembly should not be collapsed into the right of free expression."); Bhagwat, *supra* note 18 (demonstrating that associational rights historically were independent of free speech and press rights); John D. Inazu, *The Forgotten Freedom of Assembly*, 84 Tul. L. Rev. 565 (2010) (exploring the history of the freedom of assembly and the consequences of its declining importance in American legal and political theory); Jason Mazzone, *Freedom's Associations*, 77 Wash. L. Rev. 639 (2002) (analyzing popular sovereignty, not free speech, as the basis for freedom of assembly).

52 *See* Swire, *supra* note 19, at 1377–80 (discussing the role that social networks, Internet, blogs, and email play in creating associations).

53 *See* Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. Rev. 741, 797 (2008) ("[T]his Article

ciational freedom is in jeopardy, for if we don't protect the infrastructure of associational freedom, future speech or action that might emerge is thwarted.

Associational freedom is not only vital, yet misunderstood, within First Amendment jurisprudence; it underlies key aspects of Fourth Amendment jurisprudence. Recognizing this function reveals why and how we must manage surveillance.[54] It also shows that these concerns are not about whether an act or data is public or private. The solution will end up relying on new procedures to address data gathering, analysis, and storage. That result may seem obvious. Yet, such a shift would regulate the ability to use forward-looking surveillance *and* the ability to engage in backward-looking surveillance. Analysis of Fourth Amendment jurisprudence shows that the Fourth Amendment protects associational freedom. General warrants, dragnet searches, and other broad approaches to surveillance are not allowed. The reason we don't allow them is not a reasonable expectation of privacy logic as it is currently understood. We don't allow such practices, because they go to the heart of how the state may misuse its power to chill, if not eliminate, noncriminal activities it doesn't like. In short, the Constitution protects associational freedom.[55]

A. Associational Freedom Protects Acts Other than Speech

Protecting associational freedom as an independent right, separate from speech, unlocks the sort of political engagement and freedom of thought the Constitution fosters and requires.[56] Individuals and groups need space to meet and network and to share, explore, accept, and reject ideas and then choose whether to speak; these are the sorts of activities associational freedom shields. As discussed further below, recent changes in computing, data, and online practices are creating a decisive shift from forward-looking to

therefore considers how the First Amendment, as interpreted in light of modern technology, might serve as an independent source of limitations on relational surveillance.").

54 Daniel Solove and Katherine Strandburg have written about First Amendment connections to Fourth Amendment doctrine and association. *See* Solove, *supra* note 5, at 132–33; Strandburg, *supra* note 53, at 768–93. Both identify and explain ways in which First Amendment concerns are important to and might discipline Fourth Amendment information gathering issues. This Article agrees with many of their insights and seeks to build and advance them by drawing on and applying recent First Amendment scholarship. In addition, this Article adds to the analysis and argues that Fourth Amendment jurisprudence recognizes associational freedom as a Fourth Amendment matter.

55 *Cf.* Solove, *supra* note 5, at 163–64 (explaining that the Court has "pollinate[d] one amendment with concepts from another" and that "[a] close relationship . . . exists between the First and Fourth Amendments").

56 *See, e.g.*, Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis & Holmes, JJ., concurring) ("Those who won our independence believed that the final end of the State was to make men free to develop their faculties . . . . They believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth . . . ."); *see also* Richards, *supra* note 17, at 395–98 (tracing the different ways freedom of thought has been described as an integral act protected by the Constitution).

backward-looking investigations. These technological shifts make the risks to associational freedom far more acute, in part because today much of the infrastructure that enables association flows through third party technologies.[57] Privacy scholars agree that the Fourth Amendment does not protect association well, in part because the Supreme Court has not recognized a reasonable expectation of privacy in data given to a third party.[58] That observation is correct.[59] It does not, however, address associational freedom. Thus privacy scholars have looked to the First Amendment to remedy the gap in Fourth Amendment law. Daniel Solove has argued that "the First Amendment itself must be understood as an independent source of criminal procedure rules."[60] Following that logic, Kathy Strandburg has looked specifically at the problem of association, surveillance, and networks. Strandburg looks to associational interests to support why we should limit techniques that detect patterns of association or associational activity but relies on the idea of "expressive and intimate associations" as the defining characteristics of the sorts of associations that are protected.[61] She seeks to address the government's ability to gather and analyze public data to find out member lists, which she sees as impinging on freedom of association.[62] But Strandburg follows the idea that freedom of association is about expressive association: "The inquiry therefore must focus not on whether a specific association is 'expressive,' but on the likelihood that a particular instance of relational surveillance will disclose membership in expressive associations."[63] This posi-

57 Solove, *supra* note 5, at 126–27 ("In the past, much speaking, association, and reading occurred in secluded places, walled off from the rest of the world. But with modern technology, First Amendment activity occurs via e-mail, the Internet, and the telephone. It is no longer confined to private zones such as the home and no longer benefits from Fourth Amendment protection.").

58 *See, e.g.*, Solove, *supra* note 5, at 123–27 ("The ability to keep personal papers and records of associational ties private is a central First Amendment value. But despite their First Amendment importance, the broad subpoena power and the Fourth Amendment's third-party doctrine leave these documents unprotected from government scrutiny."); Strandburg, *supra* note 53, at 770 ("[T]he Supreme Court generally has not found a reasonable expectation of privacy either in information that has been conveyed to a third party or in communication traffic data."); Swire, *supra* note 19, at 1404 ("U.S. courts have found no general constitutional right, however, for individuals in the realm of data privacy.").

59 *See infra* notes 109–10.

60 Solove, *supra* note 5, at 117.

61 Strandburg, *supra* note 53, at 744, 749 ("Current legal doctrine, which centers on 'privacy' and hence on protecting the content of communications, does not adequately account for the extent to which relational surveillance threatens to chill expressive association in today's networked world.").

62 *See id.* at 794 ("Extensive government relational surveillance using network analysis data mining techniques poses a serious threat to liberty because of its potential to chill unpopular, yet legitimate, association, and also because of the chilling of legitimate association caused by possibly incorrect assessment of both legitimate and illegitimate associational membership.").

63 *Id.* at 802.

tion leaves an open question: What protection exists for associational activity that is not expressive or potentially expressive? I agree about the need to protect associational activity, but I argue that the broader notion of association in the First and the Fourth Amendment as presented here—one that looks beyond expressive association—provides greater protection for associational freedom as threatened by the power of new data generation and analysis and modern surveillance techniques.[64]

In simplest terms, associational freedom is about and protects the activities that can foster speech and lead to self-governance. Recent scholarship has shown that the right of association is an important right and distinct from speech.[65] The right is not set out in the Constitution;[66] it flows from the assembly and petition rights in the First Amendment.[67] At and even before the Founding, assembly, petition, and association rights "were essential components of political activism" that predated speech rights.[68] Originally, assembly referred to "ad hoc gatherings of citizens," and associations to "more permanent . . . organizations."[69] Assembly and association began as and are separate ideas, but the Court has conflated them over time.[70] That shift is a subtle, but powerful, mistake, because it reduces, and in some cases eliminates, proper, full protection for the acts that come before speech and are not expressive but that we need for associational freedom in any context.

The components of associational freedom work together to allow people, especially those without power, to identify problems and demand

64 One should not infer that Solove and Strandburg do not understand freedom of association. I am indebted to their work for this Article. Instead, one should note that the bulk of scholarship about association began and has continued just after the scholars had published their works, and so they did not have access to it. In other words, I seek to introduce this body of scholarship to privacy scholarship.

65 *See* Bhagwat, *supra* note 18, at 980–81.

66 *See* Ashutosh Bhagwat, *Assembly Resurrected*, 91 TEX. L. REV. 351, 358 n.55 (2012) (reviewing JOHN D. INAZU, LIBERTY'S REFUGE: THE FORGOTTEN FREEDOM OF ASSEMBLY (2012)).

67 *See* Bhagwat, *supra* note 18, at 980–81. There is some debate about whether association is a form of assembly and whether the assembly clause only protects assembly for the purpose of petitioning. *See id.* at 990–91. Nonetheless, Inazu's work has made a strong case against that position, and scholars agree that "assembly and association were essential components of political activism, from the precolonial period through the American Revolution and the nineteenth century." *Id.* at 991.

68 *Id.* at 991.

69 *Id.* at 982–83; *accord* Inazu, *supra* note 51, at 566.

70 *See* Mazzone, *supra* note 51, at 714–15 ("[A]ssembly and petition were not simply afterthoughts to free speech and free press. Rather, they originated in a separate proposed amendment. . . . Madison's original proposal combines assembly and petition in the same amendment, underscoring that these rights are linked."); *see also* Whitney v. California, 274 U.S. 357, 371 (1927) ("Nor is the Syndicalism Act as applied in this case repugnant to the due process clause as a restraint of the rights of free speech, assembly, and association.").

change.[71] The simplest aspect of this dynamic is the right to petition.[72] Petitioners "asserted not just their right to petition but also the right to 'meet together to frame and promote petitions.'"[73] Despite the *lack* of a speech right for American colonists, private grievances, public issues, and corruption were addressed by petition.[74] Petition also aided those without power. Disenfranchised groups "such as women, felons, Indians, aliens, and slaves—were nonetheless able to express their grievances, and seek benefits, through petitions."[75] Petition was influential in political fights over the Alien, Sedition, and Naturalization Act in the late 1700s, abolition, prohibition, and women's suffrage.[76] Petition thus plays an important role as part of popular sovereignty and self-governance by protecting "framing and meeting" and as a right for those who do not have speech rights, but petition reaches its full potential with another part of associational freedom—assembly.

Assemblies are not always public or expressive or engaged in petitioning or even permanent, and yet they are protected.[77] Assembly is about the ability of groups to think about, support, and dissent from (albeit peacefully) current notions of the good.[78] Some assemblies are permanent associations that combined with petitions "allow specific groups to formulate programs and demands, and to influence the course of government. Assembly in a constitutional convention permits the political collectivity—the People—to change their government entirely."[79] Assembly need not be at the level of a constitutional convention to matter. Consider the history of women's clubs. Since the time of the *Mayflower* through the Civil War to the suffrage movement, women used clubs to discuss issues frowned upon by those in power.[80] Women's ongoing and evolving role in "political life was born out of their early association with other members on the basis of shared interests and a search for solidarity."[81] Other examples of assembly were more public and temporary. Street meetings, demonstrations, election-day celebrations, parades, and strikes were common assembly practices that "played a central

71 *See* Bhagwat, *supra* note 18, at 1003; Inazu, *supra* note 51, at 612 (observing that "dissenting, public, and expressive groups [have] sought refuge under the right of assembly").

72 Petition is the formal request to the government to right a wrong or give a privilege. *See* Mazzone, *supra* note 51, at 720. The right existed in England since the thirteenth century, but by the seventeenth century, petitioning moved from being submitted mainly by individuals to being group petitions submitted by "[p]rivate associations." *Id.* at 723 (quoting David Zaret, *Petitions and the "Invention" of Public Opinion in the English Revolution*, 101 Am. J. Soc. 1497, 1525 (1996)) (internal quotation marks omitted).

73 *Id.* at 723 (quoting Zaret, *supra* note 72, at 1525).

74 *Id.* at 724.

75 *Id.* at 724–25.

76 *Id.* at 727–29.

77 Inazu, *supra* note 51, at 576–77.

78 *Id.* at 576.

79 Mazzone, *supra* note 51, at 730 (footnote omitted).

80 *See id.* at 642–44.

81 *Id.* at 644.

role in American politics through much of the nineteenth century."[82] These different, protected acts enabled and were part of political participation, but were not necessarily about direct petition or expressive speech. These acts were important ways to share ideas, persuade others to action, demonstrate the scope of support for a cause, and then petition or take other political action such as forming a more permanent political group.[83]

Of course, those in power don't always want to hear from opposing views or even let opposing groups start, let alone thrive. Members of the new American government quickly changed their minds about associations and saw them as threats to their power. No less than George Washington denounced associations in his 1796 farewell address as President.[84] The Democratic-Republican Societies, which believed that "the new government was insufficiently responsive to popular will, and that some additional mechanism was needed to keep elected officials in check," caused particular concern.[85] Much like political groups from the Tea Party to the Occupy Wall Street movement today, the societies were dispersed and sought to highlight and debate public issues, published work critical of the incumbent government, and "engaged in practical activities, like poll watching, philanthropy, [and] tracking the voting of representatives."[86] Furthermore, there is some evidence that some members of the societies participated in the Whiskey Rebellion of 1794.[87] Even though the Democratic-Republican Societies had dissolved, the Sedition Act was passed in 1798.[88] The act criminalized assembly and speech separately.[89]

The structure of the Act shows the drafters knew the difference between stopping speech and stopping the precursors to speech; if one can stop meetings and the ability to share ideas, speech and political action may never occur.[90] Section 2 is more well known and criticized for its criminalization of speech against the government (i.e., sedition). But section 1 reveals the understanding that non-speech activities are important and powerful. Sec-

82 Abu El-Haj, *supra* note 51, at 555–61.

83 *Id.* at 560 (describing the interplay between assembly and petition).

84 *See* Mazzone, *supra* note 51, at 740. Although fear of factions was part of the concern the societies raised, Mazzone shows that Washington was a "zealous critic of the early associations," and in his private letters he argued that assemblies were illegitimate because they were "self-constituted, rather than popularly elected." *Id.* at 738–39. "They are permanent assemblies, ready to criticize everything Congress does, rather than occasional gatherings in response to specific legislation." *Id.* Mazzone distinguishes modern commentators' focus on Madison and factions from Washington's hostility towards assemblies and notes that Madison urged Washington to temper his views on this point. *Id.* at 739 n.600.

85 *Id.* at 734.

86 *Id.*

87 *Id.* at 735.

88 *See* Act of July 14, 1798, ch. 74, 1 Stat. 596, 596–97 (expired 1801).

89 *Id.* §§ 1–2.

90 *Cf.* Tabatha Abu El-Haj, *Friends, Associates, and Associations: Theoretically and Empirically Grounding the Freedom of Association*, 56 ARIZ. L. REV. 53, 92 (2014) (explaining the need for individuals to be able to connect groups to have large scale political action).

tion 1 attacked associational freedom and non-speech activities by criminalizing and prohibiting people from "unlawfully combin[ing] or conspir[ing] together, with intent to oppose any measure or measures of the government of the United States."[91] Yet overt attacks on associational freedom are not the only way we can lose associational freedom.

Attacking association's infrastructure can defeat association's power. Yesterday's clubs and street meetings are today's activist groups, meet ups, and flash mobs. If one doubts that modern, data-driven and generating services foster and inform political association and action, recall that the Arab Spring, U.S. charities, and political campaigns such as the 2007 Obama campaign, Tea Party campaigns, and more have thrived by using modern networking and association technology.[92] Threats to the way these groups and other associations are formed and maintained provide another angle by which the government can undermine associational freedom. Part of the problem is that backward-looking surveillance chills association, because the government can dig into our past and find out the ideas, groups, or people we engaged with all too easily. An analog example in *NAACP v. Alabama ex rel. Patterson*[93] shows how easy it is to undermine association's infrastructure. Alabama had a law that required the NAACP to disclose "all its Alabama members and agents, without regard to their positions or functions in the Association."[94] The Court did not allow access to the NAACP member lists, because "[e]ffective advocacy" was bolstered by "group association."[95] Recent work by Tabatha Abu El-Haj shows that this position is borne out by sociology. The ability of individuals to connect disparate groups "has the potential to create 'scale shift.'"[96] A scale shift happens when individuals "'make connections among groups that would otherwise be isolated from one another' and is necessary for a major social or political transformation to occur."[97] Another important part of the *NAACP* Court's logic was that the group at issue faced threats and true violence if they were known. That idea connects to Bhagwat's insight that associational analysis often turns on protecting those out of power and the persecuted.[98] When the state requires member lists to be disclosed, it chills the willingness even to join a group. Thus fewer people will be willing to hear new ideas, let alone coordinate activity to reach the sort of scale shift that can lead to political action in general—especially by those out of power. And yet, *NAACP* started a change in

91 § 1, 1 Stat. at 596; *see also* Mazzone *supra* note 51, at 740.

92 *See* Swire, *supra* note 19, at 1371 (discussing how social networks create associations).

93 357 U.S. 449 (1958).

94 *Id.* at 451.

95 *Id.* at 460, 466.

96 Abu El-Haj, *supra* note 90, at 92.

97 *Id.* (quoting Sidney Tarrow, *Dynamics of Diffusion: Mechanisms, Institutions, and Scale Shift*, *in* THE DIFFUSION OF SOCIAL MOVEMENTS 204, 215 (Rebecca Kolins Givan et al. eds., 2010)).

98 *See* Bhagwat, *supra* note 18, at 1003–14.

perspective that hides the importance of a broad understanding of association.[99]

Losing the distinction between associational freedoms and speech incorrectly subsumes the freedoms under speech and so lessens their protection.[100] *NAACP* started the decay that turned association into a servant of speech. Although *NAACP* shows that the ability to form and sustain associations is protected, and state action that chills association (in that case the law compelling the production of the member lists) is unconstitutional, a key idea in *NAACP* was that membership was protected if it was part of free speech—"[t]he Association . . . is but the medium through which its individual members seek to make more effective the expression of their own views"—but not by itself.[101] This view leaves non-speech activities in jeopardy. As Bhagwat has shown, there is an irony in that "invok[ing] the connection with free speech . . . restrict[s] [association] by *rejecting* constitutional protection for associations that are not predominantly expressive."[102] Instead of robust protection for a range of associations and associational activities, the right of association is now afforded only to expressive associations or "freedom of an association to speak."[103] This approach reduces association and assembly from being "independent political freedom[s]" to being "an aspect of free speech."[104]

---

99 As Ashutosh Bhagwat has explained, a series of cases—from *Whitney v. California*, 274 U.S. 357 (1927), to *American Communications Ass'n v. Douds*, 339 U.S. 382 (1950)—reveal that the Court continued to see speech, press, assembly, and petition "as cognate rights that in combination constitute 'the indispensible democratic freedoms secured by the First Amendment.'" Bhagwat, *supra* note 18, at 983–86 (quoting Thomas v. Collins, 323 U.S. 516, 530 (1945)). Then came *NAACP v. Alabama ex rel. Patterson* and its progeny, and the perspective was lost. *Id.*

100 *Cf.* Abu El-Haj, *supra* note 51, at 589 ("[T]he right of assembly should not be collapsed into the right of free expression.").

101 NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 459 (1958). On a related point, when faced with a statute trying to prohibit the NAACP from aiding in litigation to which it was not a party, the Court treated litigation as part of speech and ignored the petition. Yet litigation falls under petition easily and stands on its own. *See* Bhagwat, *supra* note 18, at 986. Thus the Court was again looking to expressive speech and forgetting about associational freedom on its own.

102 *See* Bhagwat, *supra* note 18, at 988 (emphasis added) (emphasis omitted).

103 *See* Mazzone, *supra* note 51, at 678 ("Put differently, the Court purports to be analyzing freedom of association when it is really analyzing freedom of expression. The Court seems to understand associations like the Jaycees or the Boy Scouts as just like any other speaker with a message. The Court treats government regulation of membership as raising a constitutional problem only when the regulation interferes with the association's message, that is, where the presence of some individual interrupts what would otherwise be said. Freedom of expressive association is therefore reduced, in the Court's analysis, to the freedom of an association to speak.").

104 *See* Bhagwat, *supra* note 18, at 986. "[T]he Court abandoned its original insight that association and assembly, while linked to free speech and press, are cognate, independent rights." *Id.* at 988–89.

If, however, we grasp that the right of association applies to more than only expressive associations or "freedom of an association to speak,"[105] we open the door to robust protection for a range of associations and associational activities. These activities are about more than expressive speech. Ignoring this point means we recreate the problems of the Sedition Act. Recall that section 1 of the Sedition Act sought to prevent non-speech activity—"combin[ing] or conspir[ing] together, with intent to oppose any measure or measures of the government of the United States."[106] When the law focuses on and protects only expressive speech, it limits speech-enabling activity. By focusing only on expressive associations, we fail to protect associational activity that is not such speech. Instead of an obvious and easily objectionable ban on assembly, as was the case with the Sedition Act, we simply deny that assembly counts if it is not expressive. In other words, neither associational activities nor speech are spontaneously generated, and we must beware of acts or laws that attack the seeds of action and speech just as the Sedition Act sought to do.

Associations need room to form, grow, and have a chance to be part of the political process.[107] Associational freedom is a key to self-governance and must be protected to preserve our ability to self-govern.[108] Self-governance requires the ability to have private debate, coordinate activity, explore ideas, and develop arguments and skills for public engagement, without government oversight or control.[109] As Bhagwat has said, a key purpose of the First Amendment is "to protect the process of forming and maintaining" associations.[110] We need to communicate our views, build coalitions and consensus, and recruit unknown, but like-minded people.[111] We need public speech not only to attract others to associate, but to maintain associations at all, and we need associational activity that is free from government over-

105 Mazzone, *supra* note 51, at 678.

106 Act of July 14, 1798, ch. 74, § 1, 1 Stat. 596, 596 (expired 1801).

107 *See* Abu El-Haj, *supra* note 90, at 54–60; *cf.* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1912 (2013) (arguing that surveillance diminishes the capacity for "democratic self-govern[ance]" because individuals no longer have the space to develop their version of citizenship rather than one dictated or shaped by the state).

108 *See* Bhagwat, *supra* note 18, at 981.

109 *See* Solove, *supra* note 5, at 121–22 ("[P]olitical discourse does not just occur on soapboxes before large crowds; it also thrives in private enclaves between small groups of people. Freedom of speech should and does protect the ability of individuals to communicate with each other, regardless of whether the exchange of ideas occurs between two people or among a million. In other words, the First Amendment safeguards not just speeches and rallies but *conversations*. People formulate their political opinions and debate politics mostly off-stage, between friends, family, and acquaintances, among fellow religious worshippers, and within groups with shared values and commitments. Such conversations depend upon privacy. Without protection against government probing, countless conversations might never occur or might be carried on in more muted and cautious tones."); *cf.* Richards, *supra* note 17, at 387 (arguing that records of intellectual activities must be protected because those activities are vital to "free thought and expression").

110 Bhagwat, *supra* note 18, at 998; *accord* Abu El-Haj, *supra* note 51.

111 *See* Bhagwat, *supra* note 18, at 998.

sight to enable further public speech.[112] We need that freedom, because it permits dissent a chance to become action.

In short, the precursors to speech must be protected if we are to have speech and self-governance.[113] Today, the precursors to speech are fueled and mapped by our data-generating activities but are barely protected. Something deemed content—what was said on a phone or the message in an email—is given higher protection than envelope or metadata. Content fits well within standard views of speech. Envelope and metadata do not and are thus mistakenly under-protected; so much so that standard doctrine is that data handed to third parties is public and the Fourth Amendment does not protect public matters.[114] In other words, this dichotomy tracks the mistake of thinking that the First Amendment is only about speech and does not protect the means to "forming and maintaining" associations. Nonetheless, I argue that Fourth Amendment jurisprudence has a tradition of protecting associational freedom and things done in or shared with the public.

B. Associational Freedom Protects Public Acts

Like the First Amendment mistake of ignoring associational freedom as an independent interest protecting acts that are not speech, one can miss the way the Fourth Amendment protects associational freedom as something more than derivative of speech or privacy.[115] Unfortunately, as soon as the Fourth Amendment is raised, cases and scholarship are drawn to the reasonable expectation of privacy test like a black hole.[116] The emphasis is on whether an act is private rather than whether the surveillance is reasonable.[117] Many acts that are part of associational freedom are given short shrift

112 *Id.* at 998–99 ("To achieve the structural purposes of the First Amendment, therefore, one of the primary objects of First Amendment doctrine must be to protect speech, the function of which is to form and maintain associations and to communicate an association's views to outsiders—what I denote as associational speech.").

113 Roberts v. U.S. Jaycees, 468 U.S. 609, 622 (1984) ("An individual's freedom to speak, to worship, and to petition the government for the redress of grievances could not be vigorously protected from interference by the State unless a correlative freedom to engage in group effort toward those ends were not also guaranteed."); *accord* Swire, *supra* note 19, at 1385–86.

114 *Cf.* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J. concurring) (suggesting that such data will obtain constitutional protection if the Court's "Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy").

115 *But see* Solove, *supra* note 5, at 165 n.285 (acknowledging that *Berger* addresses how to tailor electronic surveillance to meet Fourth Amendment particularity requirements).

116 *Cf. id.* at 131 ("[A]lthough they overlap to some degree, the First and the Fourth Amendments protect different things. The Fourth Amendment is currently understood by the Court to protect privacy, and the test for determining the scope of the Fourth Amendment is the existence of a reasonable expectation of privacy. First Amendment activity, in contrast, can be hindered without a violation of privacy, such as when the government engages in public surveillance of political activity." (footnote omitted)).

117 *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 769 (1994). As we shall see, a reasonableness inquiry encompasses preventing or limiting sur-

because of the false belief that the Fourth Amendment only protects private, secret acts.[118] Recognizing associational protections under the Fourth Amendment brings the doctrine in line with the First Amendment and explains why certain surveillance practices should not be allowed even if the information is public.

Criminal procedure is sensitive to and protects associational freedom, but protection of associational interests is not absolute. For example, criminal associations do not receive protection.[119] Nonetheless, in *Berger v. New York*,[120] *Katz v. United States*,[121] *Kyllo v. United States*,[122] and *United States v. Jones*,[123] all of which involved surveillance of criminals, the Court raised implicit associational concerns as part of its Fourth Amendment analysis.[124] It appeared when the Court addressed the law enforcement practices at issue, the type of activity that may be affected by those practices, and the solutions offered to balance between detecting criminal activity while avoiding sweeping noncriminal activity into the detection. Thus I argue that the Court wants to ensure that associational activities are not swept up with criminal ones, because that limits the chance that surveillance will squash associational freedom and chill future associational acts.

The Fourth Amendment has a history of protecting associational freedom.[125] The Amendments trace their roots to the history of seditious libel

---

veillance that implicates associational freedom even for public acts or information. *See infra* notes 129, 173, 182 and accompanying text.

118 *Cf.* Amar, *supra* note 117, at 769 (explaining that some searches in public spaces would be unreasonable).

119 *See, e.g.*, Bhagwat, *supra* note 18, at 1008–09 (noting that criminal organizations such as the mafia are not protected as associations under the First Amendment). The First Amendment also affords less, and sometimes no, protection to certain types of speech. *See, e.g.*, Solove, *supra* note 5, at 153 ("Obscenity, fighting words, and child pornography are considered low-value speech and receive diminished First Amendment protection. The Court has also not considered conspiracy, quid pro quo sexual harassment, insider trading, and other forms of communicative activity to be protected speech." (footnotes omitted)).

120 388 U.S. 41 (1967).

121 389 U.S. 347 (1967).

122 533 U.S. 27 (2001).

123 132 S. Ct. 945 (2012).

124 Daniel Solove's work on the First Amendment and criminal procedure has clarified that the few cases where the First and Fourth Amendment have explicitly intersected have required warrants. That point fits within this Article's recommendation and indeed part of Solove's conclusion. As he points out, however, the "[o]pen [q]uestion" is "what procedures should apply when First Amendment activity falls outside the scope of current Fourth and Fifth Amendment protection." *See* Solove, *supra* note 5, at 128–30. Solove's work informs much of this Article, but as he uses a narrower definition of association and at the same time addresses a broad range of First Amendment concerns, this Article seeks to add to his work by providing a definition of associational freedom that addresses his open question in the context of data protection and that shows how associational concerns are also found in the Fourth Amendment.

125 Solove has argued that the history and case law require reading the Fourth Amendment with the First Amendment. Solove, *supra* note 5, at 132–142. As Akhil Amar has said, "our Constitution is a single document . . . not a jumble of disconnected clauses." Akhil

laws and numerous prosecutions in Britain and the American colonies used "to suppress criticism of the government."[126] As William Stuntz has explained, cases protected First Amendment interests before the First Amendment existed.[127] He argues that the law of search and seizure can be seen as the "consequence of the strong tradition of using Fourth and Fifth Amendment law as a shield against government information-gathering—a tradition that has more to do with protecting free speech than with regulating the police."[128] I seek to amend the point and argue that the Constitution protects associational freedom as well as speech, and draws on both the First and Fourth Amendments to do so.

The way the Court has addressed the government's use of surveillance technology reveals associational freedom's importance to Fourth Amendment jurisprudence. The deep concern, not over procedure, but over how a lack of procedure allows new technology to threaten associational freedom is the key to understanding how to regulate surveillance. For example, real time tracking of someone—be it with GPS or some other technology—raises associational freedom issues just as bugging and wiretapping does. As we will see, modern warrant procedures emerged to manage the tension between policing and associational freedom.[129] Before we explore how those procedures operate, we have to understand the sorts of acts that threatened associational freedom.

Even the relatively unsophisticated technology of the 1960s allowed for unsupervised, ongoing, and secret surveillance that threatened associational freedom and could not be allowed without a warrant. In *Berger*, law enforcement placed a recording device on a person and in the office of a liquor board official suspected of corruption and demanding bribes.[130] The Court distinguished wiretapping from bugging.[131] Bugging posed a larger threat, because the proliferation of tiny recording devices allowed someone to "eavesdrop[ ] on anyone in almost any given situation."[132] "[P]ostage stamp" sized devices could "pick up whispers within a room and broadcast them half

---

Reed Amar, *The Bill of Rights as a Constitution*, 100 YALE L.J. 1131, 1201 (1991); *accord* Solove, *supra* note 5, at 133.

126 William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 395 (1995).

127 *See id.* at 396–411.

128 *Id.* at 395.

129 *But see* Solove, *supra* note 5, at 128–30 (explaining that the few cases in which the First and Fourth Amendments have explicitly intersected have required warrants but have not answered "what procedures should apply when First Amendment activity falls outside the scope of current Fourth and Fifth Amendment protection"). *See* Amar, *supra* note 117, at 762–71 (arguing that warrants were distrusted in early Anglo-American law, are not required by the text of the Fourth Amendment, and that the proper inquiry is about reasonableness).

130 Berger v. New York, 388 U.S. 41, 44–45 (1967).

131 *Id.* at 47.

132 *Id.* at 46–47.

a block away to a receiver."[133] The Court speculated, "[i]t is said that certain types of electronic rays beamed at walls or glass windows are capable of catching voice vibrations as they are bounced off the surfaces."[134] That ability may have been nascent in 1967; it is common today. Even without speculation, the Court had evidence of pervasive, undetected surveillance such as automatic recording devices operated by remote control and "concealed in a book, a lamp, or other unsuspected place in a room, or made into a fountain pen, tie clasp, lapel button, or cuff link" which could send messages to someone a half mile away.[135] The Court distrusted the new ability to record someone in secret.

The Court was quite clear that threats to associational freedom, even in public spaces, were a major concern. One might assume that the areas of concern were private and where one has a reasonable expectation of privacy, but that is incorrect. In his concurrence, Justice Douglas compared bugging to "plac[ing] a government agent" wherever we might go, including public places.[136] And *Berger* was decided the year prior to *Katz*, so the reasonable expectation of privacy test had not yet been articulated, let alone adopted. Even if the test's logic and privacy were on the Court's mind, Justice Douglas was concerned about "anywhere" one might be bugged.[137] Of his list of places swept up in this surveillance, bedrooms, lawyer's offices, and perhaps business conferences may be private, but taverns, schools, trade groups, dry cleaners, banks, and restaurants, are not.[138] Protecting the ability to go to

133 *Id.* at 47.

134 *Id.*

135 *Id.* Should one doubt that the Court was concerned about the hidden aspect of surveillance, this passage further shows that the Court did not like that potential:

> Receivers pick up the transmission with interference-free reception on a special wave frequency. And, of late, a combination mirror transmitter has been developed which permits not only sight but voice transmission up to 300 feet. Likewise, parabolic microphones, which can overhear conversations without being placed within the premises monitored, have been developed.

Id.

136 *Id.* at 64–65 (Douglas, J., concurring).

137 *Id.* at 65.

138 *Id.* at 64–66 (noting the capture of "conversations involving, at the other end, The Juilliard School of Music, Brooklyn Law School, Consolidated Radio Artists, Western Union, Mercantile Commercial Bank, several restaurants," and recognizing that "[t]hese cases are but a few of many demonstrating the sweeping nature of electronic total surveillance as we know it today"). On the importance of taverns for assembly, see also Baylen J. Linnekin, *"Tavern Talk" and the Origins of the Assembly Clause: Tracing the First Amendment's Assembly Clause Back to Its Roots in Colonial Taverns*, 39 HASTINGS CONST. L.Q. 593, 594 (2012) ("The proper situs of the Assembly Clause, research reveals, is in its birthplace: colonial America's taverns. . . . [C]olonial taverns served not just as establishments for drinking alcohol but as vital centers where colonists of reputations great and small gathered to read printed tracts, speak with one another on important issues of the day, debate the news, organize boycotts, draft treatises and demands, plot the expulsion of their British overlords, and establish a new nation.").

such places has to be about something other than keeping something fully private.

I argue that the concern was that the surveillance at issue affected associational freedom. Had the surveillance been conducted a few hundred years ago, Douglas's list could have said sewing circles or Democratic-Republican Societies. The places Douglas found to be too far afield from the criminal investigation all fit into the places where historically people met, and today still meet, to share ideas and form opinions.[139] We limit and in some cases eliminate the government's ability to conduct continual, secret surveillance, because that creates room for associational freedom to operate. Associational freedom requires that we are able to meet, share ideas, and choose whether to take action in public yet still remain private from government oversight.[140]

Other cases involving surveillance further show that associational freedom is an important aspect of Fourth Amendment jurisprudence. Although *Katz v. United States*[141] has created much mayhem with the reasonable expectation of privacy test, it too is sensitive to associational freedom. I argue that *Katz*'s reasonable expectation of privacy test has an associational component, and when assessing whether someone's expectation of privacy is objectively reasonable, concerns over associational freedom are an objective standard that must be part of that analysis.[142] In *Katz*, the Court was quite clear that the Fourth Amendment concerns more than privacy.[143] The police had adhered to many, if not all, requirements of a warrant. They had, however, failed to obtain one, and argued that the public nature of the phone booth meant there was not a privacy problem requiring a warrant. The Court explained that someone does not give up their protection from surveillance just because they are in "a business office, in a friend's apartment," or in a "taxicab."[144] The phone had become a vital part of communication—one might say an important part of "forming and maintaining associations"—and the Court could not allow the executive to use its discretion about surveillance instead of a neutral magistrate's. It is the analysis that goes into obtaining a warrant that connects to and matters for associational free-

139 *See* Abu El-Haj, *supra* note 90, at 67 (explaining how recent movements used meetings at "churches, cafes, and living rooms" to solve collective action problems and generate political action but were not speech).

140 The 1976 Church Committee Report, which investigated intelligence practices of the government, also recognized that surveillance by means of bugs, wiretaps, and more captured "vast amounts of information about the personal lives, views, and associations of American citizens." *See* S. REP. NO. 94-755, *supra* note 24, at 5.

141 389 U.S. 347 (1967).

142 *See* Amar, *supra* note 117, at 806; *accord* Solove, *supra* note 5, at 118–19. I thank Brett Frischmann for pressing me to develop this point.

143 *Id.* at 350 & n.4. The Court also acknowledged that some privacy concerns and protections flowed from the First Amendment coverage of associational freedom. *Id.* at 350 n.5.

144 *Katz*, 389 U.S. at 352 (citations omitted).

dom.[145] As in *Berger*, the *Katz* Court required the executive to seek prior permission to conduct surveillance of public places[146] such as offices and hotel rooms.[147] One way to understand the Court's concern and demand for judicial oversight about the scope of the surveillance even in these somewhat public spaces was that it sought to protect where meetings occur and to protect the facilities, such as a phone, that are part of and enable further associational activity. In short, the Court was implicitly protecting associational freedoms. An additional way to understand associational freedom and the Fourth Amendment is to ask whether surveillance captures lawful along with unlawful activity. In *Kyllo v. United States*, police used a thermal imaging device to detect what was going on inside a suspect's house.[148] The Court did not allow that type of surveillance because it reached intimate details within the home.[149] But it is a mistake to read that point too narrowly. The Court said limiting the prohibition to "intimate details" would "be wrong in principle."[150] The Court reiterated and strengthened this point in *Illinois v. Caballes*.[151] In that case the police used a dog to sniff for illegal drugs. The Court distinguished that detection method from the one in *Kyllo*. A critical part of *Kyllo* was "the fact that the device was capable of detecting lawful activity."[152] The Court held that the dog sniff was different, because it only detected illegal activity. In contrast, there is a "legitimate expectation that information about perfectly lawful activity will remain private."[153] When surveillance can sweep lawful activity into its net, there must be protection *before* the surveillance commences, because "no police officer would be able to know *in advance*" whether the surveillance might pick up lawful activity and so "would be unable to know in advance whether it is constitutional."[154] And here we can see the logic come together.

Lawful activities are to be free from government oversight. Surveillance that might capture those activities requires extra steps to be constitutionally sound. As an objective matter, associational freedom is not only a lawful activity but a vital and core part of the type of activity that must not be chilled by government surveillance. Surveillance that implicates associational freedom requires limits and oversight.[155]

145 *Cf.* Amar, *supra* note 117, at 810 (noting that "if there are good reasons for suspecting strong and systematic over-zealousness on the part of certain segments of executive officialdom," preclearance by the judiciary may be required).

146 *Katz*, 389 U.S. at 352 (citations omitted).

147 *Id.* at 358.

148 Kyllo v. United States, 533 U.S. 27, 29 (2001).

149 *Id.* at 37–39.

150 *Id.* at 38 (internal quotation marks omitted).

151 Illinois v. Caballes, 543 U.S. 405, 409–10 (2005); *accord* Strandburg, *supra* note 53, at 761.

152 *Caballes*, 543 U.S. at 409.

153 *Id.* at 410.

154 *Kyllo*, 533 U.S. at 39.

155 *Cf.* Solove, *supra* note 5, at 152 (stating that only information gathering implicating "First Amendment *values*" should apply to limit government investigations).

Associational concerns also help understand why the *Jones* Court recognized tracking by GPS or other means as a problem.[156] The issues at stake in *Berger* have not vanished; they persist and reappear with tracking. Early tracking cases looked at the use of a beeper, a device that sends a signal but requires that law enforcement be near the tracking device to receive the location and follow the subject. Thirty years ago, in *United States v. Knotts*, the Supreme Court allowed the use of such devices when someone is on a public road, because beepers are seen as enhancing visual tracking, and because law enforcement is allowed to follow someone in public areas.[157] But a vital fact supported that holding. The Court found that the threat of law enforcement abusing the technology to perform "twenty-four hour surveillance of any citizen of this country . . . without judicial knowledge or supervision" was not present.[158] Public exposure mattered but continual surveillance was a strong and equal part of the inquiry. Unlike GPS trackers, beepers were not seen as allowing easy, continual surveillance.[159] The Court set aside the question of whether beeper technology would lead to "dragnet" law enforcement.[160] Questions about continual surveillance and judicial oversight are associational. Although the Court did not directly address associational freedom, its explicit discussion of easy, continual surveillance and dragnets shows the Court was assessing potential harms to associational freedom as it assessed reasonableness and surveillance. If those concerns are present, the Court will not allow surveillance absent oversight and other protections for associational freedom.

Whether prolonged surveillance even in public places harms associational freedom and thus alters the analysis—an issue *Knotts* acknowledged but set aside—drives the divergence in courts' decisions on that question. When state intermediate appellate courts have found that a warrant was not needed, they have found that driving on public roads negated privacy claims, *and* that the short length of surveillance permitted the surveillance.[161] In contrast, three state supreme courts have found that the use of a tracking device required a warrant.[162] The logic of those cases is associational. The continuous surveillance possible with GPS tracking revealed "our associa-

156 United States v. Jones, 132 S. Ct. 945, 948–49, 954 (2012).

157 United States v. Knotts, 460 U.S. 276, 285 (1983).

158 *Id.* at 283 (quoting Brief for Respondent at 9, *Knotts*, 460 U.S. 276 (No. 81-1802)) (internal quotation marks omitted).

159 *Id.* at 285.

160 *Id.* at 284. A year later, the Court refined the scope of when a beeper could be used. It prevented the warrantless use of a beeper, when it allowed law enforcement to follow someone into a private place such as a home. United States v. Karo, 468 U.S. 705, 707–11, 719–21 (1984).

161 *See* Priscilla J. Smith et al., *When the Machines Are Watching: How Warrantless Use of GPS Surveillance Technology Violates the Fourth Amendment Right Against Unreasonable Searches*, 121 YALE L.J. ONLINE 177, 178 n.7 (2011) (citing cases).

162 Commonwealth v. Connolly, 913 N.E.2d 356, 366–67 (Mass. 2009); People v. Weaver, 909 N.E.2d 1195, 1201–03 (N.Y. 2009); State v. Jackson, 76 P.3d 217, 264 (Wash. 2003) (en banc).

tions—political, religious, amicable and amorous, to name only a few."[163] Such detail went beyond the sort of data law enforcement might gather when following a car with other methods of surveillance and violated the Fourth Amendment, not because the acts were private, but because of the threats to associational freedom.[164] Federal circuit courts have differed on GPS tracking as well.[165] As the Court of Appeals for the District of Columbia Circuit explained in *United States v. Maynard*, none of the cases addressed the question whether the prolonged use of GPS tracking raised the associational concerns explicitly set aside in *Knotts*.[166] But even if they had, the issue seems easily solved.

The simplest answer would be to require a warrant for any tracking; yet the law already addresses warrants and tracking devices. The Federal Rules of Criminal Procedure (the Rules) set out the procedures required when law enforcement uses tracking devices. The Rules appear to address all the concerns GPS tracking raises. The Rules do not, however, address when a warrant is required. Just as with the history of wiretapping, the FBI has offered a position on that question.[167] The government analysis is that use of a warrant was preferable in general as it is "more likely to ful?ll the Fourth Amendment's reasonableness requirement."[168] Thus, the executive branch recognizes that warrants help ensure compliance with the Fourth Amendment. And here is an irony. *Jones* may never have reached the Court had the

163 *Weaver*, 909 N.E.2d at 1199.

164 *Id.*

165 The Seventh Circuit Court of Appeals ruled that the installation of the tracker was not a search and so did not require a warrant. United States v. Garcia, 474 F.3d 994 (7th Cir. 2007). It did not address the issue of prolonged surveillance, because the appellant had ceded that question. *Id.* at 996. The Ninth Circuit Court of Appeals' decision in *United States v. Pineda-Moreno* permitted GPS tracking without a warrant, because it did not find a difference between short and long-term surveillance and again the appellant *had ceded* that *Knotts* controlled the issue of tracking in public. 591 F.3d 1212, 1216 (9th Cir. 2010); *accord* United States v. Maynard, 615 F.3d 544, 557–58 (D.C. Cir. 2010). The Eighth Circuit Court of Appeals ruled use of a GPS tracker was not a search and focused on the method of installation, not the question of how long the tracking was used. United States v. Marquez, 605 F.3d 604, 609–10 (8th Cir. 2010).

166 *Maynard*, 615 F.3d at 558.

167 Keith Hodges, *Tracking "Bad Guys": Legal Considerations in Using GPS*, 76 FBI L. ENFORCEMENT BULL., July 2007, at 25, *available at* http://leb.fbi.gov/2007-pdfs/leb-july-2007. During the history of wiretapping the Justice Department disfavored, and at times rejected, using wiretaps as part of its enforcement arsenal. Even J. Edgar Hoover and the Treasury Department, who were not shy about aggressive law enforcement, took stands against wiretapping by law enforcement. Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 842–43 (2004). After Congress banned wiretapping, the Court held that evidence from wiretapping was inadmissible in court and anything gained from an illegal wiretap was also inadmissible as "fruit of the poisonous tree." Nardone v. United States, 308 U.S. 338, 341 (1939). This time, however, the Justice Department continued using wiretaps under the idea that they could do so but not use what they found in court or divulge what they found. *See* Kerr, *supra*, at 846.

168 Hodges, *supra* note 167, at 31.

officers followed the warrant procedures for tracking *in the warrant they had obtained*.[169] What then was happening in *Jones* to prompt the Court to take a simple failure to follow procedure case? Why would two Justices craft concurrences with extensive discussion of tracking? *Jones* is about more than procedure or a specific technology.

Jones is about threats to associational freedom from the ability to have sustained, possibly secret, mass surveillance.[170] Neither the *Jones* Court nor the *Maynard* court cites *Berger*, but *Berger*'s concerns are the key to understanding the problems tracking and other technology present. This chart illustrates the overlapping issues and how *Berger*'s concerns reappear in *Jones*.

Court's Concern	*Berger v. New York*	*United States v. Jones*
Method	Small, hidden bug that transmitted far away to law enforcement	Tracker which was difficult to detect and transmitted location data
Procedural failure	Unconstitutional warrant procedure	Failed to follow warrant procedure
Police everywhere	"[P]laces a government agent in the bedroom, in the business conference, in the social hour, in the lawyer's office—everywhere and anywhere a 'bug' can be placed." *Berger*, 388 U.S. at 64–65 (Douglas, J., concurring).	Like having "a very tiny constable" hidden in one's car. *Jones*, 132 S. Ct. at 958 n.3 (Alito, J., concurring).
Length of time	Sixty days to bug someone "is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause." *Berger*, 388 U.S. at 59.	"[T]he use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. . . . [F]or four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving." *Jones*, 132 S. Ct. at 964 (Alito, J., concurring).

169 United States v. Jones, 132 S. Ct. 945, 964 n.11 (2012) (Alito, J., concurring).

170 As one study has shown, the cost to track individuals has dropped from more than $250 an hour for covert pursuit by officers to $10 per hour with a GPS device and $5.21 per hour with cellular phone tracking. *See, e.g.*, Kevin S. Bankston & Ashkan Soltani, *Tiny Constables and the Cost of Surveillance: Making Cents Out of* United States v. Jones, 123 YALE L.J. ONLINE 335, 353–54 (2014).

Pervasive, inexpensive, and easy to use technology that can target anyone	The proliferation of tiny recording devices could allow someone to "eavesdrop[ ] on anyone in almost any given situation" with no oversight. *Berger*, 388 U.S. at 47.	Makes available "at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track." *Jones*, 132 S. Ct. at 956.
Use of spying technology	Surveillance "concealed in a book, a lamp, or other unsuspected place in a room, or made into a fountain pen, tie clasp, lapel button, or cuff link" could send messages to someone a half mile away. *Berger*, 388 U.S. at 47.	"[C]heap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously." *Jones*, 132 S. Ct. at 956.
Impinges associational freedom	One tap captured "conversations involving, at the other end, The Juilliard School of Music, Brooklyn Law School, Consolidated Radio Artists, Western Union, Mercantile Commercial Bank, several restaurants . . . . These cases are but a few of many demonstrating the sweeping nature of electronic total surveillance as we know it today." *Berger*, 388 U.S. at 65–66 (Douglas, J., concurring).	"[The] monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations." *Jones*, 132 S. Ct. at 955.

Focusing on the method of detection is a mistake. If instead we look to the harms from tracking, we see that it poses harms that parallel the ones in *Berger*. Part of the *Jones* Court is addressing tracking because, just as in *Berger* and *Katz*, the technology creates problems for the Fourth Amendment and associational freedom by enabling "arbitrary exercises of police power" and "a too permeating police surveillance" both of which threaten associational freedom.[171]

One way to understand the concern is about scale. There is a difference between trying to place a cop everywhere and having the same effect through technology.[172] Consider that once we are in a park or share an idea with

171 *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)) (internal quotation marks omitted).

172 *Id.* at 958 (Alito, J., concurring) ("The Court argues—and I agree—that 'we must assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.' But it is almost impossible to think of late–18th-century situations that are analogous to what took place in this case." (citation omitted) (quoting *id.* at 950 (majority opinion))).

someone, we assume the risk that someone might see us, overhear us, or even be an undercover agent.[173] That person may even be wearing a bug and recording us, yet there is no violation of the Fourth Amendment. The difference, I argue, is that the Court is asking when secret surveillance (as opposed to an obvious deployment of agents) poses a threat to associational freedom. As Amar has argued, "secrecy does not necessarily equal unconstitutionality. But it does raise a problem."[174] For Amar, the correct question is reasonableness: "Simply put, are secret searches and seizures reasonable?"[175] Orin Kerr has argued that the Court recalibrates the Fourth Amendment depending on whether the technology makes it "harder" or "substantially easier" for law enforcement to obtain evidence.[176] When harder, the Court lowers Fourth Amendment protections.[177] When substantially easier, the Court raises the protections.[178] But Kerr misses a core issue. He sees the issue as a game of cops and robbers with one side upping its game and forcing the other to adapt.[179] The rest of us, citizens, are missing from Kerr's calculation.[180]

Rather than equilibrium as Kerr describes it, I argue that when the Court encounters the power and scale of new surveillance technologies, it is assessing reasonableness as a question of associational harm. In that sense, associational harm is a key way to understand equilibrium. Tracking is a "dramatic technological change" that is more powerful than bugging and tapping, because it drops the cost of continual surveillance and allows it to work in secret with no notice to the person under surveillance.[181] The equilibrium is upset. But make no mistake. Tracking is simply the latest example of the larger problem. Physical and cost barriers that helped prevent govern-

173 *See* Solove, *supra* note 5, at 127 (discussing a case in which the Supreme Court found no Fourth Amendment violation when the defendant willingly spoke to an undercover agent because information voluntarily revealed to a police informant is not protected).

174 Amar, *supra* note 117, at 803.

175 *Id.* ("And if the answer to our problem does not lie in a secret newfangled warrant, neither does it lie in probable cause. It lies in reasonableness. Simply put, are secret searches and seizures reasonable? Regardless of one's answer, at least one will be asking the right question—talking sense rather than nonsense.").

176 Kerr, *supra* note 2, at 480.

177 *Id.*

178 *Id.*

179 *Id.* at 481 ("The police continuously devise new ways to catch criminals. Criminals continuously devise new ways to avoid being caught. This state of flux poses an underappreciated difficulty for judges interpreting the Fourth Amendment. New facts constantly threaten to upset the balance of police power."). Professor Susan Freiwald has argued that surveillance that is "hidden, intrusive, indiscriminate, and continuous and therefore particularly susceptible to abuse" will move a court to find that a warrant is required. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, ¶ 53. I agree that these concerns fuel when a warrant is required and argue that the reason these factors matter is that they affect associational freedom.

180 *Cf.* Ohm, *supra* note 2, at 1343–45 (arguing that balancing has to account for other parties that benefit from a new technology).

181 United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

ment's overreaching surveillance are vanishing. When those barriers go away, it is too easy for the government to engage in continual, secret spying that threatens associational freedom.[182] We may have "tiny constables" everywhere and never know about it.[183] Unfortunately, the government tends to engage in such dubious practices all too often. And today, the ability to engage in such practices has increased. Government can achieve the same goals and create the same harms with backward-looking surveillance. Understanding how we limit harms from forward-looking surveillance will help us see why current practices for searching backward and maintaining data hoards are unreasonable and further upset the balance between surveillance and freedom.[184]

II. Protecting Future and Past Associational Freedom

The concurrences in *Jones* raised concerns about the third party doctrine and raised questions regarding what might be learned from data, because those concerns and questions are part of backward-looking surveillance. The Court was calling out that such surveillance threatens associational freedom, but we lack ways to manage this new threat.[185] We can look backward and harm associational freedom as much, if not more, than when looking forward. This Part explains how the procedural protections for forward-looking surveillance reveal why and how we should protect associational freedom from backward-looking surveillance.

182 Harry Surden, *Structural Rights in Privacy*, 60 SMU L. Rev. 1605 (2007).

183 *Jones*, 132 S. Ct. at 958 n.3 (Alito, J., concurring); Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring) ("If a statute were to authorize placing a policeman in every home or office where it was shown that there was probable cause to believe that evidence of crime would be obtained, there is little doubt that it would be struck down as a bald invasion of privacy, far worse than the general warrants prohibited by the Fourth Amendment. I can see no difference between such a statute and one authorizing electronic surveillance, which, in effect, places an invisible policeman in the home. If anything, the latter is more offensive because the homeowner is completely unaware of the invasion of privacy."); *see also* Clarke et al., *supra* note 2, at 58 (detailing the history of intelligence abuses and the historical concern that an intelligence agency operating in secret "become a menace to a free government . . . because it carries with it the possibility of abuses of power which are not always quickly apprehended or understood." (quoting S. Rep. No. 94-755, *supra* note 24, at 3) (internal quotation marks omitted)).

184 *Cf.* Krent, *supra* note 14, at 51 ("My thesis is that the reasonableness of a seizure extends to the uses that law enforcement authorities make of property and information even after a lawful seizure.").

185 This point is why scholars such as Cohen, Richards, and Solove have explored and argued for greater recognition and protection of many activities that are public and not expressive speech.

A. Associational Freedom and the Protection of Future Acts

No one and no policy supports law enforcement attaching a device to track someone's every move.[186] Yet, after a warrant has issued, law enforcement may do just that for a limited time. In simplest terms, *United States v. Jones* addressed such a problem. The government had used a technique, failed to follow the warrant, and so violated the Fourth Amendment.[187] As Amar and Solove have argued, when surveillance and First Amendment concerns intersect is precisely when such procedures are needed.[188] Furthermore, "if there are good reasons for suspecting strong and systematic overzealousness on the part of certain segments of executive officialdom," preclearance by the judiciary may be required.[189] Both concerns are present with bugging, tracking, and wiretapping. All require warrant procedures, because they mitigate the potential harms to associational freedom.[190]

When forward-looking surveillance intersects with associational freedom, surveillance must be limited or the purposes of the First and Fourth Amendment are gutted. Warrant procedure is central to how we manage surveillance and civil liberties. As the Court said in *Berger*, "[t]he purpose of the probable-cause requirement of the Fourth Amendment [is] to keep the state out of constitutionally protected areas until it has reason to believe that a specific crime has been or is being committed."[191] Lack of prior review means no check and balance is even possible. A "neutral and detached authority" must evaluate the warrant application to see whether probable

186 *Cf.* Rehnquist, *supra* note 43, at 9 (offering that a police stake out of a public place such as a bar just to know who frequented it would not be allowed).

187 *Jones*, 132 S. Ct. at 948–49, 954. Warrants are not magical and can be dangerous. As Amar has argued, we err when we assume that simply because a warrant has issued, Fourth Amendment reasonableness demands are met. Amar, *supra* note 117, at 802–03 ("[C]onsider electronic surveillance. In love with the warrant, the Court has blessed hidden audio and video bugs—apparently even ones that must be installed by secret physical trespass—so long as these bugs are approved in advance by judicial warrant."). A warrant may issue but still run afoul of constitutional protection. So too for statutes; just because Congress passes a law—for example the Stored Communications Act—does not mean that the law is constitutional. The key point is to know under what circumstances reasonableness may demand stronger procedures. *See, e.g.*, Krent, *supra* note 14, at 63–77 (arguing for a reasonableness standard for search and seizure of information).

188 Amar, *supra* note 117, at 806 ("First Amendment concerns could well trigger special Fourth Amendment safeguards—heightened standards of justification prior to searching, immediate (pre-search) appealability of any proposed search (with the premises sealed to prevent interim destruction of evidence), specially trained nonpartisan marshals or magistrates or masters to carry out the search, and so on."); Solove, *supra* note 5, at 132.

189 Amar, *supra* note 117, at 810.

190 Amar has argued that options other than a warrant per se such as "heightened standards of justification prior to searching, immediate (pre-search) appealability of any proposed search (with the premises sealed to prevent interim destruction of evidence), specially trained nonpartisan marshals or magistrates or masters to carry out the search, and so on" would suffice. *Id.* at 806. I do not disagree. Rather, I here wish to show that the Court seeks some of the same outcomes in its embrace of warrants.

191 Berger v. New York, 388 U.S. 41, 59 (1967).

cause exists before issuing the warrant.[192] As the Court said a year later in *Katz*, this review is required because of surveillance's secret nature and because asking permission later would lead to "hindsight" bias rather than "objective predetermination" that the surveillance should be permitted.[193] Anything other than prior review leaves constitutional protection at "the discretion of the police."[194]

When law enforcement can watch and record us without stating specifics of a "particular offense" or the property to be seized—in other words, without establishing probable cause—the order works as a general warrant.[195] A ban on practices that operate as general warrants is a mainstay of Fourth Amendment law.[196] Allowing officers to bug someone for sixty days "is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause."[197] Without a termination date surveillance can persist even after the thing sought has been found.[198] Lack of notice "permits uncontested entry without any showing of exigent circumstances."[199] The secret recording of someone means they would never know that a search or seizure occurred as they would with other searches and seizures.[200] And, because there is not a return on the warrant, the process for giving up the information gathered, law enforcement could use "seized conversations of innocent as well as guilty parties."[201] Together, these practices enable a "blanket grant of permission to eavesdrop" in part because of the lack of "adequate judicial supervision or protective procedures."[202] These types of practices were rejected in Anglo-American jurisprudence beginning with

192 *Id.* at 54.

193 Katz v. United States, 389 U.S. 347, 358–59 (1967) (quoting Beck v. Ohio, 379 U.S. 89, 96 (1964)); *see also* Krent, *supra* note 14, at 86 (arguing that law enforcement must precommit at the legislative level to how it wants to use gathered information, because "[p]rospectivity minimizes the chances for arbitrary action or action motivated by hidden bias").

194 *Katz*, 389 U.S. at 358–59 (quoting *Beck*, 379 U.S. at 97).

195 *Id.* at 59–60.

196 *Berger*, 388 U.S. at 58. Distrust of general warrants runs deep in U.S. history; outcry over the use of general warrants motivated the writers of the Declaration of Independence. *Id.*; *see, e.g.*, Byars v. United States, 273 U.S. 28, 33–34 (1927).

197 *Berger*, 388 U.S. at 59.

198 *Id.* at 59–60.

199 *Id.* at 60; *cf.* Amar, *supra* note 117, at 803 ("Moreover, even though the warrant contemplated by the Fourth Amendment would be issued ex parte, it would be served on the owner or occupant of the searched premises, or left there, giving the target clear notice of what had been searched or seized, and when. This notification was contemporaneous with the intrusion itself. By contrast, targets of audio and video warrants may never learn that they have been searched and that their words have been seized—or they may find out years after the fact.").

200 Even with warrants, when the act is secret and no one knows what was gathered, the procedure goes against the "adversarial nature of Anglo-American judicial proceeding[ ]." Amar, *supra* note 117, at 803.

201 *Berger*, 388 U.S. at 60; *accord id.* at 66.

202 *Id.* at 60.

Wilkes v. Wood[203] and *Entick v. Carrington*.[204] They were rejected in the 1760s and two hundred years later in the 1960s for the same reason: they were and are "totally subversive of the liberty of the subject."[205] That liberty interest is associational freedom.

Tracking technology has opened the door to a new type of dragnet that requires us to remember the importance of freedom from surveillance. This dragnet evades the limits of a trespass approach to privacy.[206] The trespass approach to surveillance does important work, but it does not work alone.[207] Some issues are not amenable to the trespass approach, because no touching is required. Recall that the *Berger* court was worried about "electronic rays beamed at walls or glass windows . . . capable of catching voice vibrations as they are bounced off the surfaces."[208] Trespass cannot address that possibility just as it cannot manage the problem of a tap on a public phone booth in *Katz*. In *Jones*, Justices Sotomayor and Alito showed how trespass fails to address the larger implications of tracking. Justice Sotomayor noted that some "electronic or other novel modes of surveillance . . . do not depend upon a physical invasion on property."[209] Justice Alito agreed with that concern.[210] Just like the *Berger* court, he speculated about things that might come to pass. He pointed out that the government might also "require[ ] or persuade[ ]" installation of tracking mechanisms in all cars or might activate a stolen vehicle tracker.[211] Trespass would not address those possibilities, but the harms to associational freedom would remain. We do not have to imagine technological dystopias to understand the harms here. William Rehnquist explained them forty years ago. His example was prescient.

The question is not one of privacy as in acts or facts kept secret; the problem lies in the government's non-particularized surveillance of people.[212] Then-Justice Rehnquist suggested that one might place a police

203 (1763) 98 Eng. Rep. 489 (K.B.).

204 (1765) 95 Eng. Rep. 807 (K.B.).

205 *Wilkes*, 98 Eng. Rep. at 498.

206 Insofar as trespass ideas in Fourth Amendment jurisprudence rely on property, I agree with Amar that this view is oddly narrow and fits with *Lochner* style "[p]roperty worship." Amar, *supra* note 117, at 788–89.

207 *Cf.* United States v. Jones, 132 S. Ct. 945, 952 (2012) ("But as we have discussed, the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

208 Berger v. New York, 388 U.S. 41, 47 (1967).

209 *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring).

210 *Id.* at 962 (Alito, J., concurring) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.").

211 *Id.* at 961.

212 Rehnquist, *supra* note 43, at 11 ("The only claim of the government is a desire to know what each of its citizens is doing without regard to whether that conduct is or might be unlawful. I think almost all of us would regard this as simply not the kind of governmental interest that ought to rate high in a free society."); *accord* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 89–90 (2007).

officer at a bar daily and take down all the license plate numbers for later cross-referencing with the Department of Motor Vehicles records to gain "a reasonably accurate list of people who patronize the bar."[213] He posited that even if it were cost effective for the government to "keep a dossier of information pertaining to every citizen" most would say we should not do so.[214] Such a power would create a "justified uneasiness," because patrons would feel their names were being "taken down and filed for future reference."[215] Today what Rehnquist called "an extreme" example is now an easy reality.[216] As the Justices in the *Jones* concurrence stated, the cost issue alone has changed.[217] The possibility of low-cost surveillance was a reality in the 1960s with bugging and has only become a less expensive and easier reality today.[218] As one study has shown, the cost to track individuals has dropped from more than $250 an hour for covert pursuit by officers to $10 per hour with a GPS device and $5.21 per hour with cellular phone tracking.[219] The cost drop makes it too easy to place an officer, or "tiny constable," at every tavern door or any other place we may go.[220] With bugging, Justice Douglas equated pervasive, secret electronic surveillance with deploying police in every home or office. He offered that even if a statute authorized doing so if there was "probable cause to believe that evidence of crime would be obtained, there is little doubt that it would be struck down as a bald invasion of privacy, far worse than the general warrants prohibited by the Fourth Amendment."[221] He then said that electronic surveillance would be worse because we would be "completely unaware" of its presence.[222] Tracking has the same problem. The *Jones* Court recognized the temptation and possibility to use the technology in ways that threaten associational freedom, and thus demands stronger procedures to mitigate those potential harms.

Rehnquist's other issue, the ability to maintain dossiers, has also come to full fruition.[223] That possibility connects to Justice Sotomayor's concern over surveillance of past activities. Rather than having to set someone at a bar in real time, law enforcement can access databases to get precise information about someone at very low cost and end up with the same, if not a better, dossier that Rehnquist recognized as undesired.[224] That is why Justice Sotomayor could connect tracking to the general problems "the digital age"

213 Rehnquist, *supra* note 43, at 9.
214 *Id.*
215 *Id.*
216 *Id.*; SLOBOGIN, *supra* note 212, at 89–90.
217 United States v. Jones, 132 S. Ct. 945, 963–64 (2012) (Alito, J., concurring).
218 *See, e.g.*, Bankston & Soltani, *supra* note 170, at 354.
219 *Id.*
220 *Jones*, 132 S. Ct. at 958 n.3 (Alito, J., concurring).
221 Berger v. New York, 388 U.S. 41, 65 (1967) (Douglas, J., concurring).
222 *Id.*
223 *See* SOLOVE, *supra* note 9, at 1–26 (investigating the problems of digital dossiers).
224 Rehnquist, *supra* note 43, at 10 ("[T]his amount of information generally will be physically impossible to compile, and . . . most of us would feel that such a dossier on every citizen ought not to be compiled even if manpower were available to do it.").

poses for the third party doctrine.[225] She recognized that the digital age has opened the door to new threats to associational freedom and current law has not kept pace with this change.

B. Tracking the Past Threatens Associational Freedom

Surveillance of our past actions threatens associational freedom at least as much as surveillance of our future actions. Calling someone, visiting a web site, sending emails, and buying "books, groceries, and medications" all involve third parties and leave behind traces of our activities.[226] Our daily lives generate data exhaust that allows law enforcement to figure out exactly the same things that raise First and Fourth Amendment concerns for wiretapping and tracking.[227] That is why Justice Sotomayor asserted that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties."[228] As Rehnquist explained, these issues are not about privacy in the sense of away from public eyes.[229] The concerns about GPS and third parties are important, because they are part of a larger problem. We can now watch someone for an extended period of time, secretly and inexpensively, going forward, and we can do the same, if not more, going backwards. We have some sense of what to do about forward-looking surveillance. We must rethink backward-looking surveillance.[230]

Looking at data from a GPS company, a cellular phone company, a search company, a credit card company, or a retailer reveals all the details of that person's life just as, or in greater detail, than continual monitoring. No sophisticated, big data analysis is required; the list tells you exactly where someone went, what they bought, or what they read.[231] It is all too easy to

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

226 *Id.*

227 *See* Solove, *supra* note 5, at 126–27.

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

229 Rehnquist, *supra* note 43, at 9.

230 *Jones*, 132 S. Ct. at 955–56 (Sotomayor, J., concurring).

231 A problem for another time is the mistaken understanding of the mosaic theory as offered and what it must be in practice. It is important enough that I raise it here nonetheless. As a general matter, although several have tried to lay claim to the term "mosaic," the concept at least dates back to work done in 1986. *See* Anthony Paul Miller, *Teleinformatics, Transborder Data Flows and the Emerging Struggle for Information: An Introduction to the Arrival of the New Information Age*, 20 COLUM. J.L. & SOC. PROBS. 89, 111 (1986). In other words, mosaic seems to have different possible meanings. As used in *Jones* mosaic can be read two ways: one involves data mining and inferential claims about individual or group patterns and behaviors, and the other involves ability to take specific data about someone and assemble a picture of exactly what they did or said. Although Justice Sotomayor and scholars have looked to fears about the government using data to connect seemingly random data to create a picture of our activities, that problem was not at stake in *Jones*. Thus there has been an unfortunate conflation of the idea of connecting trivial bits of data to understand or see a pattern of behavior and the main issue with tracking: the ability to have a map or list of all the places one has gone, with whom one has met, what one bought, or

obtain this data, because the current approach to government information gathering over-focuses on what is, or is not, content and in so doing misses this type of data. Content data—the substance of a letter, email, or phone call—receive greater protection than non-content data and require a warrant.[232] Non-content data such as a phone number obtained via a pen register, business records, IP routing information, or tracking data do not require a warrant and are easily obtained with a subpoena.[233] The exact lists of our movements, meetings, and readings are available for abuse, and the content/non-content distinction fails to address the third party disclosure problems that Justice Sotomayor raises.[234]

The premise that anything one discloses to a third party is available for all to see is an absurdist conceit that increases the problems for protecting

---

what one read. *See, e.g.*, David Gray & Danielle Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62 (2013). Citron and Gray take mosaics to be about connecting trivial bits of information and offer that the law should "focus on *how* information is gathered." *Id.* at 71–72. For them, the key issue is "whether a technology has the capacity to facilitate broad and indiscriminate surveillance." *Id.* If the technique "rais[es] the specter of a surveillance state if deployment and use of that technology is left to the unfettered discretion of law enforcement officers or other government agents," the reasonable expectation of privacy is not met and Fourth Amendment concerns are triggered. *Id.* at 72. I differ by showing two things. First, gaining the sort of information that *Jones* and Citron and Gray care about is not about connecting trivial bits of data. It is about having accurate data, accessing it, and seeing what one did. Second, as discussed below, data generation, hoarding, and analysis are not going away. Thus I argue that the quantity of data does not matter as much as whether data usage by law enforcement threatens associational freedom. That analysis explains why a given practice matters. After that, one can ask about "bespoke" solutions depending on "upon the technology at issue" and "the law enforcement interests it serves." *Id.* at 72.

232 Professors Patricia Bellia and Susan Freiwald argue that those who believe that email routing information and stored email are not content have "overread" *Smith v. Maryland*. Patricia L. Bellia & Susan Freiwald, *Fourth Amendment Protection for Stored E-mail*, 2008 U. CHI. LEGAL F. 121, 163–64. They distinguish numbers from what they call communications attributes. *Id.*; *see also* Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L. REV. 949, 953–54 (1996) (defining communication attributes as "the existence, duration and subject matter of a communication, the identities of the parties to it, their physical locations and their electronic addresses").

233 For example, cell tower location data can reveal one's travel habits in much the same way that the GPS data at issue in *Jones* does. The Fifth Circuit has characterized cell tower location data as business records and thus held that no warrant is required for such data. *See In re* U.S. for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013). The Eleventh Circuit has held that cell tower data requires a warrant, but that ruling has been vacated and set for en banc rehearing. United States v. Davis, 754 F.3d 1205 (11th Cir.), *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). The courts' struggle regarding cell tower data shows the problems with the content/non-content approach to data that implicates associational freedom.

234 *See Davis*, 754 F.3d at 1216 (finding that even one cell phone data point may reveal sensitive information akin to communication information).

data exhaust.[235] The cases that embrace this position rely on the idea that business and corporate records are different than other personal records.[236] The first cases on the subject looked to a distinction between corporate records and personal records based on a conception of corporations as being different than people and having less privacy interest in their business records.[237] That position crept until finally *United States v. Miller* extended the idea that disclosure to a third party eliminated the reasonable expectation of privacy.[238] Claiming that a random teller or other functionary could recall the details of one record out of hundreds of transactions over many days or from a transaction that occurred months or years ago stretches credulity.

Even if one accepts that exposure to a person reduces or removes protection, the facts behind the idea belie that today's reality maps to the old one. Once upon a time, perhaps phone numbers, bank records, and other records were exposed to operators and banks tellers. But when was the last time someone spoke to an operator to give a number and place a call? How often do people speak to tellers to make a deposit or conduct other banking? The *elimination* of human interaction is a standard business practice to reduce cost. Calls and call records are automated, as are banks. GPS tracking, email accounts, online transactions, credit card purchases, are all designed not to expose data to a human being. The data is in the hands of the company, but the convenient legal point about a third party seeing the data is gone. There is no meaningful exposure. Now the mere *possibility* that someone could access data is enough to have exposed the data in a way that removes protection.[239] And, as Rehnquist said, the issues are about more than exposure.[240] Remember associational freedom protects things exposed

235 *Cf. Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) (questioning the third party doctrine and stating, "I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques").

236 *See, e.g.*, *id.* (same); *see also* Bellia & Freiwald, *supra* note 232, at 148 (discussing cases). President Obama's address regarding the NSA's gathering of bulk data also relied on this distinction as a way to claim that the program was not as invasive as it some argued. *See Transcript of NSA Reform Speech*, *supra* note 12 ("In sum, the program does not involve the NSA examining the phone records of ordinary Americans. Rather, it consolidates these records into a database that the government can query if it has a specific lead, a consolidation of phone records that the companies already retain for business purposes.").

237 *See* Bellia & Freiwald, *supra* note 232, at 150.

238 425 U.S. 435 (1976).

239 *See, e.g.*, Smith v. Maryland, 442 U.S. 735 (1979) (holding that no search warrant was required for the installation and use of a pen register (phone call monitoring system) as there was no legitimate expectation of privacy in the phone numbers that were dialed); *Miller*, 425 U.S. 435 (holding that there is no Fourth Amendment protection to business records of a bank such as original checks and deposit slips); *accord* Solove, *supra* note 5, at 125–26.

240 *Accord* United States v. Davis, 754 F.3d 1205 (11th Cir.) *vacated and en banc reh'g granted*, No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014); *cf.* Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011) (addressing challenges new location technologies pose to courts applying the rea-

to the public. The better question is, private from whom? With associational freedom the answer is law enforcement.

Simply assuming law enforcement having access to all third party data poses no threat or is always allowed fails to assess whether associational harm is present. To date, it might be that the world of analog recordkeeping had built in cost limits and was not so secret, and so the Court was less concerned about harms to associational freedom the legal fiction of exposure creates.[241] Those analog days are gone. We should not blithely accept that exposure to some people allows law enforcement to use data and thus ignore the potential threats to associational freedom. With digital records, the cost to track and store our movements and our behaviors has dropped as much as, if not more than, it has for GPS tracking. Furthermore, bulk access to data about one person, a specific group, or all of us is possible, and of late, the norm. In other words, data everywhere creates problems for associational freedom.

C. How Surveillance Chills and Data Tempts

Pervasive surveillance chills associational freedom.[242] Chilling, or deterrence, from activities can occur through indirect actions.[243] Several areas of information gathering—"surveillance of political activities, identification of anonymous speakers, prevention of the anonymous consumption of ideas, discovery of associational ties to political groups, and enforcement of subpoenas to the press or to third parties for information about reading habits"—have been found to chill First Amendment activities.[244] These activities are not speech, yet they are protected. I argue they are protected, because they are part of associational freedom. They are precursors to speech, independently desired, and under threat from recent government data programs.

The mechanisms for information gathering have taken different forms at different times in history, but regardless of the type of perceived threats to society, the precise method of surveillance, or when the acts occur, too often we can see a particular goal or outcome: suppression of association.[245] Recent data harvesting can be understood as part of a history of government

---

sonable expectation of privacy test). To be clear, the logic in *Miller* was that one assumes the risk that once information is shared with another, it may be revealed "even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Miller*, 425 U.S. at 443.

241 *Jones*, 132 S. Ct. at 956 (Sotomayor, J., concurring) ("And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: 'limited police resources and community hostility.'" (quoting Illinois v. Lidster, 540 U.S. 419, 426 (2004))).

242 Solove, *supra* note 5, at 143.

243 *Id.* at 142–43.

244 *Id.* at 143.

245 For a survey of the history of different ways government has overreached and then corrected attacks on civil liberties, see CLARKE ET AL., *supra* note 2, at 53–63.

mass-surveillance programs that can trample associational freedom.[246] Mail has been read, student speech and political actions watched, and library records obtained.[247] In the 1950s the FBI collected names of suspected Communists for use at congressional hearings including a security index of 26,000 people to arrest in case of a national security emergency.[248] One fifteen-year-long program gathered information about "the Communist Party, the Ku Klux Klan, antiwar groups, civil rights groups, women's rights groups, and gay rights groups."[249] And civil rights leader Martin Luther King was threatened using information from surveillance activities.[250] That work was in addition to criminal prosecutions and spying on citizens.[251] Today the problem is that the amount of data available to engage in similar information gathering is too easy to obtain and too tempting to ignore.

A large data set, a data hoard, may be accessed for a host of reasons: some desired—many not. Both the private sector and government keep such hoards, and both present threats to associational freedom. Government might access a private data hoard by demanding specific data about someone from a private data hoard.[252] With enough individual dossiers, government

246 *See* Jennifer Stisa Grannick & Christopher Jon Sprigman, *The Criminal N.S.A.*, N.Y. TIMES, June 27, 2013, http://www.nytimes.com/2013/06/28/opinion/the-criminal-nsa.html?pagewanted=all&_r=0 (arguing that the NSA PRISM program collecting large swaths of American email and other communications violates the law).

247 *See, e.g.*, Swire, *System of Foreign Intelligence*, *supra* note 2, at 1315–20 (listing a range of intelligence activities that made up what has become called actions by "The Lawless State").

248 Solove, *supra* note 5, at 139.

249 *Id.*

250 *See id.* at 140.

251 *Id.*

252 One's buying and reading habits on Amazon is an example of such data. Spiros Simitis identified the problem of private data revealing associational interests twenty-five years ago. Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L. REV. 707, 726 (1987) ("[T]he broad availability of personal data and . . . elaborate matching procedures [mean] individual activities can be accurately reconstructed through automated processing."). In response to this problem, Neil Richards has looked at private sector data collection/sharing and called for the need to protect "the ability . . . to develop ideas and beliefs away from the unwanted gaze or interference of others." Richards, *supra* note 17, at 389. As Richards argues, these areas are not protected under traditional privacy analysis, because it "misse[s]" the importance of these activities. *Id.* at 390. Julie Cohen's work on privacy and play completes the picture by connecting the problems of data, freedom from surveillance, and self-governance. *See generally* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF (2012) (arguing that moving beyond the bounds of liberal political theory is essential to understand intersections between different information rights regimes). We want people to have the "capacity for critical independence of thought and judgment," "self-actualization and reason," and "cosmopolitanism," because these capacities allow people to be full citizens of our society who can "identif[y]" and "pursu[e]" their personal and political self-fulfillment. Cohen, *supra* note 107, at 1911. But those capacities need room to develop, and in that sense we play. *Id.* We explore ideas and "boundar[ies]" of roles and social rules. *Id.* Those acts must be private in that they should be free from oversight, but they are also public in that we engage in play with others.

will have a good-sized hoard. Yet that takes time. One way to get around that effort is for government to acquire an entire private data hoard. For example, the FBI has gathered publicly available information "directly" through third parties, or the information has been handed over "voluntarily" by third parties.[253] The NSA's "Associational Tracking Program" has collected purely domestic communication information, including from and to whom a call is made, the length of the call, and when the call is made, on a daily basis for later analysis by the NSA.[254] This data has come directly from telecommunication providers such as Verizon, which complied with a court order.[255] In addition, the NSA has hacked telecommunication lines to gain access to communications and metadata passing through Google and Yahoo data centers.[256] Statements from the FBI indicate that it has received information from the NSA, and there is evidence that Muslim-American leaders' emails have been monitored.[257]

253 OFFICE OF THE ATTORNEY GEN., U.S. DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS 21–22 (2002), *available at* http://web.archive.org/web/20030403072729/http://www.usdoj.gov/olp/generalcrimes2.pdf. The NSA's recent activities map to behaviors that threaten and attack associational freedom. The NSA has targeted online activities of alleged Muslim radicalizers—those who offer troubling speeches—to secure information, such as about viewing pornography online, to discredit or embarrass the speakers. *See* Glenn Greenwald et al., *Top-Secret Document Reveals NSA Spied on Porn Habits as Part of Plan to Discredit "Radicalizers,"* HUFFINGTON POST (Jan. 23, 2014, 6:58 PM), http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html. To be clear, insofar as the targets are not residents of the United States, they receive less protection from this type of surveillance. The related concern, as Jameel Jaffer of the American Civil Liberties Union argues, is that one cannot tell whether the NSA is truly using a narrow focus as it conducts these sorts of operations. *Id.*

254 *See* Complaint, First Unitarian Church of L.A. v. NSA, No. 4:13-CV-03287-JSW (N.D. Cal. July 16, 2013), *available at* https://www.eff.org/files/filenode/firstunitarianvnsa-final.pdf; Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 5, 2013), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

255 *See* Exhibit A to Complaint, *First Unitarian Church of L.A.*, No. 4:13-CV-03287-JSW. Under FISA and the PRISM program, the NSA has also required Internet companies to provide access to their servers. *See, e.g.*, Steven Nelson, *What If Yahoo Just Said "No"?*, U.S. NEWS & WORLD REP. (Sept. 12, 2014, 5:44 PM), http://www.usnews.com/news/articles/2014/09/12/what-if-yahoo-just-said-no-to-the-nsa ("Internal NSA documents released by whistleblower Edward Snowden in June 2013 show that Microsoft in 2007 was the first major company to participate in PRISM, followed by Yahoo and then Google, Facebook, YouTube, Skype and others. A slideshow released by Snowden says the program allows direct access to the firms' servers to collect information on targets, which Yahoo has publicly disputed.").

256 *See* Max Ehrenfreund, *NSA Apparently Taps Google, Yahoo Networks Without Companies' Knowledge*, WASH. POST, Oct. 31, 2013, http://www.washingtonpost.com/world/national-security/nsa-apparently-taps-google-yahoo-networks-without-companies-knowledge/2013/10/30/f14749d0-4195-11e3-a751-f032898f2dbc_story.html.

257 *See* THE ASSOCIATED PRESS, *NSA Argues to Keep Hacked Data*, CED (Nov. 4, 2013, 12:28 AM), http://www.cedmagazine.com/news/2013/11/nsa-argues-to-keep-hacked-data ("If Congress were to shut down the government's collection of Americans' phone records

The amount of data available to government, regardless of source, creates a temptation for government to use data without limits. It is exactly this sort of temptation that can lead to "strong and systematic over-zealousness on the part of certain segments of executive officialdom" and that demands preclearance by the judiciary[258] and other protections. At least one study has shown that fear of recent, unfettered government information gathering programs has chilled associational activities.

The nonprofit PEN America has shown that the government's ability to gather information directly or from third parties has chilled associational activities of writers.[259] The study found that:

- 28% have curtailed or avoided social media activities, and another 12% have seriously considered doing so;
- 24% have deliberately avoided certain topics in phone or email conversations, and another 9% have seriously considered it;
- 16% have avoided writing or speaking about a particular topic, and another 11% have seriously considered it;
- 16% have refrained from conducting Internet searches or visiting websites on topics that may be considered controversial or suspicious, and another 12% have seriously considered it;
- 13% have taken extra steps to disguise or cover their digital footprints, and another 11% have seriously considered it;
- 3% have declined opportunities to meet (in person, or electronically) people who might be deemed security threats by the government, and another 4% have seriously considered it.[260]

As scholars of association might say, with surveillance the room to disagree about what the common good is diminishes.[261]

---

every day, which it has been secretly doing since 2006, 'we wouldn't be able to see the patterns that the NSA's programs provide us,' said Patrick Kelley, acting general counsel of the FBI. Kelley added that the FBI would not be able to weed out significant phone data if it did not have the NSA's massive data bank to tap into, and would lose valuable time if it had to instead seek the data from individual phone companies."). There is also evidence that the FBI and NSA have monitored U.S. persons, specifically Muslim-Americans. *See* Glenn Greenwald & Murtaza Hussain, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On*, INTERCEPT (July 9, 2014), https://firstlook.org/theintercept/2014/07/09/under-surveillance/. The NSA is allowed to conduct surveillance on non-U.S. persons and has done so in tracking information including porn-watching habits of alleged radicalizers. *See* Greenwald et al., *supra* note 253. As Jameel Jaffer, Deputy Director of the ACLU, notes the problem is that "the NSA's surveillance activities are anything but narrowly focused—the agency is collecting massive amounts of sensitive information about virtually everyone." *Id.* The list has been shared with fifteen agencies including "the Departments of Justice and Commerce and the Drug Enforcement Administration." *Id.* For a list of distribution recipients, see Greenwald et al., *supra* note 253.

258 Amar, *supra* note 117, at 810.

259 *See Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor*, PEN AM. (Nov. 12, 2013), http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf.

260 *Id.* at 6.

261 *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1653 (1999) ("The health of a democratic society depends both on the group-oriented process

One way to think of the problem is as the need for anonymity. Christopher Slobogin has explained that perspective: "Anonymity in public promotes freedom of action and an open society. Lack of public anonymity promotes conformity and an oppressive society."[262] He calls this problem "public privacy."[263] That seeming oxymoron captures the need to be public, yet private from government oversight. It is anonymity to the government that matters. That anonymity may be based on protections from direct surveillance or protections from the government accessing third party, private sector records of recent and past communications and acts. Julie Cohen has shown why that is so.[264] Surveillance changes behaviors, because "the experience of being watched will constrain, ex ante, the acceptable spectrum of belief and behavior."[265] Instead of robust, diverse, and challenging ideas, we will favor the "the bland and the mainstream."[266] We end up with a diminished "capacity to act and to decide," which leads to "the highest possible degree of compliance with [what the state determines is] the model . . . citizen."[267] This problem is a type of chilling effect.[268]

Put differently, we live in an information state, but not what Jack Balkin has called a "democratic information state."[269] That distinction makes all the difference in protecting associational freedom. A democratic information state exercises data discipline. Regardless of how information is gathered, democratic information states must:

> collect and collate only the information they need to ensure efficient government and national security. They do not keep tabs on citizens without justifiable reasons; they create a regular system of checks and procedures to avoid abuse. They stop collecting information when it is no longer needed and they discard information at regular intervals to protect privacy. When it is impossible or impractical to destroy information—for example, because it is stored redundantly in many different locations—democratic information states strictly regulate its subsequent use.[270]

---

of democratic deliberation and the functioning of each person's capacity for self-governance."); *cf.* Inazu, *supra* note 51, at 576 (noting that the purposes of assembly are not limited to the common good).

262 SLOBOGIN, *supra* note 212, at 92.

263 *Id.*

264 *See generally* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) (calling for strong data privacy protection).

265 *Id.* at 1426.

266 *Id.*

267 Simitis, *supra* note 252, at 733.

268 *Accord* United States v. Stewart, 686 F.3d 156, 171–73 (2d Cir. 2012); *see* Frederick Schauer, *Fear, Risk and the First Amendment: Unraveling the "Chilling Effect,"* 58 B.U. L. REV. 685, 693 (1978) ("A chilling effect occurs when individuals seeking to engage in activity protected by the first amendment are deterred from so doing by governmental regulation not specifically directed at that protected activity." (emphasis omitted)); *see also* Solove, *supra* note 5, at 154–59 (discussing cases where courts have found information gathering to have a chilling effect).

269 Balkin, *supra* note 13, at 17.

270 *Id.* at 18 (emphasis added).

Balkin's democratic information state maps to the limited information collection and return procedures required when following warrant procedures. Limiting information collection to what is necessary and rejecting broad systems of "keeping tabs on citizens" connects to the reasonableness inquiry. Calling for checks and procedures fits within the idea of judicial clearance and ongoing justification for surveillance. And, the claim that data must be destroyed or subsequent use "strictly regulate[d]" makes perfect sense because of the temptation problem.[271] Even after the checks and balances for the intake of data are in place, we need them for what may be done later. But as we have seen, these practices are not in place for data. Instead, we leave data hoards unregulated.

Claims that government should have unfettered access to or maintain its own data hoard make no sense, as soon as one appreciates how those claims affect associational freedom. The government has asserted, "[i]f you're looking for the needle in the haystack, you have to have the entire haystack to look through."[272] One irony is that the cell phone data program sought, and at one point may have had, one hundred percent of our call data; but the government now claims it has been only able to obtain thirty percent, while also wanting to return to having higher amounts of the call data. The varying claims about amounts of data and needs for data reveal the problem. On the one hand, if government is collecting all data possible that may make sense for discerning patterns of threats as opposed to targeting specific people.[273] But the new claim that we need not worry, because the program collected a smaller amount, indicates that the claims for why the program was in place are dubious or false.[274]

When the government claims it needs vast amounts of data to do its job in seeking out terrorists, it is using the same, rejected logic argued in association cases. The discussion over how much data is collected can miss the key point here.[275] Whether one calls it protecting from incitement to riot or

271 *Id.*

272 *See* Ellen Nakashima, *NSA Is Collecting Less than 30 Percent of U.S. Call Data, Officials Say*, WASH. POST, Feb. 7, 2014, http://www.washingtonpost.com/world/national-security/nsa-is-collecting-less-than-30-percent-of-us-call-data-officials-say/2014/02/07/234a0e9e-8fad-11e3-b46a-5a3d0d2130da_story.html (quoting Deputy Attorney General James Cole) (internal quotation marks omitted).

273 Whether data analysis and data mining may be used by law enforcement is an important question but is beyond the scope of this Article.

274 Nakashima, *supra* note 272 ("[T]he revelation [of the smaller data set] 'calls into question whether the rationale offered for the program is consistent with the way the program has been operating.'" (quoting Professor Edward Felten)).

275 *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (expressing concern that GPS tracking "mak[es] available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track"); *cf.* Gray & Citron, *supra* note 231, at 101 ("[T]he threshold Fourth Amendment question raised by quantitative privacy concerns is whether an investigative technique or technology has the capacity to facilitate broad programs of indiscriminate surveillance . . . ."). *But see* Orin S. Kerr, *The Mosaic Theory of the*

ensuring national security, there is a broad claim of need that in reality enables suppression of association. When associational interests are at stake, criminal procedure must account for associational interests. Criminal procedure has done so for bugging, wiretaps, and GPS tracking in real time. The law must now fully recalibrate for the new era of backward-looking data-driven surveillance.

III. Discipline and Data Hoarding

The procedural protections for information gathering are monuments of a dead era. We look at them, applaud them, and understand from where they came. They have some relevancy. But like steam engines in a railroad museum that can still run, they do not serve our needs well. The way we share and store data has shifted. The new frontier must address different problems. The government can obtain sensitive data that would be restricted and managed if obtained with forward-looking surveillance, simply by looking backward.[276] When it does so, warrant protections are gone, but the threat to associational freedom is large.[277] This Part sets out the procedures to manage backward-looking surveillance. Specifically, I argue that backward-looking surveillance should be time limited just as we limit forward-looking wiretaps and tracking. In addition, we should re-embrace the return requirement. That requirement allows government to obtain material with a warrant, but give the material back once the government investigation is over. Recapturing this limit would mitigate the government's ability to keep data hoards and dossiers that can be used to threaten our associational freedom.

A. Against General Warrants for Data

The solution to the problems of data exhaust lies in the limits we have for forward-looking surveillance. The harms of unauthorized surveillance reappear when the government is allowed to dig up our past associational activity without limit. Unfettered surveillance even in public places poses harms by chilling freedom of association. Warrant procedures are the safeguards to mitigate those harms. They are not perfect, but they create the possibility for a check and balance on executive actions. The best answer for the problems of data gathering is to institute warrant procedural protection for such requests. As we will see, each of the steps matter, but the time limits and the necessity of return are especially important.

Fourth Amendment, 111 Mich. L. Rev. 311, 314–15, 344 (2012) (arguing that exactly what the threshold is for an amount of data to be a problem is too indeterminate to be useful).

276 *See* Patricia L. Bellia, *The Memory Gap in Surveillance Law*, 75 U. Chi. L. Rev. 137, 166 (2008).

277 *See id.* at 139; *cf. In re* U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("[Authorization of] [o]rders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional.").

Given the harms, a magistrate should review a warrant for phone records, web sites, GPS coordinates or other data exhaust, and the warrant must be specific regarding the crime, from whom the data is coming, and the data to be seized.[278] Those requirements are obvious but not in place. The current system thus allows the government to forgo establishing probable cause and use a general warrant approach to surveillance.[279]

Time limited surveillance is a vital part of the balance between civil rights and government needs.[280] We all live under the possibility that tomorrow law enforcement may consider us a suspect, establish probable cause, and then conduct surveillance on us. Once that happens, the government may stumble upon our noncriminal associations, but when this occurs, law enforcement is not supposed to continue the surveillance.[281] In fact, with a wiretap, listening must be "conducted in such a way as to minimize the interception of communications not otherwise subject to interception."[282] Steps to comply with this mandate include using "spot checks"—listening for short periods such as one or two minutes—to see whether criminal acts are being discussed.[283] When discussions are not germane to the criminal investigation, law enforcement must stop listening.[284] Even one hour of uninterrupted listening can be long enough to suppress the evidence learned from the wiretap, when there is no evidence of criminal acts being discussed.[285] Unlike the bulk data programs of the NSA and FBI, the emphasis is on not listening rather than gathering all conversations and sorting them later. Even when following minimization procedures, the government cannot listen in on or track us for more than thirty or forty-five days without continually showing the need to do so.[286] Thus suppose you joined the Communist Party when it advocated the overthrow of the U.S. government, opposed the IRS and taxes, joined an Islamic charity that turned out to be a front, advocated for the ability to own and carry assault weapons, demonstrated against a war, and so on. You know that the government may begin watching you subject to some limits. That is a risk. But suppose also that after your activity, you stopped. You moved away from those areas. After you stopped, you have protection that the government will have less ability to watch you. In contrast, the current system allows a broad vacuum approach to data that reveals noncriminal activity that reaches deep into one's past. In fact, the NSA and FBI have often used this loophole to maintain dossiers of noncriminal activity precisely because they can use them to threaten people and associations not in line with incumbent power. The question "isn't it true you were a member

278 *See* Berger v. New York, 388 U.S. 41, 59 (1967).
279 *Id.*
280 *Id.* at 59–60 (explaining why time-limited surveillance is required).
281 *See* 18 U.S.C. § 2518(5) (2012).
282 *Id.*
283 *See, e.g.*, United States v. North, 735 F.3d 212, 216 (5th Cir. 2013).
284 *Id.*
285 *Id.*
286 18 U.S.C. § 2518(5); FED. R. CRIM. P. 41(e)(2)(C).

of the Communist Party?" becomes all the more powerful when you know any association from your past may be found and used against you. The threat of persecution for noncriminal acts attacks associational freedom by undermining the way associations "form and grow."[287]

Just as we don't allow unending surveillance because it "is the equivalent of a series of intrusions, searches, and seizures pursuant to a single showing of probable cause,"[288] we must limit how far back law enforcement can dig. But what would a termination date look like? Forward-looking surveillance requires a date by which it ends;[289] yet currently law enforcement may ask for as much data going as far back as a third party may keep records. In the past, those records may not have been kept for long because of cost. Today, however, it is much less expensive to keep such records, *and* businesses often keep such records as part of complying with government regulations and/or part of using data to operate and understand their business. Thus law enforcement might be able to ask for a month, a year, two years, seven years of data—in short, for as much data as possible.

I offer that a good way to limit this sort of grab is to mirror the time limits for forward-looking surveillance. Establishing the optimal time limit for backward-looking surveillance is beyond the scope of this Article. Indeed each of the three branches of government has ways to address the issues this Article raises. As with earlier changes in surveillance power, courts have started to establish some limits on surveillance that implicates associational freedom. The legislature could step in and offer a solution similar to the way it did when passing the Wiretap Act. Or the executive could issue an order to limit the way data is used. That said, I offer as a starting point one model. A thirty-day limit, as is the case for wiretapping, could be the baseline.[290] If, however, one believes location data is not content or to be protected as much as what one might say on the phone, data exhaust would be closer to GPS tracking data. Even so, requests for data should be limited to forty-five days just as GPS tracking is limited to forty-five days for forward-looking surveillance.[291] For example, assume there is a forty-five day time limit, and imagine you are investigating a bank robbery. To obtain the first chunk of data, you'd follow warrant procedures, obtain and analyze the data, and see what you could learn about your suspects. If that request revealed enough data for the prosecution, you'd stop. If the data indicated more people were involved and/or the robbery was part of a larger, complicated criminal endeavor, you'd go back to the judge, make your case, and request authorization for more data on the new people. In addition, you could ask permission to go back another forty-five days for the original suspects. As with forward-looking surveillance, there may be a long surveillance period—months or even years of data if approved—and/or large surveillance net—covering many different

287 *See supra* notes 109–10 and accompanying text.
288 Berger v. New York, 388 U.S. 41, 59 (1967).
289 *Id.*
290 18 U.S.C. § 2518(5).
291 FED. R. CRIM. P. 41(b)(4); FED. R. CRIM. P. 41(e)(2)(C).

conspirators. The goal is that once the investigation has what it needs and there is no evidence of new suspects, the backward-looking data requests would have to stop. By limiting how far back an investigation can search, this approach protects associational concerns surveillance inherently threatens, because it opens the door to freedom from future persecution. Nonetheless, the ability to access our records reveals another constitutional infirmity.

Current data gathering does not provide for the return of data once an investigation is over, but return or destruction is precisely what the Constitution requires.[292] A core but underappreciated principle of criminal procedure is that the government must return items taken as part of an investigation once they are not needed.[293] A major problem for the *Berger* Court was that the New York statute did not provide for a return on the warrant, and thus law enforcement could use "seized conversations of innocent as well as guilty parties"[294] in perpetuity. Similar to the minimization procedures for wiretapping, return imposes a limit on the way the government can have access to data not pertinent to an investigation. As Harold Krent has explained, information taken by law enforcement must be "consistent with the reasonableness requirement of the Fourth Amendment. Once such purposes no longer exist, justification for continued possession of . . . information ceases."[295] The need to delete data has been missed, perhaps because it was not seen as the equivalent of papers or the less tenable content/non-content distinction. But if a recorded conversation, which today would be digital, has to be destroyed, data should be treated the same way. The focus should be on the harm, which is the way the retained information could include innocent people's information and/or could be used in perpetuity. Return as deletion would limit the ability to hoard data for non-investigative activity. In addition, we must have notice about what data is being collected from third parties absent "exigent circumstances."[296] Without that protection, we never know that the data has been collected. Instead there is a "blanket grant of permission to eavesdrop" that lacks "adequate judicial supervision or protective procedures."[297]

This approach does not turn on a property distinction. *Katz* explained that the Constitution protects people, not places, but we still have extra protection for places such as the home. I argue that the Constitution protects

---

292 *Berger*, 388 U.S. at 60; *accord id.* at 66 (Douglas, J., concurring).

293 Krent, *supra* note 14, at 50–51 (arguing for increased limits "on what law enforcement officers can do with property and information after a legitimate search and seizure" including subjecting data to the return requirement). Krent's focus was mainly on the way law enforcement might further disclose information and relied on the idea of coerced information gathering to determine reasonableness. *Id.* at 51, 76–77. Those concerns matter, but this Article asks about the harms from collection regardless of disclosure to a general public and when there is not coercion.

294 *Berger*, 388 U.S. at 60.

295 Krent, *supra* note 14, at 69.

296 *Berger*, 388 U.S. at 59–60 (noting that the state statute at issue in *Berger* "permits unconsented entry without any showing of exigent circumstances").

297 *Id.* at 60.

associational freedom and has extra protection for speech. As Balkin explained, a democratic information state must limit its data collection, delete the data, or "strictly regulate its subsequent use."[298] Those ideals fit within the way the Fourth Amendment protects associational freedom.

What we need is data separation—a way to keep government away from the data hoards by which it is tempted to abuse associational freedom. Limited collection at the outset of an investigation—i.e., avoiding bulk data grabs—separates government from data not related to the investigation. If for some reason bulk data grabs were reasonable, deletion of the data after the investigation is over would reestablish data separation. That would eliminate the government's data hoard. Government would have to go back to private hoards for the same data. Assuming we have procedures with judicial oversight and limited data requests, we would have maintained data separation at both the intake and ongoing use level. We will have started to discipline data hoarding. That said, there are limits to the associational freedom analysis.

B. Associational Freedom in Perspective

Associational freedom cannot explain all aspects of limiting surveillance; not all surveillance triggers the limits offered here.[299] Pervasiveness is a key factor in determining whether the surveillance in question implicates associational freedom and thus must be restricted. Secrecy matters. Cost plays a role as well. None of these factors is dispositive. As I have argued throughout this Article, the method must be to identify when surveillance chills associational freedom. Some examples help see how this may work.

Consider watching someone in public. Following a car with one or a team of police or watching people in public places are different practices than the ones that raise associational alarms. They are analog acts with high costs. They don't sweep in all of a suspect's noncriminal activities to date or the activities of the rest of us. As the *Jones* court pointed out, that changes if all cars are required to have GPS or enough do that third parties now in effect track us for the police. Video camera or closed-circuit television surveillance is another example of shifting threats to associational freedom. Such systems have been allowed in part because they film public places.[300] But whether a system itself is unconstitutional has not been addressed.[301] A large-scale camera system has obvious associational implications. It would

298 Balkin, *supra* note 13, at 18.

299 *See, e.g.*, Solove, *supra* note 5, at 152 ("Almost every search or seizure could be understood to have some dimension that might involve a First Amendment activity because all human interaction involves communication and association. In the end, the First Amendment could swallow up all of criminal procedure." (footnote omitted)).

300 SLOBOGIN, *supra* note 212, at 155 ("[C]ourts that have considered application of the Fourth Amendment to cameras aimed at public streets or other areas frequented by a large number of people have declared that such surveillance is not a search, on the ground that any expectation of privacy one might have in these areas is unreasonable.").

301 *Id.*

catch us as we went to offices, churches, temples, hotels, and bars. It would capture with whom we went to those places or who entered them for later cross-referencing. Yet current technology may not allow law enforcement to search hundreds or thousands of hours to identify who was doing those activities. The cost to store the video may still be expensive given the size of the files. But the cost to store data keeps dropping and facial recognition software keeps improving. The science fiction world of feeding a face into a computer to see whether there is a match even in a vast sea of noisy data will be a reality much faster than we might think. As that happens, associational freedom analysis would tilt towards requiring procedures and oversight to limit law enforcement's ability to access and use the data.

There are some other open questions here. Government could create its hoard based on proper, targeted investigation and surveillance. As with other areas of investigation, government would likely be allowed to keep that data just as it keeps fingerprints, mug shots, and DNA from those under suspicion or if they are convicted felons.[302] Even so, as technology makes the ability to analyze such information easier and more powerful, government might learn about much more than criminal matters. Associational analysis will be required, when the technology shifts the power of government to learn from the data. That analysis may still allow use of the data, because we don't afford felons the same rights as non-felons.[303] But the key point is to have the debate and explain how such use does not threaten associational freedom. The idea of data analysis brings us to another problem that this Article has left for another time, but that should be noted.

Data hoards are not going away, and they can be useful. The ideas set forth here seek to limit the harms that data hoards can foster. One idea might be to delete hoards regularly, as some businesses do with their records. Or we might limit the amount and how long data is stored by government or even third parties.[304] After all, we know that the government has gone into private data either under the cloak of national security or as outright invasion. Yet, we may want to have the ability to search that data in a targeted manner, precisely because we can tell who planned a robbery, kidnapped a child, or planted a bomb. Rather than trusting the government to do the right thing, an escrow with proper oversight could be in place if we choose to maintain data hoards for governmental use.[305] This solution brings us back to our problem and core point. A data escrow is still a data hoard. Data

302 *See* Krent, *supra* note 14, at 95–96.

303 *Id.* at 96–97.

304 Private sector data practices are a subject for another time, but one reason not to dictate terms is that the private sector uses data to improve its business and learn. *See* VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA 27 (2013).

305 A version of this idea has been offered in response to the NSA data-gathering program. President Obama has agreed with the Final Report of the Review Group on Intelligence and Communications Technologies proposal that bulk metadata should be kept in third party hands or some special third party storage entity. *See* Josh Keller et al., *Obama's Changes to Government Surveillance*, N.Y. TIMES, Jan. 17, 2014, http://www.nytimes.com/interactive/2014/01/17/us/nsa-changes-graphic.html?ref=technology. That proposal

hoards always present a great temptation for abuse. No matter what we decide is the best way to manage access to data hoards, there will always be the temptation—perhaps even in good faith as the executive tries to protect us—to cut corners or use new methods that appear sound. The key principle must be to ask whether new techniques threaten associational freedom, and if so, what we must do to protect that freedom.

The idea is perhaps radical but not all encompassing. It is radical in the true sense of the word. Associational freedom is at the root of our democracy. Our Constitution protects acts that are not speech and are not private. As such I have argued that associational freedom must be part of the reasonableness inquiry. The idea is limited because of practical factors. The reasonableness inquiry often requires recalibration. The concurrences in *Jones* called out a current moment for recalibration: the potential for unending forward and backward tracking. They noted that assuming that anything we share with third parties had no protection from law enforcement harmed "associational freedom." I have sought to support that point by showing what that freedom is, what actions can harm it, and the grounds for protecting it. Once we understand associational freedom, not only can we better set limits on current surveillance, but we have the tools to assess new surveillance technology as it emerges.

Conclusion

Associational freedom has many forms, is vital to our democracy, and must be protected. Yet, it has been forgotten as an independent interest. Instead of recognizing, as the Founders did, that many activities that are not speech and not private still deserve protection, we have moved to a world where only speech and private acts are free from government oversight. Thus many activities such as meeting, reading, sharing ideas, and traveling have become fair game for government surveillance. But surveillance chills associational freedom. Indeed, surveillance has been used time and again to suppress associational freedom of precisely the groups—free thinking, dissident, challenging—the Constitution is supposed to protect. In the past, surveillance was expensive and difficult. Today, it is cheap and easy. In addition, the sort of surveillance that threatened associational freedom often required judicial oversight and limits. But technology has created a loophole. The government can simply go to a third party and demand data. There is little, to no, oversight, and the request can cover years of data about where we went, with whom we spoke, and what we have read. The government can have unfettered access to a perfect picture of our activities and associations regardless of whether they are criminal. This Article has argued this asymmetry of protection cannot be allowed to continue. It has offered that protecting associational freedom in all its forms—the right to petition,

relates to national security and NSA practices. *Id.* Nonetheless, the insight should apply for domestic surveillance as well.

to assemble, to share ideas, to critique, to celebrate, to read, to coordinate activity, to march, and more—is a core part of our democracy and is protected by the Fourth Amendment.