THE REVOLUTION WILL BE TWEETED, BUT THE TWEETS WILL BE SUBPOENAED: REIMAGINING FOURTH AMENDMENT PRIVACY TO PROTECT ASSOCIATIONAL ANONYMITY

Chris J. Chasin†

Abstract

The associational privacy doctrine has historically protected the anonymity of expressive association, shielding those in unpopular social, political, and religious groups from the substantial chilling effect that public identification can have on First Amendment activity. Group activity, however, has changed since the doctrine's establishment: technology and social media are now an inseparable part of modern social movements and modern life. Government surveillance of network data, an increasingly visible law enforcement practice since September 11, now threatens to strip the anonymity so vital to expressive activity.

This surveillance occurs at three distinct levels. At the recipient level, the government can access information voluntarily transmitted over the Internet. At the transmitter level, the government can obtain communications information from service providers. And at the reconstructive level, the government can use data mining software and disparate, scattered sources of information to reconstruct individual activities and social networks.

At each of these levels, the information that the government seeks falls outside the scope of the Fourth Amendment's protections, which are based on an unworkable binary conception of privacy. But privacy is fluid, and access at each of these levels has a clear potential to chill expressive association. Expanding on existing Fourth Amendment and First Amendment scholarship, this Article examines the First Amendment hazards of failing to protect these "unreasonable" expectations of privacy. It seeks to more fully integrate associational privacy concerns into the Fourth Amendment context by proposing a novel framework of potential expansions to the Katz *doctrine,*

---

† Research and Bluebook Editor, Volume 162, *University of Pennsylvania Law Review*; J.D. Candidate, 2014, University of Pennsylvania Law School; B.A., Haverford College. The author thanks Anita Allen for her invaluable guidance and mentorship, Lydia F. Emery for her helpful comments, and the editors of the University of Illinois Journal of Law, Technology & Policy for their thoughtful revisions.

based on the recognition of "unreasonable" expectations of privacy.

TABLE OF CONTENTS

I. INTRODUCTION

The past decade has seen a rapid growth in society's technological consumption. Technology has enacted a radical and permanent change to the way society works, plays, and associates, in the process becoming unavoidably integrated into daily life. This proliferation of technology creates problems for expressive associations and challenges the protections of the right to associational privacy.[1] For a non-extremist expressive association to remain viable, it can no longer avoid using technology or try to control the technology use of its members. However, technology use brings with it significantly

1. An expressive association is an association engaged in expressive activities protected by the First Amendment. BLACK'S LAW DICTIONARY 735 (9th ed. 2009).

increased exposure to government investigations and surveillance, creating a strong chilling effect on associational activity.[2] If the traditional values of associational privacy are to remain protected, greater restrictions must govern how, and when, the government can gain access to information pertaining to an individual's technology and network use, and a new conception of the Fourth Amendment must be adopted to protect certain "unreasonable" expectations of privacy.

The year 2011 was a critical turning point in popular conceptions of the societal role of technology and the Internet. The first decade of the new millennium saw the Internet grow to accommodate many functions of daily life. Americans increasingly took to Facebook,[3] Twitter,[4] LinkedIn,[5] Google,[6] and Yelp[7] to express themselves, to communicate, and to learn.[8] But as the "Arab Spring" faded into the "American Autumn," it became clear that the Internet had also taken on a role as a critical component in expression, association, and democracy.

Occupy Wall Street ("Occupy") retained the trappings of traditional protest (signs, chants, and encampments in public places) that were so familiar to the Bonus Army of the 1930s, the Civil Rights marchers of the 1960s, and the anti-war protestors of the 1970s. But Occupy also had a media tent, where generators powered laptops, cameras, and 4G Wireless hotspots while volunteers worked around the clock to update accounts on Twitter, Facebook, YouTube, Flickr, Wordpress, and Tumblr.[9] During the Civil Rights movement, controversial images of police brutality appeared in newspapers and on the evening news; during Occupy, videos and images of police brutality circulated the Internet almost immediately after the incident occurred,[10] sometimes reemerging later as pop culture icons.[11]

---

2. *EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association*, ELEC. FRONTIER FOUND. (Nov. 6, 2013), https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association [hereinafter EFF].

3. FACEBOOK, http://www.facebook.com (last visited Feb. 12, 2014).

4. TWITTER, http://www.twitter.com (last visited Feb. 12, 2014).

5. LINKEDIN, http://www.linkedin.com (last visited Feb. 12, 2014).

6. GOOGLE, http://www.google.com (last visited Feb. 12, 2014).

7. YELP, http://www.yelp.com (last visited Feb. 15, 2014).

8. *See* Steve Olenski, *Social Media Usage up 800% for U.S. Online Adults in Just 8 Years*, FORBES (Sept. 6, 2013, 10:13 AM), http://www.forbes.com/sites/steveolenski/2013/09/06/social-media-usage-up-800-for-us-online-adults-in-just-8-years/ ("[S]ince the year 2005, the number of online U.S. adults who use social media sites has risen from 8% to 72% as it currently stands in the year 2013.").

9. *See* Sam Schlinkert, *The Technology Propelling #OccupyWallStreet*, DAILY BEAST (Oct. 6, 2011, 5:09 PM), http://www.thedailybeast.com/articles/2011/10/06/occupy-wall-street-protests-tech-gurus-televise-the-demonstrations.html (highlighting the role technology played in sustaining the Occupy Wall Street movement).

10. *See, e.g.*, Jamie Hall, *Police PEPPER SPRAY UC Davis STUDENT PROTESTERS!*, YOUTUBE (Nov. 18, 2011), http://www.youtube.com/watch?v=wuWEx6Cfn-I (depicting U.C. Davis police pepper-spraying non-violent protestors); *see also* Christina Boyle & John Doyle, *Pepper-Spray Videos Spark Furor as NYPD Launches Probe of Wall Street Protest Incidents*, N.Y. DAILY NEWS (Sept. 29, 2011, 4:00 AM), http://www.nydailynews.com/news/crime/pepper-spray-videos-spark-furor-nypd-launches-probe-wall-street-protest-incidents-article-1.952167 (reporting on several videos depicting the unwarranted pepper-spraying of non-violent protestors).

11. *See, e.g.*, PEPPER SPRAYING COP, http://pepperspraying cop.tumblr.com (last visited Feb. 12, 2014) (displaying examples of an Internet meme based on a photograph of Lieutenant John Pike pepper-spraying

Beyond the bounds of Zuccoti Park, society's relationship with technology has fundamentally changed. Over forty-six percent of American adults own smartphones.[12] Online, fifteen percent of adult Americans use Twitter,[13] and sixty-five percent of online adults use social networking sites like Facebook, LinkedIn, or Myspace.[14] Two-thirds of Americans shop online, and over one-third of Americans use online banking.[15] As a society, we have come to rely heavily on technology and the Internet.

Yet this technology is open to abuse. Privacy is sacrificed to obtain functionality and responsiveness. The increasing incorporation of technology into daily life has exposed associational activities to government surveillance and investigation.[16] Traditional constitutional and statutory protections for electronic information have not kept pace with the ever-increasing role of technology in modern life. First Amendment activities, however, have evolved with technology. Associational privacy has always been treated as protecting against compelled testimony.[17] Yet, the right to associational privacy has not been similarly extended into the Fourth Amendment context as a restraint on government investigative activity generally.[18]

Modern technology now enables the government to bypass the traditional protections of associational privacy. The doctrines have not changed, but changes in the world to which they are applied have left associational privacy unprotected against government investigation and surveillance, creating the potential for significant chilling of expressive association.[19] This Article examines how new technologies create chilling effects[20] on membership in expressive associations, implicating the right to associational privacy. In part, the impact of technology on associational privacy is an inevitable result of

---

seated U.C. Davis students during a November 18, 2011, Occupy protest).

12. AARON SMITH, PEW RESEARCH CTR., NEARLY HALF OF AMERICAN ADULTS ARE SMARTPHONE OWNERS 2 (2012), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/Smartphone%20ownership%202012.pdf.

13. AARON SMITH & JOANNA BRENNER, PEW RESEARCH CTR., TWITTER USE 2012, at 2 (2012), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2012/PIP_Twitter_Use_2012.pdf.

14. MARY MADDEN & KATHRYN ZICKUHR, PEW RESEARCH CTR., 65% OF ONLINE ADULTS USE SOCIAL NETWORKING SITES 2 (2011), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2011/PIP-SNS-Update-2011.pdf.

15. JAMES HORRIGAN, PEW RESEARCH CTR., ONLINE SHOPPING 2–6 (2008), *available at* http://www.pewinternet.org/files/old-media//Files/Reports/2008/PIP_Online%20Shopping.pdf.pdf.

16. An association is "[a] gathering of people for a common purpose [or] the persons so joined." BLACK'S LAW DICTIONARY 141 (9th ed. 2009).

17. The majority of associational privacy cases involve compelled testimony, either by an individual (e.g., forcing a door-to-door solicitor to wear a nametag) or by a group (e.g., subpoenaing membership lists). *See generally* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (restricting the government's ability to subpoena the membership list of the NAACP without sufficient justification).

18. *But cf.* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 806 (1994) (arguing that First Amendment concerns should be incorporated into the Fourth Amendment's constitutional reasonableness analysis).

19. *See* EFF, *supra* note 2 ("The Electronic Frontier Foundation (EFF) has provided a federal judge with testimony from 22 separate advocacy organizations detailing how the National Security Agency's (NSA) mass telephone records collection program has impeded the groups' work, discouraged their members and reduced the numbers of people seeking their help via hotlines.").

20. A chilling effect is a result of law or practice that seriously discourages the exercise of a constitutional right. BLACK'S LAW DICTIONARY 274 (9th ed. 2009).

increased publication of information through social media and other sources. In part, however, this chilling effect is a result of statutory protections for domestic electronic communications lagging decades behind the evolution of technology and modern conceptions of electronic privacy.

The types of privacy violations examined in this Article arise at three distinct levels of communication: those of the recipient, the transmitter, and reconstruction. Recipient-level access occurs when law enforcement officers view public content or private content that they lawfully gained access to through deceit. Transmitter-level access occurs when third-party service providers supply the police with content or transactional data. Finally, reconstructive access occurs when the government uses data mining to generate information about the individual that has not been shared with others through the analysis of disparate data sources. Each level of access is accompanied by a different "unreasonable" expectation of privacy.

The obvious argument against responding to this chilling effect is that expressive associations take the risk of surveillance when they use technology and social media.[21] However, expressive associations have no choice: to decline to use modern technology and media, in this day in age, would render all but the most disciplined extremist groups unable to recruit members, coordinate activities, and function effectively. A group is thus faced with the Catch-22 of either (a) exposing itself to surveillance so that it may use modern technology or (b) avoiding all possible avenues of surveillance, and thereby handicapping its ability to function. Either of these alternatives has a clear chilling effect on the group's speech.

Most scholarly approaches addressing this problem call for either improvements to existing statutes or the recognition of new constitutional rights.[22] However, neither of these approaches presents a satisfactory solution to the problem. The creation of new rights, though theoretically effective, would create too high a burden on government interests and the judiciary, incentivizing the covert use of illegal methods of data acquisition and resulting in an even greater chilling effect. Revision of the outdated statutory protections may be effective in the short term, but it is unlikely that statutory revisions imposing direct restrictions can keep up with the evolution of technology and society. Statutory revision is also likely to be insufficient due to the non-representative nature of legislatures with regard to technology adaptation. Those with the most interest in Internet associational privacy protections are Internet natives who grew up using the Internet, but the government is almost solely composed of Internet migrants who have adopted the Internet late in their lives.[23] It is doubtful that these two groups have the

21. This is not a new phenomenon. As Anita Allen notes in UNPOPULAR PRIVACY, there is "nothing new about 'Americans [being] . . . willing to give up a certain amount of privacy in exchange for the fun and convenience' of novel inventions" such as the Kodak camera or the postcard. ANITA L. ALLEN, UNPOPULAR PRIVACY, at x (2011) (citing FREDERICK S. LANE, AMERICAN PRIVACY: THE 400-YEAR HISTORY OF OUR MOST CONTESTED RIGHT 31–32 (2009)).

22. *See generally infra* Part V.B–C.

23. Though Internet natives will increasingly populate government, by the time they do so, they will be "migrants" to the next wave of technological development. Mark Prensky, *Digital Natives, Digital*

same conceptions of the Internet and therefore unlikely that they recognize the same rights and responsibilities in Internet activity.[24]

This Article sets forth a new proposal which takes into account both privacy interests and government policing needs in an attempt to protect associational privacy and modern conceptions of Internet privacy. To achieve this, it is necessary to reject the current Fourth Amendment doctrine's binary "reasonable expectation" conception of privacy[25] and to instead reimagine a multi-faceted Fourth Amendment framework recognizing that expectations of privacy can be complex. This framework recognizes the existence of "unreasonable" expectations of privacy, and this Article sets forth statutory proposals that seek to balance those expectations with valid governmental interests.

II. FIRST AMENDMENT ASSOCIATIONAL PRIVACY

A. NAACP v. Alabama *and Subsequent Cases*

The concept of associational privacy is relatively young, having been endorsed by the Supreme Court fifty-five years ago in *NAACP v. Alabama* ex rel. *Patterson*.[26] *NAACP v. Alabama* arose from Alabama's effort to terminate the NAACP's thirty-eight-year presence in the state through the enforcement of a corporate qualification statute.[27] The State Attorney General filed suit against the NAACP in an Alabama court seeking to enjoin the NAACP from conducting further activities in Alabama, effectively ousting it from the state.[28] As part of its discovery, the state demanded the NAACP's general membership records. The NAACP refused to produce these records and was held in contempt of court.[29] The NAACP appealed to the Supreme Court, contending that its membership rolls were constitutionally protected against the forced disclosure.[30]

Immigrants, ON HORIZON, Sept.–Oct. 2001, at 1, 2.

24. Marc Prensky, who first used the "native/migrant" typology, cautioned that "[a]s Digital Immigrants learn – like all immigrants, some better than others – to adapt to their environment, they always retain, to some degree, their 'accent,' that is, their foot in the past." *Id.* at 1–2. *But see* David S. White & Alison Le Cornu, *Visitors and Residents: A New Typology for Online Engagement*, FIRST MONDAY (Sept. 5, 2011), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3171/3049 (rejecting the age-focused native/migrant model for a usage-based visitor/resident model).

25. Andrew D. Selbst, *Contextual Expectations of Privacy*, 35 CARDOZO L. REV. 644, 654–69 (2013).

26. NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958).

27. *See id.* at 452 ("The Association has never complied with the qualification statute, from which it considered itself exempt. In 1956 the Attorney General of Alabama brought an equity suit in the State Circuit Court, Montgomery County, to enjoin the Association from conducting further activities within, and to oust it from, the State."); *see also* Anita L. Allen, *Associational Privacy and the First Amendment:* NAACP v. Alabama, *Privacy and Data Protection*, 1 ALA. C.R. & C.L. L. REV. 1, 5 (2011) ("The NAACP's mission to remove racial and color discrimination from American life was at variance with the state's aim of maintaining an unequal caste system of racial segregation.").

28. *NAACP*, 357 U.S. at 452.

29. *Id.* at 453–54.

30. Brief for Petitioner at 25–30, NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449 (1958) (No. 91). Prior to appealing to the United States Supreme Court, the NAACP filed two petitions for certiorari with the Alabama Supreme Court, both of which were denied. *NAACP*, 357 U.S. at 454.

The Court began its analysis by recognizing that group association enhances the effective advocacy of public and private viewpoints and is therefore inseparable from the constitutional "liberties" against state action guaranteed by the Fourteenth Amendment.[31] Alabama need not take a "direct act" to restrict petitioner's freedom of association rights, the Court observed, because even unintentional abridgments of expressive rights must be constitutionally reasonable.[32]

"Inviolability of privacy in group association," Justice Harlan wrote, "may in many circumstances be indispensible to preservation of freedom of association, particularly where a group espouses dissident beliefs."[33] To identify the NAACP membership publicly would expose it to retaliation, which the Court felt would induce members to withdraw and dissuade others from joining "because of fear of exposure of their beliefs shown through their associations and of the consequences of this exposure."[34] That the repressive effect resulted from private community pressures and not state action did not influence the Court's consideration, because the initial state action was necessary for the private pressures to take hold.[35] The Court therefore held the privacy of the NAACP's membership lists from state scrutiny to be integrally related to the right of members to associate freely with others and as such found the lists to be immune from discovery under the Fourteenth Amendment.[36]

The doctrine of associational privacy has expanded significantly since *NAACP v. Alabama*. In *Bates v. City of Little Rock*, the Court upheld the NAACP's refusal to identify its members to city tax revenue officials.[37] In *Talley v. California*[38] and *McIntyre v. Ohio Elections Commission*,[39] the Court extended the *NAACP* protections to the right to anonymously distribute literature. The protection of anonymous leaflets, in turn, expanded to protect the right to anonymity of door-to-door advocates and solicitors.[40] *NAACP* has

---

31. *Id.* at 460.

32. *Id.* at 461; *see, e.g.*, Grosjean v. Am. Press Co., 297 U.S. 233, 250–51 (1936) (rejecting a pretextual tax with the plain purpose of penalizing a selected group of newspapers).

33. *NAACP*, 357 U.S. at 462.

34. "[O]n past occasions revelation of the identity of its rank-and-file members has exposed these members to economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility. Under these circumstances, we think it apparent that compelled disclosure of petitioner's Alabama membership is likely to affect adversely the ability of petitioner and its members to pursue their collective effort to foster beliefs which they admittedly have the right to advocate . . . ." *Id.* at 462–63.

35. *Id.* at 463.

36. *Id.* at 466.

37. Bates v. City of Little Rock, 361 U.S. 516, 523–26 (1960) (holding that the operation of an occupational license tax was insufficient justification for a city to require the NAACP to publicly disclose its membership roles).

38. Talley v. California, 362 U.S. 60, 63–66 (1960) (rejecting a municipal ordinance forbidding the distribution of leaflets unless they bear the name and address of the distributor as a facially void restriction that might "deter perfectly peaceful discussions of public matters of importance").

39. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995) (finding that a state prohibition on anonymous campaign literature was contrary to the First Amendment's protection of anonymity in expression where there was not a justifiable state interest).

40. *See* Buckley v. Am. Constitutional Law Found., Inc., 525 U.S. 182, 200 (1999) (finding a Colorado statute requiring that those circulating initiative petitions wear identification badges to discourage expressive

also served as the groundwork for many of the Court's penumbral privacy decisions such as *Griswold.*[41]

NAACP, however, only protects anonymity where the privacy interest in individual expression or group association outweighs the state's interests. In *Uphaus v. Wyman*,[42] the Court allowed New Hampshire to compel a communist-affiliated group to identify individuals staying at one of its camps. The Court distinguished the case from *NAACP* on the grounds that the camp was a public event (as opposed to a confidential membership list) and that the "investigation . . . of subversive[s]" is a good faith state aim.[43] Similarly, in *Church of the American Knights of the Ku Klux Klan v. Kerik*, the Second Circuit Court of Appeals refused to extend *NAACP*'s protections of anonymous speech to the Ku Klux Klan's right to wear masks, distinguishing the right to anonymous speech from the right to conceal one's appearance by costume during a public demonstration.[44]

Fundamentally, *NAACP* and its progeny stand for the proposition that anonymity in expressive speech and association is worthy of protection. Although states do have the ability to limit anonymous speech, such restrictions are subject to exacting scrutiny,[45] demonstrating the high value that the Court places on associational privacy rights.

B. Associational Privacy Considerations in the Technological Context

Little attention has been paid to the impact that our increasing reliance on technology may have on physical movements and associational privacy concerns.[46] This oversight partially results from the unprecedented role of technology in modern society. However, it primarily stems from the Court's failure to address issues of governmental surveillance in the associational

---

participation by requiring identification without sufficient cause); *see also* Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 168–69 (2002) (holding a municipal regulation requiring that door-to-door solicitors obtain a permit from the mayor to be an undue burden on expressive speech).

41. *See* Griswold v. Connecticut, 381 U.S. 479, 483 (1965) ("Disclosure of membership lists of a constitutionally valid association, we held, was invalid . . . . In other words, the First Amendment has a penumbra where privacy is protected from governmental intrusion."); *see also* Allen, *supra* note 27, at 11 ("Heirs of *Griswold* also owe a debt to *NAACP*'s vigorous defense of freedom from state interference").

42. Uphaus v. Wyman, 360 U.S. 72, 81 (1959).

43. *See id.* at 80–81 (describing the investigation as "undertaken in the interest of self-preservation" and noting that because "the camp was operating as a public one," it was legally obligated to maintain records of its guests).

44. Church of the Am. Knights of the Ku Klux Klan v. Kerik, 356 F.3d 197, 209 (2d Cir. 2004).

45. *See id.* at 208 (noting that the Court applies an exacting scrutiny standard—requiring narrow tailoring and an overriding state interest—when reviewing statutes threatening associational privacy rights).

46. *But see* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 113–114 (2010) (evaluating technology's impact on privacy and arguing that the traditional public-private dichotomy neglects technology-dependent circumstances where privacy protections are expected); DANIEL J. SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 164–205 (2011) (examining the privacy impact of technological evolution and arguing for preemptive lawmaking to ensure that the evolution of privacy law remains safely caught up with the adoption of new technologies); Anita L. Allen, *Driven Into Society: Philosophies of Surveillance Take to the Streets of New York*, 1 AMSTERDAM L. FORUM, 2009, at 35 (applying traditional philosophical approaches to New York's Lower Manhattan Security Initiative). Many scholars, however, have considered the direct applications of associational privacy to the Internet, especially in the context of anonymous speech.

privacy case law.

The associational privacy cases fundamentally target statutes or civil suits and not law enforcement investigations.[47] This focus is no doubt caused, in part, by public complacence regarding domestic surveillance prior to the release of the Church Reports.[48] The primary cause, though, is the inherent difficulty in challenging government surveillance. Private citizens do not have standing to challenge surveillance until the fruits of the surveillance are used against them.[49] Yet, an individual is unlikely to be aware they are under surveillance unless a criminal prosecution results.[50] Thus baseless surveillance, the kind most likely to chill speech, is also effectively unprotected against because it will not yield a criminal prosecution.

This oversight likely resulted from the limited means of surveillance available in 1958: short of physical intrusion, government agencies were limited to tapping phones or intercepting mail and therefore could only capture interactions between two parties. Moreover, individuals in the era of the telephone operator and shared connections considered telephone conversations to be much less private than they are today.[51] In the modern era, communications are both more frequent and more informative, providing government surveillance efforts with a much fuller picture of one's associational network. People have higher expectations of privacy in private communications, even though the transmission of phone calls and e-mails inherently requires entrusting them to third-party service providers.[52] It is therefore necessary to extend traditional associational privacy considerations to government surveillance activities because those activities are increasingly likely to have a chilling effect on First Amendment exercise.

Congress has already taken limited steps to protect associational privacy from government surveillance through the Privacy Act of 1974, which prohibits government agencies from maintaining records on individual exercise

---

47. *See supra* notes 27, 37–42 and accompanying text (offering examples of associational privacy cases).

48. The Church Reports were a series of fourteen reports prepared by the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities (the "Church Committee") examining the legality and morality of domestic and foreign intelligence activities. The Church Committee's investigations revealed massive domestic surveillance programs, including many that specifically targeted First Amendment activity. For examples of these trespasses, see *infra* notes 49–51 and accompanying text.

49. *See* Laird v. Tatum, 408 U.S. 1, 11 (1972) (finding that a party who knew "a governmental agency was engaged in certain activities . . . [and] armed with the fruits of those activities, the agency might in the future take some other and additional action detrimental to that individual" lacked standing).

50. Potential plaintiffs will likely remain unaware that they specifically are under surveillance until the fruits of the surveillance are used against them. The mere existence of a government surveillance program, without a specific action against the plaintiff, is insufficient to create a justiciable conflict. *See id.* at 10–11 (affirming the refusal to hear a case wherein class action plaintiffs complained of the chilling of their First Amendment rights via the mere existence, without more, of a governmental investigative and data-gathering activity allegedly broader than was necessary).

51. *See* Lee v. Florida, 392 U.S. 378, 381 (1968) ("A party-line user's privacy is obviously vulnerable.").

52. *See* Hien Timothy M. Nguyen, *Cloud Cover: Privacy Protections and the Stored Communications Act in the Age of Cloud Computing*, 86 NOTRE DAME L. REV. 2189, 2212 (2011) (reasoning that when an individual sends an email, he has the same expectation of privacy as exists in a document stored locally on a home computer).

of First Amendment activities.[53] However, the Privacy Act of 1974 only protects against the maintenance of retrospective records and is subject to significant gaps in protection.[54] It only applies to federal agencies, and few states have implemented similar omnibus privacy protections.[55] This leaves many state and local governments free to investigate and record individuals' First Amendment activities.

America's history demonstrates the risk that government surveillance poses when the government wrongly targets expressive associations. Dr. Martin Luther King, Jr. was the subject of physical and audio surveillance by the FBI, which culminated in an attempt to blackmail Dr. King into committing suicide.[56] The NSA, CIA, FBI, and Army intelligence services monitored the Vietnam era anti-war movement.[57] The CIA and FBI operated twelve distinct mail-opening programs between 1940 and 1973, targeting threatening groups like the Federation of American Scientists and the Quaker American Friends Service Committee, as well as authors, businesses, political candidates, and government officials.[58] More recently, the news media and civil rights organizations have revealed that the Department of Defense's Counterintelligence Field Activity Agency had again been accumulating and maintaining data about domestic advocacy groups, including, again, the American Friends Service Committee.[59] This history of surveillance demonstrates the very real risk of government monitoring that individuals face when engaged in First Amendment expression.

Exacerbating the chilling potential of this history of surveillance is the escalating publicity and audacity of the government's surveillance practices in the domestic and international spheres. Since the September 11 attacks, the

---

53. The 1974 Act provides that government agencies must "maintain no record[s] describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute . . . or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7) (2012).

54. The exception for "authorized law enforcement activities," for instance, allows fear-fueled "preventative policing" or pretextual criminal investigations to open the door to the monitoring of First Amendment activities. *See, e.g.*, Clarkson v. Internal Revenue Service, 678 F.2d 1368, 1375 (11th Cir. 1982) (reasoning that Section (e)(7) is violated if the agency collects "protected information, unconnected to any investigation of past, present, or anticipated violations of the statutes which it is authorized to enforce . . . ."); *see also* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1166 (2002) (noting that the Privacy Act "contains many exceptions and loopholes that have limited its effectiveness").

55. *See* Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 605 n.319 (1995) (listing the thirteen states with general fair information practices statutes applicable to the state government).

56. SELECT COMM. TO STUDY GOV'T OPERATIONS, INTELLIGENCE ACTIVITIES, S. REP. NO. 94-755, bk. 2, at 219–23 (1976).

57. *Id.* at 18, 77.

58. *Id.* at 168.

59. Lisa Myers et al., *Is the Pentagon Spying on Americans?*, NBC NEWS (Dec. 14, 2005, 6:16 PM), www.nbcnews.com/id/10454316/ns/nbcnightlynews-nbc_news_investigates/t/pentagon-spying-americans/#.UQyTq6U1pkg (reporting on leaked Department of Defense documents detailing the surveillance of anti-war activists); *see also No Real Threat: The Pentagon's Secret Database on Peaceful Protest*, AM. CIV. LIBERTIES UNION (Jan. 17, 2007), http://www.aclu.org/national-security/no-real-threat-pentagons-secret-database-peaceful-protest (describing documents obtained through FOIA requests that reveal widespread surveillance of anti-war activists, including the American Friends Service Committee).

government has increasingly turned to surveillance of electronic activity as a key tool in the fight against stateless enemies.[60] The attention paid to government surveillance, growing since 2001, has skyrocketed with Edward Snowden's gradual release of information about the NSA's most intrusive programs.[61] Although much of the attention Snowden has brought to bear is focused on the NSA and the FISA Court, the concerns it raises are just as applicable to the FBI and state and local police.

Recent cases show that associational privacy is no less important today than it was when *NAACP* was decided.[62] In *NAACP*, the Court sought to protect members of the NAACP from "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility" that would be brought about by the disclosure of their membership.[63] Similarly, Occupy Wall Street protestors have faced economic reprisal, loss of employment,[64] and the threat of physical coercion.[65] In light of the chilling effect that government investigations can impart on protected First Amendment association, greater safeguards are necessary.

III. FOURTH AMENDMENT PROTECTIONS IN THE DIGITAL SPHERE

A. The Framers' Fourth Amendment

The Fourth Amendment, like much of the Bill of Rights, originated as a

---

60. *See, e.g.*, Bill Mears, *Newly Declassified Documents Released on Post-9/11 Surveillance*, CNN U.S. (Dec. 21, 2013, 8:32 PM), http://www.cnn.com/2013/12/21/us/obama-national-security-documents/ ("The Obama administration has released more once-secret national security documents, this time detailing the origins of increased electronic surveillance to collect foreign intelligence in the months after the 9/11 attacks.").

61. *See, e.g.*, Ewen MacAskill & Gabriel Dance, *NSA Files: Decoded*, GUARDIAN (Nov. 1, 2013), http://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 ("[Edward Snowden] wanted to start a debate about mass surveillance. He succeeded beyond anything the journalists or Snowden himself ever imagined. His disclosures about the NSA resonated with Americans from day one. But they also exploded round [sic] the world.").

62. *See, e.g.*, Perry v. Schwarzenegger, 591 F.3d 1147, 1157–58 (9th Cir. 2010) (protecting the internal communications of the campaigns intervening as proponents of Proposition 8 from disclosure); Tree of Life Christian Schs. v. City of Upper Arlington, No. 2:11–cv–00009, 2012 WL 831918, at *4 (S.D. Ohio Mar. 12, 2012) (protecting the identity of a religious group's largest donor from discovery in a suit concerning land-use restrictions); Dunnet Bay Constr. Co. v. Hannig, No. 10–CV–3051, 2011 WL 5417123, at *7 (C.D. Ill. Nov. 9, 2011) (protecting the internal communications of a political campaign committee from disclosure).

63. NAACP v. Alabama *ex rel*. Patterson, 357 U.S. 449, 462 (1958).

64. *See, e.g.*, Jennifer Bjorhus, *U.S. Bank Temp Says Occupy Post Got Her Fired*, STAR TRIBUNE (Nov. 4, 2011, 8:13 PM), http://www.startribune.com/business/133277348.html (reporting on a bank employee who was fired for posting on the Occupy Minnesota Facebook page); Elizabeth Flock, *Occupy Wall Street Costs Two Journalists Their Jobs*, WASH. POST (Oct. 28, 2011, 4:37 PM), http://www.washingtonpost.com/blogs/blogpost/post/occupy-wall-street-costs-two-journalists-theirjobs/2011/10/28/gIQA4NN6PM_blog.html (detailing the firings of freelance journalist Caitlin Curran and freelance opera host Lisa Simeone following their participation in Occupy Wall Street protests).

65. *See, e.g.*, FBI SITUATIONAL INFO. REPORT 61 (Sept. 15, 2011), *available at* http://documentcloud.org/documents/549516/fbi-spy-files-on-the-occupy-movement-1.pdf (revealing FBI knowledge of planned sniper attacks on Occupy Wall Street in Houston); Seth Koenig, *Occupy Maine Adjusts, Beefs Up Security Watches After Chemical Bomb Attack*, BANGOR DAILY NEWS (Oct. 25, 2011, 2:15 PM), http://bangordailynews.com/2011/10/25/news/portland/occupy-maine-adjusts-beefs-up-security-watches-after-chemical-bomb-attack/ (reporting a drive-by chemical bomb attack on the Occupy Maine encampment in Portland).

response to the coercive practices of the Crown and the early colonial governments.[66] In the Colonies, revenue officers were issued writs of assistance, which empowered them, in their discretion, to search any locations at which they suspected smuggled goods could be found.[67] This power was often misused, and the records of that era are replete with instances of customs officials abusing their unconstrained authority to search for contraband.[68] Another common practice was the use of the general warrant to authorize broad searches and seizures in pursuit of those guilty of seditious libel. The Privy Council and Secretary of State often used the general warrant, and the seditious libel laws more broadly, to silence political opposition and punish those who gave "insurrectionary speeches" in Parliament.[69] These practices, however, were increasingly challenged in the years directly preceding the American Revolution, and many colonists rallied around John Wilkes's victory in challenging Lord Halifax's use of a general warrant to search Wilkes's house and those of forty-nine others suspected to have abetted in the publication of *North Briton, Number 45*.[70] Soon thereafter, Lord Camden attacked the use of general warrants in *Entick v. Carrington* in an opinion that many understood to outlaw general warrants, and suspicionless searches more generally, as an affront to English liberty.[71]

---

66. *See, e.g.*, Leonard W. Levy, *Origins of the Fourth Amendment*, 114 POL. SCI. Q. 79, 79 (1999) ("Before the American Revolution, the right to be secure against unreasonable searches and seizures had slight existence.").

67. Boyd v. United States, 116 U.S. 616, 625 (1886). For more on the writs of assistance, see generally Horace Gray, Jr., *Writs of Assistance*, *in* JOSIAH QUINCY, JR., REPORTS OF CASES ARGUED AND ADJUDGED IN THE SUPERIOR COURT OF JUDICATURE OF THE PROVINCE OF MASSACHUSETTS BAY BETWEEN 1761 AND 1772 395, 469–82 (Boston, Little, Brown & Co. 1865). James Otis argued that these writs were "then the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that was ever found in an English law book" because they placed "the liberty of every man in the hands of every petty officer." *Id.* (citing THOMAS M. COOLEY, A TREATISE ON THE CONSTITUTIONAL LIMITATIONS WHICH REST UPON THE LEGISLATIVE POWER OF THE STATES OF THE AMERICAN UNION 303 (Boston, Little, Brown & Co. 1868)).

68. James Otis provided several examples of these abuses, including one in which Mr. Ware, a customs officer, used the writ as a means of retaliation: [original spelling and grammar retained] "Justice Walley had called . . . Mr Ware before him by a constable to answer for a breach of Sabbath-day acts, or that of profane swearing. As soon as he had finished, Mr. Ware asked him if he had done. He replied, Yes. Well then, said Mr. Ware, I will shew you a little of my power. I Command you to permit me to search your house for uncustomed goods; and went on to search his house from the garret to the cellar; and then served the constable in the same manner." Gray, *supra* note 67, at 476.

69. ANDREW E. TASLITZ, RECONSTRUCTING THE FOURTH AMENDMENT: A HISTORY OF SEARCH AND SEIZURE, 1789–1868, at 18 (2006).

70. Wilkes was the anonymous author of *North Briton, Number 45*, which criticized a speech given in defense of a 1763 excise tax on cider that authorized extensive search powers. *Id.* at 20–21. In response to the pamphlet, Lord Halifax issued a general writ ordering four messengers "to make strict and diligent search for the authors, printers, and publishers of [the] seditious and treasonable paper . . . and them, or any of them, having found, to apprehend and seize, together with their papers." *Id.* After his seizure and imprisonment, Wilkes and many of other forty-nine individuals arrested and searched pursuant to the warrant filed suit for trespass, ultimately prevailing with substantial jury-awarded damages against Lord Halifax and Undersecretary of State Robert Wood, who had supervised the warrant's execution. *Id.* After these events "Wilkes became a popular idol, the 'personification of constitutional liberty to Englishmen on both sides of the Atlantic.' 'Wilkes and Liberty' became a patriot's slogan in America." *Id.*

71. Lord Camden clearly expressed his disgust with the practice of general warrants, writing that: "[i]f this point should be decided in favor of the Government, the secret cabinets and bureaus of every subject in this kingdom would be thrown open to the search and inspection of a messenger, whenever the secretary of state shall see fit to charge, or even to suspect, a person to be the author, printer, or publisher of a seditious

The Supreme Court, in *Boyd v. United States*, asserted that this history was in the minds of the Fourth Amendment's framers when they forbade unreasonable searches and seizures.[72] Based on its reading of *Entick*, the Court concluded that the ban on unreasonable searches and seizures was a protection not against the physical "breaking of [a man's] doors and the rummaging of his drawers," but the "invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offense . . . ."[73] The Court further went on to explain that compelling production of private books or papers in a criminal (or similarly situated) case forces the defendant to act as a witness against himself in violation of the Fifth Amendment and "is the equivalent of a search and seizure—and an unreasonable search and seizure—within the meaning of the Fourth Amendment."[74]

The next major shift in Fourth Amendment doctrine occurred in *Olmstead v. United States*, a Prohibition-era case challenging the constitutionality of wiretaps used against a band of rumrunners in the Pacific Northwest.[75] The defendants argued that the multi-month wiretap on their home and business telephones constituted a "search" in violation of the Fourth Amendment.[76] In that case, the Court defined the scope of the Fourth Amendment in terms of the framers' original understanding of the amendment as a protection of the sanctity of the home and the privacy of personal papers.[77] The Court therefore found that the language of the amendment could not "be expanded to include telephone wires reaching to the whole world from the defendant's house or office" because "[t]he intervening wires are not part of his house or office any more than are the highways along which they are stretched."[78] Thus, under *Olmstead*, a search and seizure required "a seizure of [a man's] papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."[79]

B. Katz *and the Reasonable Expectation Standard*

The Fourth Amendment standard set forth in *Olmstead* remained in force until 1967, when the Court reconsidered its treatment of electronic surveillance in *Katz v. United States*.[80] During Katz's trial for interstate gambling, the government tried to introduce recordings made through a listening device attached to the outside of the public telephone booth from which Katz had

---

libel." *Id.* Nonetheless, Camden's ultimate holding was limited to the conclusion that the Secretary of State, without legislative approval, lacked the authority to authorize such searches. *Id.*

72. Boyd v. United States, 116 U.S. 616, 626–27 (1886).
73. *Id.* at 630.
74. *Id.* at 635.
75. Olmstead v. United States, 277 U.S. 438 (1928).
76. *Id.* at 457.
77. *Id.* at 469.
78. *Id.* at 465.
79. *Id.* at 466.
80. Katz v. United States, 389 U.S. 347 (1967).

placed incriminating calls.[81] In addressing this question, the Court abandoned the traditional locus-based approach to the Fourth Amendment, observing, "the Fourth Amendment protects people, not places."[82] The Court, in light of "the vital role that the public telephone has come to play in private communications,"[83] concluded that the Fourth Amendment's protections extended to the telephone booth, just as they had previously been extended to the business office,[84] the taxi-cab,[85] and the apartment of a friend.[86] In his now-famous concurrence, Justice Harlan sought to define how the Fourth Amendment applied to the individual in light of the Court's declaration that the Fourth Amendment protected persons and not places.[87] Looking to the Court's prior Fourth Amendment decisions, he identified a twofold requirement that "(1) a person have exhibited an actual (subjective) expectation of privacy and (2) that the expectation be one that society is prepared to recognize as 'reasonable.'"[88]

The Court, in *Smith v. Maryland*, explicitly adopted Justice Harlan's "reasonable expectation" analysis as the mechanism to be used in determining whether a Fourth Amendment privacy interest was at stake.[89] In *Smith*, the government sought to admit call records obtained via a pen register[90] to prove that the defendant had placed harassing calls to the victim.[91] The Court found that no "search" under the Fourth Amendment had occurred because society would not recognize a reasonable expectation of privacy in dialed telephone numbers conveyed to third parties such as the phone company.[92]

Smith v. Maryland is representative of a robust string of cases holding that "a reasonable expectation of privacy" cannot exist when information or communication is voluntarily shared with non-recipient third parties such as telecommunication providers and banks.[93] Because Fourth Amendment privacy interests are personal and individual in nature, the collection of large amounts of transactional metadata has been held constitutional under *Smith* absent any iota of individual particularized suspicion.[94] Recently, however,

81. *Id.* at 348.
82. *Id.* at 351.
83. *Id.* at 352.
84. Silverthorne Lumber Co. v. United States, 251 U.S. 385, 392 (1920).
85. Rios v. United States, 364 U.S. 253, 261–62 (1960).
86. Jones v. United States, 362 U.S. 257, 267 (1960).
87. *Katz*, 389 U.S. at 360–62 (Harlan, J., concurring).
88. *Id.* at 361 (Harlan, J., concurring).
89. Smith v. Maryland, 442 U.S. 735, 740 (1979).
90. A pen register is a device attached to a telephone line that is used to identify the outgoing numbers dialed.
91. *Smith*, 442 U.S. at 742–43.
92. *Id.*
93. *See id.* (holding that phone numbers dialed, but not the content of the calls, falls outside the Fourth Amendment's scope); United States v. Miller, 425 U.S. 435, 442–43 (1976) (holding that the Fourth Amendment does not protect the contents of original checks and deposit slips when they are voluntarily conveyed to a bank).
94. Amended Memorandum Opinion at 9, In re Application of the Federal Bureau of Investigation for an Order requiring the Production of Tangible Things from [REDACTED], No. BR 13-109 (F.I.S.A. Ct. Aug. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf (holding that, per *Smith*, "[W]here one individual does not have a Fourth Amendment interest, grouping together a large

Judge Leon of the District Court of the District of Columbia has challenged this notion, arguing that the "almost Orwellian" nature of such metadata collection programs was inconceivable when *Smith* was decided and that *Smith* is inapplicable in cases of general and suspicionless metadata collection.[95]

More recent cases in the field of vehicular tracking indicate that a broader doctrinal shift in Fourth Amendment jurisprudence might be underway. In its 1983 opinion in *United States v. Knotts*, the Court held, based on *Katz* and *Smith*, that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[96] In that case, the government engaged in surveillance through an electronic beeper mounted in a five-gallon container of precursor, which was used in combination with visual surveillance to determine the location of a drug laboratory.[97] The Court highlighted that "[v]isual surveillance from public places along [the driver's] route or adjoining [the drug laboratory] would have sufficed" to reveal the same information obtained via the beeper and that the beeper therefore did not uniquely create a Fourth Amendment violation.[98] A year later in *United States v. Karo*, the Court clarified *Knotts*, holding that the installation of a beeper or transfer of an item equipped with a beeper did not constitute a Fourth Amendment violation, but that the use of the beeper in a private space not subject to visual surveillance did constitute a Fourth Amendment violation.[99] The Court also rejected the government's argument that it should be able to use beepers in private residences absent a warrant if there is reasonable suspicion of criminal activity, concluding that such an intrusion was contrary to the Fourth Amendment and the result of "a deprecation of the benefits and exaggeration of the difficulties associated with procurement of a warrant."[100] *Karo* and *Knotts* combined thus established a general rule allowing the warrantless electronic tracking of vehicles so long as

---

number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*.").

95. *See* Klayman v. Obama, No. 13-0851 (RJL), 2013 WL 6571596 (D.D.C. Dec. 16, 2013). *Klayman* was one of several constitutional challenges to the NSA's metadata collection program revealed in the Snowden leaks. Judge Leon concluded that "the question before [the court] is *not* the same question that the Supreme Court confronted in *Smith*," and instead styled the question at issue as when "present-day circumstances—the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply?" *Id.* at *18. Judge Leon concluded that in light of the duration of the surveillance, the relationship between the NSA and telecommunications companies, the scope, and the sheer quantity of metadata collected by modern general surveillance efforts, *Smith* was inapplicable to the case at hand. *Id.* at *19–22. *But see* American Civ. Liberties Union v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708, at *22 (S.D.N.Y. Dec. 27, 2013) (concluding, in the opposite, that *Smith* continues to govern in Fourth Amendment challenges to the NSA's metadata collection program). As of the time of this writing, it is unclear how these seemingly contradictory opinions will be reconciled.

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

97. *Id.* at 277–79.

98. *Id.* at 282.

99. United States v. Karo, 468 U.S. 705, 713–15 (1984). On the second point, the Court specifically noted that "[t]he monitoring of an electronic device such as a beeper is, of course, less intrusive than a full-scale search, but it does reveal a critical fact that the government is extremely interested in knowing and that it could not have otherwise obtained without a warrant." *Id.* at 715.

100. *Id.* at 717.

the surveillance does not intrude on private spaces protected by the Fourth Amendment.

This standard and the broader conceptions of Fourth Amendment privacy contained in *Smith* and *Katz* have been challenged by recent opinions in a line of cases involving the GPS tracking of automobiles. In *United States v. Maynard*, a D.C. Circuit case, the defendant raised a Fourth Amendment challenge to the admission of a month of GPS-tracking data obtained via a transponder affixed to his personal automobile.[101] The court, in trying to determine whether this month-long surveillance constituted a search, introduced what has come to be known as the "mosaic" theory of the Fourth Amendment. Looking to Supreme Court precedent, the court recognized that there was no right to privacy in a specific automotive trip. Rather than ending the examination with the question of whether the individual act (using GPS to track a car) was a search, the court instead proceeded to consider the collective sum of the different acts of surveillance accrued over time.[102] Looking to a number of Fourth Amendment precedents, the court found that "[i]n considering whether something is 'exposed' to the public" the question it should ask was "not what another person can physically and may lawfully do but rather what a reasonable person expects another might actually do."[103] Although an individual may not have a reasonable expectation of privacy in an individual trip over public roads, the court found, it was reasonable for the defendant to believe that a month of his driving activities was private.[104] The court therefore decided that, while tracking the car over the course of one day would not have been a constitutional violation, the month of sustained tracking did arise to the level of a Fourth Amendment violation.[105]

Maynard was appealed to the Supreme Court in *United States v. Jones*.[106] Justice Scalia, writing for the majority, reached the same outcome as the D.C. Circuit (excluding the GPS tracking data), but did so using different reasoning. Rather than looking to *Katz*, Justice Scalia looked to the "degree of privacy against government that existed when the Fourth Amendment was adopted" and applied a traditional Fourth Amendment property-right-based rationale.[107] The majority therefore found the Fourth Amendment violation to reside, not in the violation of informational privacy, but in the physical intrusion necessary to install the GPS tracker.[108] In fact, the majority never reached *Maynard*'s

101. United States v. Maynard, 615 F.3d 554, 555–58 (D.C. Cir. 2010).

102. *Id.* at 561–63.

103. *Id.* at 559.

104. Although each individual trip may have been exposed to the public, "the whole of one's movements over the course of one month is not *actually* exposed to the public because the likelihood anyone will observe all those movements is essentially nil." *Id.* at 558.

105. *Id.* at 561–65.

106. United States v. Jones, 132 S. Ct. 945 (2012).

107. *Id.* at 950. In his *Knotts* concurrence, Justice Brennan explained that *Katz* did not erode the principle that "when the Government *does* engage in physical intrusion of a constitutionally protected area in order to obtain information, that intrusion may constitute a violation of the Fourth Amendment." United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring).

108. *Jones*, 132 S. Ct. at 952.

determination that GPS tracking qualified as a search under *Katz*.[109] Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, concurred in the judgment but rejected the majority's application of early Fourth Amendment precedent as "unwise" and "strain[ing] the language of the Fourth Amendment."[110] Indeed, Justice Alito convincingly highlighted a number of challenges a property-based approach to Fourth Amendment law would face in the remote-tracking context.[111] Instead, and in the absence of legislative protections of privacy (which Justice Alito encouraged),[112] the concurring Justices sought to apply *Katz*, adopting the Circuit Court's reasoning that while "short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable[,]" longer-term GPS monitoring "in investigations of most offenses impinges on expectations of privacy."[113] The concurring Justices thus embraced, at least implicitly, the mosaic theory. Justice Sotomayor, who concurred in support of the majority's finding of an "irreducible constitutional minimum," also expressed her support for Justice Alito's conclusion that longer-term GPS surveillance impinges expectations of privacy, creating the possibility that five Justices are ready to embrace the Circuit Court's "mosaic" theory.[114]

C. Opposition to the Katz *Standard and Current Fourth Amendment Conceptions*

Within the privacy field, the *Katz* standard and the sufficiency of Fourth Amendment protections more generally have come under increasing attack. Several noted scholars have challenged the notion that the Fourth Amendment is the outer limit of constitutional privacy protections against searches and seizures, arguing instead that the First Amendment supplies independent procedural protections or supplemental protections to be considered within the application of the Fourth Amendment.[115] The Fourth Amendment jurisprudence is also subject to criticism for its perpetual failure to keep up with the evolution of modern technology and societal expectations of privacy.[116] Daniel Solove once memorably noted that the privacy-minded

---

109. *See* Orin Kerr, *My Instincts Were Wrong—At Least I Now Think They Were—On* Maynard, VOLOKH CONSPIRACY (Dec. 3, 2013, 8:28 PM), http://www.volokh.com/2013/12/03/instincts-wrong-least-now-think-maynard/ (arguing that *Jones* did not resolve *Maynard*'s question of whether GPS tracking is a search under *Katz*).

110. *Jones*, 132 S. Ct. at 958 (Alito, J., concurring).

111. *See id.* at 961–62 (highlighting four primary problems, other than incongruity with existing precedent, that the majority opinion engendered).

112. *Id.* at 964. Justice Alito emphasized that "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id.*

113. *Id.*

114. *See* Orin Kerr, *What's the Status of the Mosaic Theory After* Jones*?*, VOLOKH CONSPIRACY (Jan. 23, 2012, 1:59 PM), http://www.volokh.com/2012/01/23/whats-the-status-of-the-mosaic-theory-after-jones/ (analyzing the impact of *Jones* on the mosaic theory and concluding that five Justices seem ready to embrace it in at least a limited context).

115. *See infra* Part IV.C.

116. *See* Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 105 COLUM. L. REV. 279, 292–306 (2005) (highlighting how existing Fourth Amendment jurisprudence based on physical-world rules is unable to effectively address the collection of digital evidence).

might as well "go live as a hermit in a cabin on a mountaintop" because that was the only place where the Fourth Amendment would still be able to protect individual privacy.[117]

The *Katz* reasonable expectation of privacy has itself been criticized for being under-protective,[118] outdated,[119] misguided,[120] misapplied,[121] and generally insufficient. Scholars have set forth a number of alternative standards, many of which seek to shift the focus from the circumstances of a search to the outcome of the search. Daniel Solove, for instance, suggests looking at the "problems" created by the search.[122] The existing proposals to incorporate First Amendment concepts into Fourth Amendment jurisprudence are all similarly focused on outcome-based impacts and not the circumstances of the search.[123] The mosaic theory also adopts an outcome-based perspective, and both *Maynard*[124] and *Jones*[125] provide clear warning that the *Katz* standard is no longer the exclusive definition of Fourth Amendment rights.

D. The Misplaced Trust Doctrine

A thread of cases parallel to *Katz* and *Smith* addresses what happens when a communication's contents are revealed by one of its participants. In *Hoffa v. United States*, the Court established that the Fourth Amendment provides no protection against a wrongdoer's misplaced belief that a person to whom he confides his wrongdoing will not reveal it, establishing what is now known as the "misplaced trust doctrine."[126] *United States v. White* further extended the

---

117. SOLOVE, *supra* note 46, at 110.

118. *See* Aya Gruber, *Garbage Pails and Puppy Dog Tails: Is That What* Katz *Is Made of?*, 41 U.C. DAVIS L. REV. 781, 790–91 (2008) (arguing that the *Katz* test's fluid, flexible nature and reliance on individual precautionary behavior render the test less protective than a literal reading of the Fourth Amendment and cautioning that, unless addressed, these flaws might "swallow" the entirety of Fourth Amendment privacy protection).

119. *See* Daniel J. Polatsek, Note, *Thermal Imaging and the Fourth Amendment: Pushing the* Katz *Test Towards Terminal Velocity*, 13 J. MARSHALL J. COMPUTER & INFO. L. 453, 478 (1995) ("It is apparent the *Katz* test is clearly outdated in terms of its usefulness when presented with the new challenges of today's technology.").

120. *See* ERIC NEISSER, *Do We Expect Our Garbage to Be Inspected by Police*, in RECAPTURING THE SPIRIT: ESSAYS ON THE BILL OF RIGHTS AT 200, at 93 (1991) (arguing that the Fourth Amendment standards the government is held to are meant to be greater than the protections against intrusions by private citizens); SOLOVE, *supra* note 46, at 114 (arguing that the Court's interpretation of the *Katz* standard as requiring "total secrecy" to create a reasonable expectation of privacy has undermined the Fourth Amendment's protections, and urging a shift to a "problem"-based privacy schema); Orin S. Kerr, *The Curious History of Fourth Amendment Searches*, 2013 SUP. CT. REV. 67, 86–90 (2012) (noting that *Katz* adopted the mistaken conception that the standard it was overruling was based on "trespass").

121. *See* Christopher Slobogin & Joseph E. Schumacher, *Reasonable Expectations of Privacy and Autonomy in Fourth Amendment Cases: An Empirical Look at "Understandings Recognized and Permitted by Society,"* 42 DUKE L.J. 727, 740–42 (1993) (finding substantial dissonance between the Court's conclusions and societal conclusions (as indicated by empirical data) of when a "reasonable expectation of privacy" exists).

122. Daniel J. Solove, *Why Privacy Matters Even If You Have 'Nothing to Hide,'* CHRON. HIGHER EDUC. (May 15, 2011), https://chronicle.com/article/Why-Privacy-Matters-Even-if/127461/.

123. *See infra* the discussion of proposals by Professor Solove and Professor Strandburg contained in Part IV.C.

124. United States v. Maynard, 615 F.3d 554 (D.C. Cir. 2010).

125. United States v. Jones, 132 S. Ct. 945 (2012).

126. Hoffa v. United States, 385 U.S. 293, 301–03 (1966). In *Hoffa*, the defendant raised a Fourth Amendment challenge to the government's use of a paid informant who reported on conversations had in the

misplaced trust doctrine, holding that it also applies to the use of concealed radio transmitters.[127] Both of these opinions relied heavily on the distinction between trust in the privacy of a physical space, which the Fourth Amendment protects, and trust in an individual, which the Fourth Amendment does not cover. Thus, groups holding meetings open to the public are unprotected from surveillance or recording by those in attendance under the Fourth Amendment.[128] Likewise, the Fourth Amendment does not protect against officers using deceit to secure consent to enter, so long as the deception pertains to a desire to engage or participate in an illegal activity.[129] The Court in *Lewis v. United States* wrote:

> [W]hen, as here, the home is converted into a commercial center to which outsiders are invited for purposes of transacting unlawful business . . . [a] government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises for the very purposes contemplated by the occupant.[130]

The *Lewis* Court, however, made a point of distinguishing the holding of *Gouled v. United States*, which held that the secretive searching of an office by a business acquaintance of the defendant working with federal officers constituted a Fourth Amendment violation, despite the fact that "the initial intrusion was occasioned by a fraudulently obtained invitation rather than by force or stealth."[131] This outcome falls in line with empirical evidence showing that the public considers undercover activity by officers posing in "trusted" roles such as a chauffeur or secretary to be highly invasive.[132] Officers also are not permitted to use deception about the existence of a warrant,[133] the purpose of their search,[134] or the object of their search[135] to

---

defendant's hotel room. The Court held that, while the Fourth Amendment would protect the privacy of the defendant's hotel room against electronic surveillance or physical intrusion, it did not protect against guests invited into a private place due to misplaced confidence. *Id*.

127. United States v. White, 401 U.S. 745, 754 (1971).

128. *See, e.g.*, United States v. Aguilar, 883 F.2d 662, 703 (9th Cir. 1989) (holding that surveillance of churches was not in violation of the Fourth Amendment because churchgoers lacked a reasonable expectation of privacy).

129. Lewis v. United States, 385 U.S. 206, 206–07 (1966).

130. *Id.* at 211.

131. *Id.* at 209–10 (citing Gouled v. United States, 255 U.S. 298 (1921)).

132. Slobogin & Schumacher, *supra* note 121, at 740.

133. *See* Bumper v. North Carolina, 391 U.S. 543, 548 (1968) (holding that the defendant's grandmother had not consented to a search of her house when that consent was based on a police officer's misrepresentation that he had a search warrant); Hadley v. Williams, 368 F.3d 747, 748–49 (7th Cir. 2004) (concluding that a homeowner did not consent to the arrest of her son within the house when the consent was based on officer's guarantee that they had an arrest warrant).

134. *See* United States v. Bosse, 898 F.2d 113, 114 (9th Cir. 1990) (holding that the defendant's consent for state officers to inspect his property in relation to a pending application for a state license did not extend to an undisclosed ATF agent accompanying the state officers); United States v. Tweel, 550 F.2d 297, 300 (5th Cir. 1977) (holding that consent for the copying of financial records did not exist when the auditing IRS agent misled the defendant about the criminal nature of the investigation); United States v. Phillips, 497 F.2d 1131, 1133 (9th Cir. 1974) (holding that consent did not exist when narcotics officers had local police obtain consent on the pretense of investigating a burglary when the real purpose was to seize the defendant and secure the premises of his apartment).

135. *See* United States v. Dichiarinte, 445 F.2d 126, 128–29 (7th Cir. 1971) (holding that agents are limited to the scope of consent given by a defendant and cannot search for or seize items outside the scope of the consent).

generate consent for a search or seizure.

E. Statutory Standards

A robust body of statutory law providing additional privacy protections has historically supplemented the Supreme Court's Fourth Amendment jurisprudence and has been encouraged by Supreme Court Justices in numerous instances where technological evolution outpaces constitutional protections.[136] The first such statute, Section 605 of the Federal Communications Act of 1934, emerged as a legislative response to *Olmstead*'s holding that a telephone tap, absent physical trespass, was not a Fourth Amendment violation.[137] Congress made a second attempt at statutorily regulating surveillance in Title III of the Omnibus Crime Control and Safe Streets Act of 1968, motivated by the need to supplement the limited guidance the Court's Fourth Amendment jurisprudence provided to law enforcement officers.[138] Title III, which preempted weaker state laws, regulated both surveillance of face-to-face communications and surveillance of calls placed over the public telephone network.[139] In 1978, Title III was joined by the Foreign Intelligence Surveillance Act (FISA), which specifically addresses the demands of national security and foreign espionage and establishes a top-secret approval process for foreign surveillance via a specially constituted court comprised of federal judges.[140]

The culmination of these supplemental privacy-protecting statutes was the Electronic Communications Privacy Act (ECPA), passed in 1986 to regulate surveillance and seizure of communications in newly evolving digital streams of communication and commerce. The ECPA was a direct response to the limited scope of Title III, which the development of the Internet and network technology had rendered insufficient.[141] ECPA, like its predecessors, exists

136. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (urging that the best solution for privacy concerns created by dramatic technological change may be legislative in nature); Olmstead v. United States, 277 U.S. 438, 465–66 (1928) (raising the possibility that Congress can use the laws of evidence to prevent the use of surveillance forms and that the Court should not attempt to do the same by expanding the meaning of the Fourth Amendment); *see also* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805 (2004) (arguing that "statutory rules rather than constitutional rules should provide the primary source of privacy protections regulating law-enforcement use of rapidly developing technologies").

137. Section 605 provided that "no person not being authorized by the sender shall intercept any . . . communication and divulge or publish the [details or substance] of such intercepted communication to any person." Federal Communications Act of 1934, 47 U.S.C. § 605(a) (2012). *See also* ANITA L. ALLEN, PRIVACY LAW AND SOCIETY 969 (2d ed. 2011) (describing how Section 605 "did not have much muscle" due to its failure to preempt weaker state laws).

138. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197.

139. *Id.* § 801, 82 Stat. at 211–25.

140. 50 U.S.C. §§ 1801–85c (2012).

141. Senator Patrick Leahy, during a hearing on the ECPA before the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice, explained that the ECPA was needed because "[o]ur primary wiretap law, title III of the Omnibus Crime Control and Safe Streets Act of 1968, fails to cover the unauthorized acquisition of data transmissions. That includes everything from inter-bank orders to private electronic mail hookups—some of the fastest growing areas of communications today." *Electronic Communications Privacy Act: Hearing on H.R. 3378 Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary*, 99th Cong. 3 (1986) (statement of Sen. Patrick J. Leahy).

both to provide clear guidance to police officers on how to comply with the Fourth Amendment (because, under *Katz*, the existence of "privacy" might not be obvious) and to create protections for information otherwise unprotected by the Fourth Amendment (such as transactional data).[142]

The ECPA consisted of three separate and specifically focused statutes: the Wiretap Act, which governs the real-time acquisition of content data from a service provider;[143] the Pen Register Statute, which governs the real-time acquisition of non-content transactional data from a service provider;[144] and the Stored Communications Act, which governs the collection of retrospective content and non-content data from a service provider.[145]

Under the Wiretap Act, government entities can actively intercept oral, wire, and electronic communications, so long as the intercept occurs contemporaneously with transmission and is secured under a "super warrant."[146] Due to the high procedural requirements to obtain a super warrant, wiretaps are rarely used, especially in the computer context.[147] Although electronic wiretaps are less common than are telephone wiretaps, they are also less protected. Illegally obtained wiretap evidence used in a criminal trial is subject to a suppression remedy, but only if the wiretap intercepts voice communications.[148] Thus, victims of illegal electronic wiretaps are left with only civil remedies.

Another mechanism through which the government can obtain prospective information is the Pen Register Statute, which governs the use of pen registers and trap and trace devices to gather transactional information.[149] To obtain legal authority to use a pen register or trap and trace device, a

---

Of particular concern to Sen. Leahy was the Supreme Court's interpretation of Title III as requiring that a communication be capable of being overheard in order to engender privacy protection. *Id.* at 4.

142. *Id.* at 3.

143. 18 U.S.C. §§ 2510–22 (2012).

144. *Id.* §§ 3121–27.

145. *Id.* §§ 2701–11. These statutes are often collectively referred to as the Electronic Communications Privacy Act (ECPA), after the 1986 law of the same name that amended the Wiretap Act and established the Stored Communications Act and Pen Register Statute. Pub. L. No. 99-508 (1986). *See* ORIN S. KERR, COMPUTER CRIME LAW 458 n.2 (2d ed. 2009) (noting the interchangeable use of the individual names and ECPA).

146. A Title III "super warrant" is quite burdensome to obtain. For electronic communications, the order must be authorized by the Justice Department and signed by a judge. To obtain a Title III warrant, the application for the order must show probable cause to believe the interception will reveal evidence of a federal felony, and establish that (1) "normal investigative procedures have been tried and failed, or reasonably appear to be unlikely to succeed or to be too dangerous" and (2) "the surveillance will be conducted in a way that minimizes the interception of communications that do not provide evidence of a crime." U.S. DEP'T OF JUSTICE, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 168 (2009), *available at* www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf.

147. *See* ADMIN. OFFICE OF THE U.S. COURTS, APPLICATIONS FOR ORDERS AUTHORIZING OR APPROVING THE INTERCEPTION OF WIRE, ORAL, OR ELECTRONIC COMMUNICATIONS 7–8 (2012), *available at* www.uscourts.gov/uscourts/Statistics/WiretapReports/2011/2011WireTap.pdf (reporting that in 2011 a total of 2,732 wiretaps were authorized, ninety-six percent of which were telephone wiretaps).

148. *See* 18 U.S.C. § 2515 (2012) ("Whenever any wire or oral communication has been intercepted, no part of the contents . . . may be received in evidence . . . if the disclosure of that information would be in violation of this chapter."); *see also* KERR, *supra* note 145, at 460 (arguing that the limited statutory suppression remedy, original to the ECPA, was rational at the time of its creation since the computer communications in use at the time implicated lesser privacy concerns than voice communications).

149. 18 U.S.C. §§ 3121–27 (2012).

government attorney must apply for a court order and certify that "the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency."[150] The court, in turn, can only consider the completeness of the certification submitted and not the certification's compliance with the underlying standard when granting the order.[151] Unlike a wiretap application, a pen register applicant does not need to show that minimization procedures are in place or that other investigative techniques would not suffice.[152] Furthermore, while an application to extend a wiretap must either set forth the results thus far obtained from the interception or justify the failure to obtain such results, the extension of a pen register only requires the re-filing of the original identification and certification.[153]

The Stored Communications Act (SCA) governs retroactive investigative access to transactional and content data.[154] The statute regulates the relationship between service providers and the government by restricting the government's ability to compel providers to disclose client information and limiting service providers' ability to disclose customer information voluntarily to the government.[155] The SCA applies to two categories of digital service provider: Electronic Communication Service (ECS) providers and Remote Computing Service (RCS) providers. Electronic Communication Services provide their users with the ability to send or receive electronic communications, such as e-mails or other inter-device communications.[156] Under 18 U.S.C. § 2703(a), the government may require an ECS provider to disclose the contents of a communication retained in "electronic storage" in the course of its transmission.[157] Remote Computing Services provide their users with remote storage or processing systems.[158] Although RCS was initially intended to describe the now-dated practice of terminal computing, it currently serves as an apt description of cloud-computing solutions. RCS providers may only disclose communications that they hold or maintain on behalf of their customers solely for the purpose of providing storage or computer

150. *Id.* § 3122(b)(2).

151. S. Rep. No. 99−541, at 47 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3601 ("To issue an order, the court must first be satisfied that the information sought is relevant to an ongoing criminal investigation. This provision does not envision an independent judicial review of whether the application meets the relevance standard, rather the court needs only to review the completeness of the certification submitted.").

152. KERR, *supra* note 145, at 502.

153. *Id.* (contrasting the requirements for a wiretap extension in 18 U.S.C. § 2518(f) and the requirements for a pen register extension in 18 U.S.C. § 3123(c)(2)).

154. *See generally* 18 U.S.C. §§ 2701−12 (2012).

155. *See id.* §§ 2702–03 (governing voluntary disclosure and compelled disclosure).

156. *See id.* § 2510(15) (describing ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications"); *see also* KERR, *supra* note 145, at 512 (describing how the early use of computer networks to communicate prompted privacy concerns because providers commonly maintained stored copies of transmissions).

157. *See id.* § 2510(17) (noting that a service provider may retain communications in "electronic storage" incidentally to transmission, such as data packets saved at an intermediate relay, or for backup protection purposes).

158. *See id.* § 2711(2) (defining RCS as "the provision to the public of computer storage or processing services by means of an electronic communications system"); *see also* KERR, *supra* note 145, at 512 (describing the now-outdated role RCS played in the era before spreadsheet programs and the privacy concerns that resulted from third-party providers' data retention policies).

processing.[159]

Although the definitions of RCS and ECS currently in force were sensible at the time of passage, their application becomes confusing in the modern Internet, which is problematic because RCS and ECS communications have different access standards. E-mails, for instance, were clearly ECS communications at the time of passage, because the e-mail technology of 1986 downloaded the e-mail onto the user's computer before accessing it. But nowadays, opened e-mail, unless deleted, remains on the provider's servers. Thus, Gmail functions as both an ECS provider (as to the message in transit) and an RCS provider (as to the opened message stored on its server).[160] Popular cloud-storage provider Dropbox poses a more complicated example. To the extent that Dropbox is used for file storage, it functions as an RCS, but it also allows the sharing of files with third parties, which might render it an ECS as well.

Different standards apply to the acquisition of both ECS and RCS data. For instance, a search warrant is required to compel a provider of ECS to disclose the contents of communications that have been in "temporary electronic storage" for 180 days or less.[161] Conversely, ECS communications that have been in storage for over 180 days, and RCS communications, can be obtained by three means: (1) a standard search warrant; (2) a subpoena accompanied by notice; or (3) a § 2703(d) court order accompanied by notice.[162] Similarly, non-content transactional data is obtainable using a § 2703(d) court order or a search warrant.[163] Basic subscriber information, however (such as name, address, connection records, type and duration of service, telephone number or network address, and payment means) can be obtained with only a subpoena.[164]

Collectively, the Electronic Communications Privacy Act provides some level of protection against the compelled disclosure of data by third-party service providers, going beyond the limits of Fourth Amendment jurisprudence. However, that protection, perhaps appropriate given the state of technology in 1986, is now poorly matched to societal expectations of privacy and the breadth of technology usage.

While the ECPA governs law enforcement access to domestic electronic content for purposes of criminal prosecution, the Foreign Intelligence Surveillance Act (FISA) governs domestic and foreign surveillance against the agents of foreign powers.[165] While ECPA applications are based on probable

159. 18 U.S.C. § 2703(b)(2) (2012).

160. KERR, *supra* note 145 at 513; *cf.* Theofel v. Farey-Jones, 359 F.3d 1066, 1076 (9th Cir. 2004) (deviating from the traditional understanding of ECS and RCS and proposing that all e-mails held by a server are protected under the ECS rules until "the underlying message has expired in the normal course").

161. 18 U.S.C. § 2703(a) (2012).

162. *Id.* § 2703(d) (2012); *see also id.* § 2705 (allowing delayed notice where notice might cause an adverse result such as physical injury, flight from prosecution, destruction of evidence, or witness intimidation).

163. 18 U.S.C. § 2703(c)(1) (2012).

164. *Id.* § 2703(c)(2).

165. 50 U.S.C. § 1801 (2012).

cause to believe that the target of surveillance has committed a crime, FISA searches are based on probable cause that the target of the surveillance application is a foreign power or the agent of a foreign power.[166] Applications for surveillance or communications contents under FISA are processed through the Department of Justice, and approved by a specially constituted FISA Court, while stored content may be acquired without judicial oversight through a variant of the administrative subpoena known as a National Security Letter.[167]

Domestic and foreign surveillance were originally intended to exist as wholly separate spheres. Prior to September 11, FISA conditioned the issuance of national security warrants on the absence of intent to collect evidence for possible criminal prosecution because such intent would indicate that the warrant was being used for domestic criminal enforcement purposes as opposed to national security purposes.[168] The Patriot Act, however, significantly relaxed this standard to require only that a "significant purpose" of the surveillance be the acquisition of foreign intelligence and to allow for broader collaboration (and thus information sharing) with federal law enforcement officers.[169] The separation between domestic and foreign surveillance has also been eroded by executive orders authorizing the interception of international communications by United States citizens without the requisite legal procedure.[170] Although FISA exists as a parallel to ECPA, FISA-obtained materials are admissible in domestic criminal prosecutions, subject only to challenges based on the legality of the acquisition, challenges often decided through in camera, ex parte hearings.[171]

Prior to 2013, former NSA officials reported that the NSA was eavesdropping on domestic as well as international phone calls and e-mails and that at the program's outset it intercepted 320 million calls a day.[172] The Edward Snowden leaks dramatically confirmed the substance of these reports, revealing massive surveillance efforts targeting domestic communications

166. KERR, *supra* note 145, at 671.

167. 50 U.S.C. §§ 1804−05 (2012). Note, however, that surveillance of communications between two foreign parties can occur based solely on the authorization of the Attorney General. *Id.* § 1802.

168. *See* 50 U.S.C. § 1804(a)(6)(B) (2012) (detailing the current "purpose" standard); *id.* § 1806(k)(1) (allowing consultation with federal officers); *see also* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. 107–56, 115 Stat. 272 (2001) (amending §1804(a)(7)(B) and creating § 1806(k)(1)).

169. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. 107–56, 115 Stat. 272 (2001).

170. *See* Hon. Alberto R. Gonzales, Attorney Gen. of the U. S., Dep't of Justice, Prepared Statement (Feb. 6, 2006), *available at* http://www.justice.gov/archive/ag/speeches/2006/ag_speech_060206.html (arguing for the legality of the "terrorist surveillance program"); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (revealing the previously undisclosed NSA warrantless eavesdropping program authorized by executive order).

171. 50 U.S.C. § 1806 (2012).

172. *See* James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/all/1 (recounting the allegations of William Binney, a former NSA crypto-mathematician and cofounder of the Signals Intelligence Automation Research Center); *see also* Jane Mayer, *The Secret Sharer: Is Thomas Drake an Enemy of the State?*, NEW YORKER, May 23, 2011, at 46 (providing first hand and anecdotal evidence to indicate the existence of domestic surveillance programs on a massive scale).

being carried out under the FISA statute.[173] While the prior "rumors" of foreign surveillance left the FISA foreign surveillance–domestic surveillance distinction intact, the Snowden revelations have shown disconcerting blurring of the foreign-domestic dichotomy. The loss of this distinction can bring the full chilling force of foreign surveillance efforts to bear on situations where domestic surveillance would be minimally justified. Although FISA and foreign intelligence gathering fall outside the scope of this Article, their extension into domestic surveillance activities has a clear chilling effect on speech, and as awareness of government surveillance increases, the impact of that chilling effect on domestic surveillance governed by ECPA will undoubtedly increase as well.

On the whole, the existing Fourth Amendment framework provides insufficient protections for First Amendment activities in light of the increasingly digital world and the correspondingly increased avenues available to the government by which to conduct surveillance. The statutory protections that were designed to be applicable are wholly outdated and no longer serve to provide the privacy protection and the clear guidance to law enforcement officers that they once did. Experience demonstrates that nothing short of reimagining the *Katz* standard to reflect modern notions of privacy will extend sufficient Fourth Amendment protections to adequately guard First Amendment activities protected, in theory, by the associational privacy doctrine.

IV. GOVERNMENT MONITORING OF THE INTERNET AND TECHNOLOGY

The government has a plethora of available avenues through which to monitor Internet activity.[174] These methods can be divided into three basic categories, according to the degree of separation from the content-generating user. Part III.A will examine recipient level surveillance, wherein investigators directly access publicly available online information. Part III.B will examine transmitter level surveillance, wherein a third party service provider grants the government access to information about a user's stored data or network activity. Finally, Part III.C will examine reconstructive surveillance, wherein algorithms are used to aggregate and extract information from data already in the government's possession.

---

173. *See* Secondary Order at 2, *In re* Application of the Federal Bureau of Investigation (FISA Ct. Apr. 25, 2013) (No. BR 13-80), *available at* http://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order (ordering Verizon Wireless to release three months of call detail records or "'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls."); *see also* [Redacted] PRISM Collection Manager, S35333, PRISM/US-984XN Overview (Apr. 2013), http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (revealing the details of PRISM, a program through which the NSA has direct access to the servers of most major online service providers).

174. Some of these avenues consist of statutorily created "backdoors" into what would otherwise be secure communication systems that exist pursuant to the Communications Assistance for Law Enforcement Act. *See infra* note 228 and accompanying text.

A. Recipient Level Surveillance

Recipient level surveillance is the most common and most harmless type of electronic surveillance that the government can use on private citizens. Recipient level surveillance includes accessing public websites and public communications on Facebook, Twitter, and other social networks.[175] It also encompasses situations where investigators use deceit to "go undercover" in social networks, forums, or e-mail lists and gain access to otherwise restricted resources that are "voluntarily" shared with them but are not publicly accessible.

When police access public Internet content, the current conception of the Fourth Amendment poses no bar to the subsequent use of that data. However, the use of false identity and deception to gain access to information willingly shared but not publicly available raises substantial ethical objections. Such use creates a significant invasion of individual privacy, and as a policy matter, it encourages excessive use of surveillance. Such deception-based access can chill group communications by creating a fear of surveillance within semi-private contexts.

Monitoring of public Internet content has not always been unrestricted.[176] Prior to 2001, the guidelines for FBI surveillance practices required "facts or circumstances [that] reasonably indicate that a federal crime has been, is being, or will be committed" before an agent could "mine the internet for information."[177] Following September 11, the Attorney General relaxed that standard to allow the FBI to collect publicly available information, to obtain publicly available information from third-party collection and analysis entities, and to "carry out general topical research, including conducting online searches and accessing online sites and forums."[178]

With the relaxation of investigative Internet use guidelines and increases in general Internet usage, it is unsurprising that the Internet and social media have become an integral component of law enforcement investigative and preventative policing procedures. According to a recent survey of law enforcement personnel, roughly four out of five law enforcement officers use

---

175. Such straightforward Internet monitoring is facially similar to the use of surveillance cameras to record or monitor expressive activities. *See generally* Christopher Slobogin, *Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 252–67 (2003) (highlighting the constitutional harms of public camera surveillance). However, surveillance cameras can capture only public expressive activities, while online monitoring can intrude into discussions of logistics and philosophy. When an online conversation occurs in a limited-access venue (behind password protection, for instance), recording it is akin to installing a surveillance camera within the union hall or the leader's hotel room.

176. This observation applies only to the present act of monitoring. The subsequent recording of publicly available Internet information relating to First Amendment exercise in "agency records" is regulated by the Privacy Act of 1974. *See supra* notes 53−54 and accompanying text.

177. *See* Solove, *supra* note 54, at 1096 (quoting DICK THORNBURGH, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND DOMESTIC SECURITY/ TERRORISM INVESTIGATIONS § II.C.1 (1989)).

178. JOHN ASHCROFT, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES ON GENERAL CRIMES, RACKETEERING ENTERPRISE AND TERRORISM ENTERPRISE INVESTIGATIONS 21−22 (2002); *see also* MICHAEL MUKASEY, DEP'T OF JUSTICE, THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 20 (2008) (superseding the 2002 guidelines but leaving the endorsed methods essentially unchanged).

social media in an investigative capacity, and forty-eight percent do so on at least a weekly basis.[179] Even police departments in smaller cities have begun assigning detectives to monitor social media sites.[180] Criminals' online presence can provide valuable evidence to individual investigations, and in some cases, can lead to the indictment of entire gangs.[181]

Social media monitoring has also provided preemptive warnings of illegal activity, allowing police to prevent crimes before they begin or to coordinate surveillance to catch the criminals in the act.[182] This preventative use is surprisingly common, with forty-one percent of surveyed law enforcement officers reporting that they use social media to monitor for potential criminal activity.[183]

The use of recipient level surveillance can nonetheless have disconcerting implications for First Amendment rights. During the eviction of the Occupy Miami encampment in January 2012, independent journalist and free-speech activist Carlos Miller was the lone journalist arrested.[184] Miller had made a public Facebook post announcing that he would be documenting the Occupy eviction.[185] The Miami-Dade Police Department Homeland Security Bureau, the police department's anti-terrorism wing, noticed the post on Miller's Facebook.[186] The Facebook post was subsequently forwarded to the department's public information officers, along with a photo of Miller and a notation that he had been arrested previously while photographing law enforcement officers.[187] Although it is disputed what factors led to the arrest,

---

179. LEXISNEXIS, LAW ENFORCEMENT PERSONNEL USE OF SOCIAL MEDIA IN INVESTIGATIONS: SUMMARY OF FINDINGS 5, 10 (2012), *available at* http://www.lexisnexis.com/government/investigations (surveying 1,221 law enforcement professionals in June 2012, on their social media usage and experience).

180. *See, e.g.*, Julie Masis, *Is This Lawman Your Facebook Friend?*, BOSTON GLOBE, Jan. 11, 2009, at 1 (describing how "Woburn[, Massachusetts] employs a detective whose responsibility is to monitor Facebook and Myspace.").

181. *See* Joseph Goldstein, *43 in Two Warring Gangs Are Indicted in Brooklyn*, N.Y. TIMES, Jan. 20, 2012, at A22 (reporting the indictment of forty-three members of warring gangs the Hood Starz and the Wave Gang, responsible for six homicides and thirty-two shootings, following surveillance on Facebook and Twitter); Mosi Secret, *Facebook Friends Boasted of Gang War, Police Say*, N.Y. TIMES, Sept. 13, 2012, at A29 (reporting the indictment of forty-nine members of the warring Rockstarz and Very Crispy Gangsters, after the rival gangs used Facebook to threaten each other and brag about their exploits, including posing for pictures with the possessions of murdered rivals and publicly keeping score (i.e. "Rockstarz are up 3-0").).

182. *See, e.g.*, Masis, *supra* note 180 (describing an incident wherein "police were able to prevent underage drinking at a high school graduation party using information they obtained on Facebook. 'The [partygoers] were talking about who was going to get the booze first[.]'"); Oren Yaniv, *CYBERBUSTED! Cop 'Friends' Gang to Snuff Out Crime*, DAILY NEWS, May 31, 2012, at 10 (describing how a Brooklyn police officer was able to friend members of the Brower Boys, a gang behind a string of robberies and assaults, which enabled officers to coordinate video surveillance and catch gang members in the act).

183. LEXISNEXIS, *supra* note 179, at 5.

184. Carlos Miller, *MDPD's Homeland Security Bureau Was Monitoring My FB Page Hours Before My Arrest*, PINAC (Apr. 22, 2012), http://www.pixiq.com/article/MDPDs-Homeland-Security-Bureau-Monitoring-My-FB-Page (describing the events of Miller's arrest, during which the memory card of Miller's camera was deleted, and the subsequent results of a public records request for records related to Miller's arrest).

185. *Id.*

186. *Id.*

187. *Id.*; *see also* E-mail from Maritza Aschenbrenner, Detective, Miami-Dade Police Homeland Security Bureau, to Alvaro A. Zabaleta et al. (Jan. 31, 2012, 9:57 PM), *available for download at* http://www.dropbox.com/s/d37534bg93jia07/RawDashCam_20120130-20120314_Run_01.pst ("Carlos Miller is a Miami multimedia journalist who has been arrested twice for taking pictures of law enforcement. He has

this kind of "situational awareness" where police know the identities and backgrounds of those in attendance at protests could clearly lead to biased or retaliatory police actions targeting individuals based not on what they are doing but on who they are.

A slightly more comic example of police monitoring social media for potential "threats" occurred when activist Danny Panzella took to Facebook at the last minute to coordinate a "flash mob street action" in New York to mirror a similar "End the Fed" event happening in Philadelphia.[188] Danny arrived to find that, though he was one of only two protestors who showed up to pass out fliers on the street, forty police officers had surrounded the Federal Reserve building in preparation for the event.[189] Similar tactics have been used to monitor and protect against protests at World Trade Organization and G-8 meetings, as well as the 2012 national political conventions.[190] In situations like these, it can be challenging to strike the right balance between society's interest in effective preventative policing and the individual's right to expression, which can be unduly chilled through disproportionate police response.[191]

The misuse of Facebook and other electronic data by police is morally objectionable, even if those data are public. Facebook posts, even public ones, are intended for an audience of friends, not random strangers. Perhaps the Miller case is disturbing precisely because an innocent statement intended for friends was subsequently read and used by an unintended recipient to target Miller at the Occupy eviction. Or, perhaps, the issue is that the government's use goes beyond mere reading. Representative Patrick Meehan, during a meeting of the Subcommittee on Counterterrorism and Intelligence of the Committee on Homeland Security, observed that:

> [I]f an individual willingly and publicly uses Facebook, Twitter, or the comments section of a newspaper website, they, in effect, forfeit their right to any expectation of privacy. However, other private individuals reading public Facebook status updates is different than the Department of Homeland Security reading them, analyzing them, and possibly disseminating and collecting them for future purposes.[192]

Currently, police use of recipient-level surveillance is relatively

publicly posted on social networks that he will be taking pictures today in order to document the eviction.").

188. TruthSquadTV, *US Government Monitoring Facebook for Federal Reserve Protests*, YOUTUBE (Aug. 8, 2011), http://www.youtube.com/watch?v=58pwSxlyurk.

189. *Id.*

190. Marko Papic & Sean Noonan, *Social Media as a Tool for Protest*, STRATFOR GLOBAL INTELLIGENCE (Feb. 3, 2011, 3:54 PM), http://www.stratfor.com/weekly/20110202-social-media-tool-protest.

191. The presence of a single police officer has a minor chilling effect, but that effect is offset by the public safety benefits of having a proportionate law enforcement presence. However, advanced warning of protests by unpopular groups increases the likelihood of an overwhelming police presence driven not by public safety needs but by distrust of the protesting individuals.

192. *DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy: Hearing Before the Subcomm. on Counterterrorism and Intelligence of the Comm. on Homeland Security*, 112th Cong. 2 (2012) (statement of Patrick Meehan, Chairman, S. Comm. On Counterterrorism and Intelligence).

unrestricted. Under *Katz*, the Fourth Amendment does not protect publicly posted online content, since online content bears no reasonable expectation of privacy.[193] Even privately posted content (i.e., content where viewing is restricted to "friends") is not protected when the police gain access to it through the disclosure of someone who was voluntarily granted access, such as a Facebook friend or Twitter follower.[194] This reasoning currently extends, per the misplaced trust doctrine, to situations where a police officer uses a false identity to become a defendant's "friend" and thereby to access that individual's restricted information.[195]

The greatest bars at present to investigative and preventative usage of social media are administrative and not legal. Many officers do not use social media in investigations because they are not allowed to access it on departmental computers or because they do not know how to use it.[196] However, these barriers will erode as the social media market-share increases and as law enforcement agencies institutionalize their social media usage. As social-media-based policing increases, it is increasingly likely that police will use public posts to investigate and prevent criminal acts.

Such capture of publicly available information is unquestionably legal under the current interpretation of the *Katz* framework.[197] It is also unlikely that such surveillance would run afoul of the Privacy Act of 1974, given that community policing is a valid law enforcement activity.[198] And in many ways, such activities appear no different than the traditional function of the beat cop. Where information is public and the police can investigate or prevent crime by accessing it, the public good necessitates that they should do so. This analogy

193. *See* United States v. Gines-Perez, 214 F. Supp. 2d 205, 212–14 (D.P.R. 2002), *vacated on other grounds* 90 Fed. Appx. 3 (1st Cir. 2004) (rejecting a criminal defendant's contention that he had a reasonable expectation of privacy in a photo posted to his company's public website because the site was still "under construction" and was not yet intended for public commercial use); *see also* United States v. Meregildo, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012) ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment.").

194. *Meregildo*, 883 F. Supp. 2d at 526 ("Where Facebook privacy settings allow viewership of postings by 'friends,' the Government may access them through a cooperating witness who is a 'friend' without violating the Fourth Amendment.").

195. *See, e.g.*, Heather Kelly, *Police Embrace Social Media as Crime-Fighting Tool*, CNN (Aug. 30, 2012, 5:23 PM), http://www.cnn.com/2012/08/30/tech/social-media/fighting-crime-social-media/index.html (arguing that although use of fake profiles constitutes a violation of Facebook's terms of service, the practice is common, legal, and indistinguishable from the common investigative tactic of posing as a potential buyer of illicit goods). For more on the potential application of the misplaced trust doctrine, see notes 346–49, *infra*, and accompanying text.

196. LEXISNEXIS, *supra* note 179, at 7. The survey reported that, when asked why social media is not used in investigations, thirty-seven percent of respondents reported being unable to access social media during working hours and thirty-three percent of respondents reported not having enough knowledge to use social media. *Id.* Only four percent of respondents reported believing that the information contained in social media was not useful to the investigation. *Id.*

197. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (setting forth the principle that Fourth Amendment protection applies when (1) a person has "exhibited an actual (subjective) expectation of privacy" and (2) "that the expectation [is] one that society is prepared to recognize as 'reasonable'").

198. Recall that the Privacy Act of 1974 prohibits agencies from maintaining records regarding individual First Amendment activity unless they are pertinent to a legitimate law enforcement activity. Application of this provision, however, is likely to be limited both by the interpretational challenges of defining "exercise[] of rights guaranteed by the First Amendment" in the context of the Internet and the broad scope of community policing and crime prevention functions. 5 U.S.C. § 552a(d)(7) (2012).

becomes strained, however, when the police use deceit to gain access to otherwise private information, such as that contained in private groups, forums, or e-mail lists.

Applying *Katz* in this context, there is no reasonable expectation of privacy, because anything shared with a third party is no longer private. *Katz*'s binary treatment of the "reasonable expectation" of privacy is not a sufficient model in the Internet context, and the precedents governing its application to the Internet have been tainted by extreme factual situations that have undermined the standard protections.[199]

In a number of cases, the courts have allowed the discovery of social media profiles on the theory that there is no privacy in information disclosed to a third party, even when the extent of disclosure beyond that party is limited through privacy controls.[200] However, this approach equates privacy with secrecy, when in reality information can still be private even if it is not secret.[201]

Privacy law theory makes clear that privacy functions in spheres and that information shared with friends or family may nonetheless be considered "private" vis à vis the world at large.[202] Robert Sprague argues for a confidentiality standard that would allow individuals to retain their privacy rights even when information is published, based on the fact that "[t]he intent in publishing the information is often only to share it with a few friends."[203] That the content is widely accessible is an indirect consequence, Sprague argues, and the accessing of that information by outside parties is tantamount to invasion of privacy.[204] Lior Strahilevitz similarly argues that a large amount of information shared with others—statements made to medical professionals, the clergy, coworkers, family, and friends—may nonetheless be considered

199. *See* Robert Sprague, *Rethinking Information Privacy in an Age of Online Transparency*, 25 HOFSTRA LAB. & EMP. L. J. 395, 407–08 (2008) (noting that the precedents regarding computer and Internet privacy stem from *Pennsylvania v. Sodomsky*, 939 A.2d 363 (PA. Super. Ct. 2007), a case concerning child pornography and cautioning that "bad facts make bad law.").

200. *See* Jasmine E. McNealy, *The Realm of the Expected: Redefining the Public and Privacy Spheres in Social Media*, *in* SOCIAL MEDIA: USAGE AND IMPACT 255, 262–64 (Hana S. Noor Al-Deen & John Allen Hendricks eds., 2012) (listing cases); *cf.* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (finding private messages sent in Facebook and Myspace to be protected under the SCA).

201. *See* Sprague, *supra* note 199, at 408–09 (noting the need for an attitudinal shift towards acceptance of the idea that just because a few people have access to information does not mean it is no longer private).

202. Although privacy theory, and a number of cases, support the information spheres approach to privacy, the Court's application of the third party doctrine has clung to the outdated conception that only absolute secrecy can create a reasonable expectation of privacy. *See, e.g.*, Briscoe v. Reader's Digest Ass'n, 483 P.2d 34, 37 (Cal. 1971) (noting that the claim underlying the right to privacy "is not so much one of total secrecy as it is of the right to *define* one's circle of intimacy—to choose who shall see beneath the quotidian mask."); *see also* Solove, *supra* note 54, at 1176–84 (demonstrating that courts are deeply divided about whether to adhere to the "secrecy paradigm" or to recognize privacy in public or disclosed information); *id.* at 1153 ("Certainly, public disclosure does not eliminate the privacy of information; indeed, even information that is exposed to others may retain its privacy character. . . . [P]rivacy depends upon degrees of accessibility of information . . . ."). *But see* Hoffa v. United States, 385 U.S. 293, 302 (1966) ("Neither this Court nor any member of it has ever expressed the view that the Fourth Amendment protects a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it.").

203. *See* Sprague, *supra* note 199, at 410.

204. *Id.*

private, especially where strong social norms govern.[205] Strahilevitz also points out that in the Internet context, the volume of digital "noise" can sometimes be sufficient to minimize or neutralize the exposure of publicly shared information.[206] Thus, many "Internet natives" might consider their electronic communications to limited audiences to be private, despite the fact that such communications do not fit within *Katz*'s "reasonable" expectation of absolute privacy.[207]

Daniel Solove has also highlighted that there is a difference between what we expect to be private vis-à-vis others and what we expect to be private vis-à-vis the government.[208] The focus, he concluded, should be on whether "collective society wants the *government* to be able to know rather than whether certain matters are public or private based on the extent of their exposure to others."[209] In a hypothetical, he asks "[i]f we allow a loved one to read our diary" would we also "want the government to be able to read it?"[210] Solove finds that the very existence of the Fourth Amendment answers this question, indicating that the government stands in a different position than ordinary citizens or private sector organizations.[211]

There are also valid policy reasons to disfavor treating "undercover" online activity equally with undercover investigations in the real world. The undercover investigation of an expressive association in the real world requires, at a minimum, showing up to the meetings and being familiar with the organization, its literature, and its goals. These investments serve as an effective check on the frequency of such investigations. A police officer, however, can gain access to a private Facebook page or group or an e-mail listserv in all the time it takes to send a friend request or message requesting access and to receive approval. This allows the police, with the same resources, to infiltrate many more semi-private spheres of communication. This efficiency encourages and enables excessive monitoring of expressive associations by reducing the contravening practical considerations against which the need for any surveillance activity is weighed, such as whether the surveillance is the best use of the officer's time or departmental resources. Perhaps part of the complication is a popular notion of implicit trust that those within private communication channels, such as restricted access forums, are who they claim to be.[212]

---

205. Lior J. Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 970 (2005).

206. *Id.* at 968–69.

207. As Daniel Solove has noted, the "problem with focusing on whether information is private is that privacy is a product of context, not the status of particular facts. Easy distinctions such as intimate versus nonintimate and secret versus nonsecret fail to account for the complex nature of what is considered private. Privacy is a dimension of social practices, activities, customs, and norms that are shaped by history and culture." Solove, *supra* note 54, at 1153.

208. *Id.* at 1154.

209. *Id.* at 1156.

210. *Id.*

211. *Id.*

212. This trust arguably stems from the combination of access and irrelevance. A paralegal, for instance, would expect some level of privacy in posts to a paralegal-only listserv, even though the information posted to it is not absolutely private. Obviously, this contention does not hold true in contexts where the very nature of

Although police misuse of publicly available information online is unfortunate and disconcerting, it is not contrary to the tenets of associational privacy or the current interpretation of the Fourth Amendment. However, police use of false identity and deception to gain access to information that is willingly shared but not publically available is more problematic both from privacy and policy perspectives. Such actions can chill communications between group members by creating a fear of surveillance within semi-private contexts.

B. Transmitter Level Surveillance

Transmitter level surveillance consists of the real-time or retroactive acquisition of data from a third party.[213] The acquisition of such data is constitutionally regulated by *Katz*'s reasonable expectation of privacy, which provides little protection, because the non-content data involved are accessible to the third party service provider and are therefore not considered to be private.[214]

Government acquisition of transmitter level data has been at the forefront of privacy concerns recently, primarily following the subpoena of an Occupy protestor's Twitter account. The protestor, Malcolm Harris, was charged with disorderly conduct after allegedly marching on the roadway of the Brooklyn Bridge during an October 1 march.[215] Prosecutors sought to subpoena Harris's Twitter account, both for user information (such as associated e-mail addresses) and for any tweets posted between September 15 and December 31, 2011.[216] Both Harris and Twitter sought to quash the subpoena on Fourth Amendment grounds, which the court rejected.[217] In particular, the court found that Harris's tweets, even if later deleted, were public because "it is the act of tweeting or disseminating communications to the public that controls."[218] More worrisome, though, are the non-public transactional records that New York may acquire alongside the tweets. Twitter's records of Harris's IP address, for instance, can tell investigators where Harris was when he logged into Twitter, giving them the ability to track his location for a three-month period.[219]

---

the discussion signals that privacy should not be assumed (such as an online venue focused on illegal activities).

213. *See* People v. Harris, 949 N.Y.S.2d 590 (N.Y. Crim. Ct. 2012); Eric Lichtblau, *Wireless Firms Are Flooded by Requests to Aid Surveillance*, N.Y. TIMES (July 8, 2012) (providing examples of retroactive acquisition of data (tower "dumps")).

214. *See* United States v. Miller, 425 U.S. 435, 443 (1976) (allowing the government to subpoena an individual's bank records and noting that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

215. *Harris*, 949 N.Y.S.2d at 591–92.

216. *Id.*

217. *Id.* at 594–96.

218. *Id.* at 595 (the court subsequently highlighted the plethora of services that store and display since-deleted tweets).

219. *See* Aden Fine, *Twitter Appeals Ruling in Battle Over Occupy Wall Street Protestor's Information*,

The second-hand information the government can obtain includes more than just tweets and the accompanying transactional data, however. The government, through service providers, can gain access to a wealth of personal information. Cell phones, even those without GPS, provide general location data to carriers based on the cell towers that route traffic.[220] Among other methods, police can request "tower dumps," which provide data on all subscribers connected to a tower during a given period of time.[221] One in four responding police agencies now admits to using cell tower dumps.[222] In 2010, Colorado authorities requested twenty tower dumps to aid in their search for a missing girl.[223] Sheriff Leon Lott of Richland County, South Carolina ordered four tower-dumps from two cell-phone towers to aid in his 2011 investigation of the theft of his gun and rifle collection from the back of his police-issued SUV while it was parked in his driveway.[224]

Tower dumps, conceivably, could enable police to ascertain who attended a known meeting or participated in a protest without requiring a single officer in attendance. Similar to the traditional subject matter of pen registers and trap-and-trace devices,[225] call logs can reveal much about an individual's associations. And police are increasingly accessing these data. During the second half of 2012, Google received 8,438 requests for information on 14,791 accounts, over twice as many requests as occurred during the same period in 2009.[226] Cell phone carriers reported 1.3 million law enforcement demands for subscriber information in 2011 in relation to investigations at the local, state, and federal levels.[227] In fact, federal law requires that telecommunications providers, including Voice over Internet Protocol (VOIP) providers like Skype and broadband Internet providers, ensure that government agents can tap or obtain information about any voice communication over their network.[228]

FREE FUTURE (Aug. 27, 2012, 12:44 PM), https://www.aclu.org/blog.technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy (highlighting the privacy concerns implicated in granting access to over three months of transactional Twitter data).

220. *See generally In re* Application of United States for Order for Disclosure of Telecomms. Records, 405 F. Supp. 2d 435, 449 (S.D.N.Y. 2005) (discussing the limits of such technology). At least one court has held that cell-site data is not accessible under the Pen Register statute, since the data is not incidental to the transmission of a communication. *In re* Application for Pen Register and Trap/Trace Device with Cell Site Location Auth., 396 F. Supp. 2d 747, 761–62 (S.D. Tex. 2005).

221. Lichtblau, *supra* note 213.

222. John Kelly et al., *Cellphone Data Spying: It's Not Just the NSA*, USA TODAY (Dec. 8, 2013, 5:10 PM), http://www.usatoday.com/story/news/nation/2013/12/08/cellphone-data-spying-nsa-police/3902809/.

223. *Id.* Authorities subsequently requested DNA samples from 500 potential suspects that the data-dumps helped to identify. Ultimately, the abductor was found when his mother turned him in.

224. *Id.* ("'We were looking at someone who was breaking into a lot of vehicles and was not going to stop,' Lott said. 'So, we had to find out as much information as we could.'").

225. The terms "pen register" and "trap and trace" are legacy terms describing the technology of the 1960's and 70's. KERR, *supra* note 145, at 498. A pen register was a device that could record the numbers dialed from a phone line, and a "trap and trace" was a device that could record the numbers of incoming calls. *Id.*

226. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/US (last visited Feb. 15, 2014).

227. *See* Lichtblau, *supra* note 213 ("[T]he widened cell surveillance cut[s] across all levels of government—from run-of-the-mill street crimes handled by local police departments to financial crimes and intelligence investigations . . . .").

228. *See* 47 U.S.C. §§ 1001–21 (2012) (establishing the Communications Assistance for Law

The present ECPA framework provides insufficient protections to privacy in general and associational privacy in particular. Information about an individual's associations is easily obtained through transactional data, which receive too little protection under the present framework. Twitter's most recent transparency report, for instance, reveals that during the first half of 2013, it received 905 user information requests for 1,319 accounts.[229] Of those requests, only thirty-four percent were judicially approved court orders or warrants; the rest were issued under subpoena or other less rigorous means.[230] The arbitrary and judicially uncertain 180-day rule for stored communications, and the complexity of the SCA generally, make it difficult for laymen to know when their communications are protected, and how protected they are. Most important, though, the proliferation of technology has greatly increased the amount of "privacy" that the ECPA protects, magnifying its shortcomings. Members of associations wishing to remain anonymous must not only forego the use of Facebook, Twitter, e-mail, and other modern communication mechanisms; they must also leave their phone at home when they go to meetings. However, these options are not viable for grassroots groups like Occupy Wall Street that lack centralized command and control functions, because they rely on this technology to organize and coordinate. Even if the group could function without electronic devices, many individuals no longer have the convenience of leaving their technology at home.[231] Thus, individuals are faced with a choice of participation or privacy, but not both.

Political association has always been on the brink of being thrust into the public sphere and has at times been made public through government misconduct. But society recoils at the memory of the instances when that has occurred.[232] If political association is made public and participation is therefore chilled, the damage is done not just to the silenced individual but also to the robustness of the civil discourse as a whole. In the modern world, the use of technology and the Internet is unavoidable. Neither Internet natives nor Internet migrants can avoid putting much of their information in third-party hands. To ask them to accept the risk of government access to that information is to ask them to accept the direct government access blocked in *NAACP* and legislatively opposed via the Privacy Act of 1974. Asking Internet users to

---

Enforcement Act's requirements as applicable to telephone companies); *see also* Communications Assistance for Law Enforcement Act and Broadband Access and Services, 70 Fed. Reg. 59,664 (Oct. 13, 2005) (extending CALEA's interpretation to cover VOIP and broadband Internet access services).

229. *Information Requests*, TWITTER, https://transparency.twitter.com/information-requests/2013/jan-jun/us (last visited Feb. 15, 2014) (data reflects domestic requests).

230. *Id.*

231. Many employers, for instance, now expect their employees to carry their cell phones with them wherever they go and to be able to respond to e-mails instantaneously. *See* IPSOS, WORKPLACE TRENDS: IMPACT OF TECHNOLOGY 13 (2006), *available at* http://www.ipsos-na.com/download/pr.aspx?id=5890 (reporting that ninety-two percent of "knowledge workers" engage in work-related communications in non-work situations, and seventy-three percent report not being able to switch off their communications devices on weekends); *see also* Complaint at 4, Allen v. City of Chicago, No. 10-CV-03183 (N.D. Ill. May 24, 2010) (reporting on Chicago's practice of providing police officers with PDAs and requiring that the officers respond to work communications on receipt, whether or not they were on the clock).

232. The most flagrant examples of such instances include the House Un-American Activities Committee hearings and the violations revealed in the Church Reports.

accept government access to their online selves is to undermine associational privacy and, thus, irrevocably to chill the speech of the minority and the national discourse.

C. Data Mining

The final form of surveillance is data mining, the analysis of existing information to generate new information and insight. Data mining, by definition, consists of "the application of database technology and techniques—such as statistical analysis and modeling—to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results."[233] Thus, data mining is not so much surveillance as the analysis of surveillance and other information products. Nonetheless, the outcome of data-mining—extensive dossiers on targets and remarkably accurate predictive analyses—has at least as much of a chilling effect as traditional surveillance forms.

The government maintains a vast number of databases (almost 2,000 as of 2001) concerning immigration, bankruptcy, social security, military personnel, new hires, births, deaths, arrests, marriages, divorces, property ownership, voter registration, workers' compensation, and licensed professions.[234] These databases can be supplemented by massive private databases such as Experian, which has credit and demographic information on 215 million U.S. citizens, and MIB, Inc., which has the medical profiles of 15 million individuals.[235] The government also has access to "private" information, such as content and non-content traffic data obtained from telephone companies and Internet Service Providers through ECPA procedure or through FISA channels such as National Security Letters.[236] These databases, themselves something of a new creation, constitute a vast pool of information. What is revolutionary, though, is the newfound ability to analyze the data in a meaningful manner—to combine it across sources and to generate new intelligence with it. The invasion of privacy that can occur from the data mining of these vast troves of information can constitute something completely new, unanticipated by the framers and unaddressed by existing jurisprudence.

In a commercial context, data mining is how Amazon knows what products to suggest based on a customer's purchase history and how Google knows what ads to run based on a user's search history.[237] Data, in the form of account information, demographic information, past searches, past purchases,

---

233. U.S. GEN. ACCOUNTING OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 4 (2004), http://www.gao.gov/new.items/d04548.pdf; *see also* Lee Tien, *Privacy, Technology and Data Mining*, 30 OHIO N.U. L. REV. 389, 393–94 (2004) (noting that this definition "seek[s] to distinguish mere information retrieval using traditional query and report tools, which describe *what* is in a database, from "true" data mining, which uses automated processes to discover patterns. Because such patterns are themselves knowledge, the field is often referred to as "knowledge discovery.") (emphasis added).

234. Tien, *supra* note 233, at 389–90.

235. *Id.* at 390.

236. See the discussion in Part II.E for examples of where such transactional data could originate.

237. *The NSA Is Watching, but So Are Amazon and Google*, DALLAS NEWS (July 15, 2013, 10:37 AM), http://www.dallasnews.com/business/retail/20130714-the-nsa-is-watching-but-so-are-amazon-and-google.ece.

and other online activities, are analyzed to develop a predictive model showing (a) who customers are and (b) what products or promotions are likely to interest them.[238] These commercial data-mining systems have become so powerful and so accurate that they can even predict life events of which the customer's close family is unaware.[239] Though such systems are arguably harmless[240] in commercial usage, their accuracy can nonetheless be disconcerting.

However, government data mining can be significantly more intrusive. Not only does the government have the ability to use inter-departmental data, but it also is one of few entities with the ability to collect data from across industries, giving it a uniquely complete picture of the individual.[241] This picture can be used to look for patterns that might indicate future actions, or to find connections that might otherwise be overlooked. The constitutionality of data mining has traditionally been based on the constitutionality of the acquisition of the underlying data, though the mosaic theory and the rise of outcome-based conceptions of the Fourth Amendment both challenge this notion.

Fundamentally, data mining activities can be classified into three categories of use. The simplest use of data mining is record recall, accessing the raw information already collected about an individual and group.[242] Another category of use is subject-based "link" analysis, which begins with a particular individual and builds outwards through his or her data to create a full picture of his or her social, financial, business, and geographic links with others.[243] Finally, pattern-based analysis consists of searching data, with no suspicion as to any individual, for known patterns associated with a specific activity or characteristic.[244]

---

238. *Id.*

239. *See, e.g.*, Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. TIMES (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (describing how Target's data mining effort to predict pregnancies among customers was so accurate that the company sent a teen customer pregnancy-related advertising before she had informed her father of her pregnancy).

240. Even in the commercial context, data mining's ability to turn seemingly innocuous information into a complete picture of the individual challenges the personal moral obligation to protect individual privacy. *See generally* Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?,* 64 ALA. L. REV. 845 (2013) (examining the individual's moral obligation to protect their own privacy).

241. Judge Posner writes:

> [W]ith digitization, not only can recorded information be retained indefinitely at little cost, but the information held by different merchants, insurers, and government agencies can readily be pooled, opening the way to assembling all the recorded information concerning an individual in a single digital file that can easily be retrieved and searched.

RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 135 (2006).

242. As Katherine Strandburg notes, this kind of analysis is unlikely to chill expressive activity unless it is blatantly abused to study groups identified by their expressive activities. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741, 758–60 (2008).

243. *See id.* at 758 ("Targeted 'link analysis' focused on a particular individual would be used to determine the associative groups to which that individual belongs"); Tien, *supra* note 233, at 395 ("Subject-based analysis resembles traditional investigation: a particular subject is the starting point, and the technology automates the process of finding key relationships or associations.").

244. *See* Strandburg, *supra* note 242, at 758 ("[N]etwork 'models' of malevolent associations [are]

The analysis of these data has the potential to wholly remove the veil of privacy from individual associations by enabling investigators to reconstruct an individual's entire social network through his or her communications with others. Such data collection can contribute to the war on terrorism by allowing the government to find potential indicators of terrorism in otherwise innocuous and irrelevant data.[245] Data mining is a necessary tool if the government is to be able to cope with the massive volumes of data that flow through the Internet.[246] Proponents of data mining contend that there is no privacy harm in the process: the mined information is rarely seen by humans and generally exists only in databases unless it triggers closer scrutiny.[247] Yet many scholars disagree that data mining is harmless, and even proponents of data mining recognize that it may trigger legitimate and compelling privacy issues.[248]

If transmitter level surveillance damages associational privacy, data mining destroys it. After all, how can there be any privacy in membership when government computers can immediately calculate an individual's social links and suggest what group "patterns" that person fits into? The *NAACP* Court protected group membership lists from government request; data mining allows the government to reconstruct a likely version of the membership list without having to ask for it.

The ease with which this information can be had effectively chills expressive association just as the acquisition of the information by subpoena did in *NAACP*. The risks that data mining can create for group members compound that chilling effect. Because data mining is so focused on social networks, individuals can be exposed to suspicion through the actions of other members of their associations. In an era of data mining, the concern becomes not just "is this group safe to join," but "are its members safe to be in a group with?" These chilling concerns are precisely why the Privacy Act of 1974, which was created in response to concerns about government use of computerized databases, bars government maintenance of records on an individual's First Amendment exercises.[249] The exceptions to that provision are too broad, however, rendering the provision insufficient to reduce the chilling effect of data mining.[250]

The first major government data-mining program to receive public

---

developed and data mining techniques used for 'pattern analysis' in the hope of identifying terrorists or other criminally or socially troublesome networks."); Tien, *supra* note 233, at 395 (describing how in pattern-based queries "some model or pattern of behavior is identified and then one searches for instances of that pattern in a database or databases.").

245. *See* POSNER, *supra* note 241, at 141 ("In an era of global terrorism and proliferation of weapons of mass destruction, the government has a compelling need to gather, pool, sift, and search vast quantities of information, much of it personal.").

246. *Id.* at 143.

247. SOLOVE, *supra* note 46, at 183.

248. *See, e.g.*, Tien, *supra* note 233, at 391 (discussing how data mining can pose serious threats to certain civil liberties).

249. ALLEN, *supra* note 137, at 655.

250. An exception, for instance, is provided for "authorized law enforcement activity." 5 U.S.C. § 552a(e)(7) (2012). Inherent in the war on terror is the assumption that anyone could be a terrorist or otherwise a threat to security; thus, an arguable law enforcement justification for data mining could be said to exist for everyone.

attention was the Total Information Awareness program, developed by the Department of Defense in 2002.[251] The Total Information Awareness database was to consist of financial, educational, health, and other information that would be used to identify potential terrorists based on patterns of activity observed in past terrorist attacks.[252] Following public outcry based on privacy concerns, the Total Informational Awareness program was ultimately unfunded by a unanimous Senate vote, though many observers believe that similar, more clandestine data mining programs endure.[253] A more recent phenomenon is "fusion centers," which have been described as an amalgamation of commercial and public sector resources designed to optimize and streamline the collection, analysis, and dissemination of information on individuals.[254] Internal Department of Homeland Security documents reveal that these fusion centers played a significant role in responding to law enforcement inquiries surrounding Occupy Wall Street.[255]

A 2004 GAO Report reported that 52 agencies had or were implementing data mining efforts across 199 distinct data mining programs, 122 of which involved the use of personal information.[256] A later report highlighted that insufficient policies and oversight within Department of Homeland Security data mining programs were jeopardizing the programs' privacy protections.[257] Data mining has been, and potentially is currently, used in concert with warrantless wiretaps to allow the extraction of data from private communications on a massive scale.[258] Such systems use packet-sniffing to electronically search for specific, targeted content such as a distinct image or phrase.[259]

---

251. SOLOVE, *supra* note 46, at 183.

252. *Id.*

253. *See, e.g.*, *id.* at 185 (arguing that the TIA didn't really die, but instead "live[s] on in various projects with obscure names such as Basketball, Genoa II, and Topsail . . . . [P]rojects significantly more clandestine [than the TIA]."); *see also* Mark Clayton, *US Plans Massive Data Sweep*, CHRISTIAN SCI. MONITOR, Feb. 9, 2006, at USA 1 (describing ADVISE, a Department of Homeland Security data mining program similar in scope to TIA).

254. Fusion Center data ranges from:

> [A]ll sources of financial records; all contacts with the criminal justice system by criminals and non-criminals, all tribal, local, state, federal, private, and university law enforcement records including US Postal Inspectors, all forms of education (day cares, preschools . . .); government issued licenses and permits, medical records . . . hospitality and lodging, gaming industry, telecommunications service providers . . . US Post Offices, postal and shipping services, private security . . . .

Lillie Coney, Elec. Privacy Info. Center, Statement to the Department of Homeland Security Data Privacy and Integrity Advisory Committee 5 (Sept. 19, 2007), *available at* http://epic.org/privacy/fusion/fusion-dhs.pdf.

255. *Production 1*, P'SHIP FOR CIVIL JUSTICE FUND (May 22, 2012), http://www.justiceonline.org/commentary/index-of-document-productions.html (last visited Feb. 15, 2014).

256. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-04-548, DATA MINING: FEDERAL EFFORTS COVER A WIDE RANGE OF USES 2–3 (2004).

257. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-11-742, DATA MINING: DHS NEEDS TO IMPROVE EXECUTIVE OVERSIGHT OF SYSTEMS SUPPORTING COUNTERTERRORISM 32 (2011).

258. *See* Eric Lichtblau & James Risen, *Spy Agency Mined Vast Data Trove, Officials Report*, N.Y. TIMES, Dec. 16, 2005, at A1 (describing the "pattern analysis" of domestic call data collected during the warrantless domestic surveillance authorized by President Bush); *see supra* note 172 and accompanying text (alleging that instead of intercepting specific communications, the NSA has elected to intercept all data and to analyze those data after the fact).

259. *See* Jeralyn, *NSA Surveillance: Packet-Sniffing Vs. Data Mining*, TALKLEFT: POL. CRIME (Jan. 4,

The most favorable assessments of data mining, of course, originate within the government.[260] Several scholars, including Judge Posner, also support data mining on the basis that the use of data mining actually benefits privacy. Judge Posner contends that data mining protects privacy by filtering out irrelevant information and ensuring that only data that warrant suspicion are seen by human eyes.[261] The primary hazard of such data mining, according to Judge Posner, is that the information could be "used to blackmail or otherwise intimidate the administration's critics and political opponents."[262] However, scholars such as Daniel Solove raise a host of other concerns about the data mining process, primarily based on concerns of accuracy, process, and transparency.[263] These concerns reflect the fear of wrongful targeting aggravated by the lack of procedures to address such errors.[264] Furthermore, even if a data-mining program is perfect, the necessary lack of transparency ensures that citizens will have no way to be reassured of that fact.[265] Similarly, there is a risk that data mining systems will target people for their First Amendment protected activities.[266] Indeed, it seems almost certain that a successful data mining program would have to take into account factors like religion, individual expressions, associational memberships, and the like,

---

2006, 7:11 PM), http://www.talkleft.com/story/2006/01/04/949/26006/waronterror/NSA-Surveillance-Packet-Sniffing-vs-Data-Mining (last visited Feb. 15, 2014) (packet-sniffing can look for specific letters, numbers, or symbols).

260. At a congressional hearing on NSA surveillance, Attorney General Alberto Gonzales said:

> Our enemy is listening, and I cannot help but wonder if they are not shaking their heads in amazement at the thought that anyone would imperil such a sensitive program by leaking its existence in the first place, and smiling at the prospect that we might now disclose even more or perhaps even unilaterally disarm ourselves of a key tool in the war on terror.

Wartime Executive Power and the National Security Agency's Surveillance Authority: Hearings Before the S. Comm. on the Judiciary, 109th Cong. 15 (2006) (statement of Alberto R. Gonzales, Att'y Gen. of the United States).

261. *See* POSNER, *supra* note 241, at 130 ("An electronic search no more invades privacy than does a dog trained to sniff out illegal drugs, though the dog's 'alerting' to the presence of drugs in a container provides probable cause for a (human) investigator to search the container."). It should be noted that Judge Posner's metaphor is inexact, because unlike a dog's 'alert,' a data-mining program's recognition of a pattern—as opposed to recognition of content via packet sniffing—does not, alone, have the potential to create probable cause.

262. *Id.* Posner's concerns about improper use of data are not unfounded; his concerns harken to the attempts to blackmail Martin Luther King, Jr. revealed in the Church Report.

263. *See* SOLOVE, *supra* note 46, at 186–94 (raising concerns of inaccuracy, due process, transparency, equality, and First Amendment protection with regards to data mining). Solove's concerns largely mirror the dissociation between intelligence data mining practices and general fair information practice principles. *See also Fair Information Practice Principles*, FED. TRADE COMMISSION (Nov. 23, 2012), http://web.archive.org/web/20130303163422/http://www.ftc.gov/reports/privacy3/fairinfo.shtm (archived version of website, which identifies the five principles of fair information practices: (1) notice/awareness, (2) choice/consent, (3) access/participation, (4) integrity/security, and (5) enforcement/redress).

264. *See* SOLOVE, *supra* note 46, at 186–94.

265. *See generally id.* at 193–194 (discussing the importance of transparency in government-run data mining).

266. *See Unitarian Church, Gun Groups Join EFF to Sue NSA Over Illegal Surveillance*, ELEC. FRONTIER FOUND. (July 16, 2013), https://www.eff.org/press/releases/unitarian-church-gun-groups-join-eff-sue-nsa-over-illegal-surveillance (discussing the current lawsuit brought by nineteen organizations against the National Security Agency for violating their First Amendment right of association by illegally collecting their call records). *See also* Daniel J. Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112, 154–59 (2007) (describing the "chilling effects" data mining could have on First Amendment protected activities).

creating a clear potential for misuse.

Beyond the practical concerns lies a more theoretical and fundamental privacy issue: that pattern-based data mining itself in some way invades individual privacy, even if the component data are all legally obtained. Data mining is not simply the centralization of data such that it can be searched in the same manner that one searches Google.[267] If it were, then the privacy concerns involved would be exactly those implicated by the underlying work. However, data mining does more: once the data are collected, those data are analyzed and patterns, many of which are so subtle or complicated that they would not be recognized by human intelligence analysts, are reported.[268] Like turning straw into gold, data mining can create an invasion of privacy using solely public data that would otherwise have minimal investigative value.[269]

This process implicates the "mosaic theory" of privacy, which posits that privacy interests should be measured by the sum of the parts and not by the privacy interest in the individual pieces of data forming the whole.[270] The mosaic theory originated in the FOIA context in *United States Department of Justice v. Reporters Committee for Freedom of the Press*[271] and has since been applied to criminal investigations by the D.C. Circuit in *United States v. Maynard*.[272] However, this theory is still novel within the Fourth Amendment context, and its application is hotly contested.[273]

In *Reporters Committee for Freedom of the Press*, the Court held that statutory privacy protections prohibited the release of an individual's criminal rap sheet pursuant to a FOIA request even though the underlying offenses were all matters of public record.[274] In *Maynard*, police (in violation of the terms of

---

267. Tien, *supra* note 233, at 393–94 (distinguishing "mere information retrieval using traditional query and report tools, which describe *what* is in a database, from 'true' data mining, which uses automated process to discover patterns.").

268. U.S. GEN. ACCOUNTING OFFICE, *supra* note 233. *See also* Hian C. Kob & Gerald Tan, *Data Mining Applications in Healthcare*, 19 J. HEALTHCARE INFO. MGMT. 64, 65 (2005) ("Data mining aims to identify valid, novel, potentially useful, and understandable correlations and patterns in data by combing through copious data sets to sniff out patterns that are too subtle or complex for humans to detect.").

269. Natasha Singer, *Mapping, and Sharing, the Consumer Genome*, N.Y. TIMES (June 12, 2012), http://www.nytimes.com/2012/06/17/technology/acxiom-the-quiet-giant-of-consumer-database-marketing.html?pagewanted=all&_r=1&.

270. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749 (1989) (holding that in interpreting the privacy exemption to FOIA, the privacy interests should be measured by the sum of the parts of all the documents involved, not each document by document).

271. *Id.* at 763–65 (finding that information contained in public records scattered across the country and the same information contained in a unified document involve vastly different privacy interests, because the unified document is not otherwise freely available).

272. *Maynard*, 615 F.3d at 560–64 (rejecting the possibility that the long-term GPS tracking of a car was not a Fourth Amendment search because the defendant's individual movements were constructively exposed), *aff'd in part by* United States v. Jones, 132 S. Ct. 945, 950–54 (2012) (rejecting the mosaic theory and instead affirming on trespass grounds).

273. *Compare* Orin Kerr, *D.C. Circuit Introduces "Mosaic Theory" of Fourth Amendment, Holds GPS Monitoring a Fourth Amendment Search*, VOLOKH CONSPIRACY (Aug. 6, 2010, 2:46 PM), http://www.volokh.com/2010/08/06/d-c-circuit-introduces-mosaic-theory-of-fourth-amendment-holds-gps-monitoring-a-fourth-amendment-search/ (highlighting the practical and legality principle concerns inherent in using an aggregate approach to defining "search" for Fourth Amendment purposes), *with* Solove, *supra* note 54, at 1185 (noting that making distinctions based on the status or source of information fails to account for the "aggregation problem" caused by the accumulation of details).

274. *See Reporters Comm. for Freedom of Press*, 489 U.S. at 762–70 (noting that the role of availability

their warrant) affixed a GPS tracker to a suspect's vehicle and subsequently monitored the suspect's location for a month.[275] The D.C. Circuit, sitting en banc, found that the mosaic theory set forth in *Reporters Committee for Freedom of the Press* applied and that the suspect had a reasonable expectation of privacy as a result.[276] However, this application of the mosaic theory to an ongoing investigation created retroactive unconstitutionality, wherein initially constitutional investigative techniques become retroactively unconstitutional through their continued use.[277] In effect, the use of the GPS tracker was initially legal, but it became illegal because the tracker produced too much evidence. This outcome is clearly impractical, because it denies investigators clear guidance and withholds the determination of an investigative procedure's constitutionality until after the procedure's use has been completed.[278]

Data mining presents a stronger privacy violation than those the Court has recognized in the FOIA context, because it consists not only of the amalgamation of otherwise disparate publicly available data but the subsequent analysis of that data to reveal information not otherwise apparent. Applying the mosaic theory to data mining is also a much simpler proposition than applying it retroactively to ongoing criminal investigations as the D.C. Circuit did in *Maynard*.[279] The legality of the information input into data mining processes is based solely on its means of acquisition. The act of data mining is discrete: only information, not the investigative actions generating that information, is aggregated. Thus, application of the mosaic theory to data mining inputs can prevent the kind of retroactivity problems created by *Maynard*.

Applying the mosaic theory to data mining, it is clear that data mining, if measured by the same standard, would constitute a search. In *Maynard*, the Court reasoned that:

> [T]he whole of a person's movements over the course of a month is not actually exposed to the public because the likelihood a stranger would observe all those movements is not just remote, it is essentially nil. It is one thing for a passerby to observe or even to follow someone during a single journey as he goes to the market or returns home from work. It is another thing entirely for that stranger to pick up the scent again the next day and the day after that, week in and week out, dogging his prey until he has identified all the places, people, amusements, and chores that make up that person's

---

of information in defining privacy "supports the distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole.").

275. *Maynard*, 615 F.3d at 549.

276. *Id.* at 562 ("A reasonable person does not expect anyone to monitor and retain a record of every time he drives his car, including his origin, route, destination, and each place he stops and how long he stays there; rather, he expects each of those movements to remain 'disconnected and anonymous'. . .").

277. Kerr, *supra* note 273 (highlighting the "bizarre consequence of creating retroactive unconstitutionality").

278. *See* Benjamin M. Ostrander, Note, *The "Mosaic Theory" and Fourth Amendment Law*, 86 NOTRE DAME L. REV. 1733, 1748 (2011) (discussing how the application of the "mosaic theory" to the Fourth Amendment would not only be wrong in principle, it would be impractical in application).

279. *Maynard*, 615 F.3d at 558–63.

> hitherto private routine.[280]

Similarly, the whole of a person's credit card billing, phone calls, medical records, tax records, e-mail history, library book records, living arrangements, enrollments, memberships, and biographical information is exposed to third parties, and at least some of it is therefore unprotected by the reasonable expectation of privacy. Yet, this information is not, under the *Maynard* view, exposed to the public, because no reasonable person would expect a third party to gain access to, combine, and analyze all of these disparate records. To combine and analyze this data, therefore, would likely constitute a Fourth Amendment search under *Maynard* and would require a warrant or probable cause.[281] If *Maynard* is, as it should logically be, extended into the context of data mining, it becomes clear that the constitutional protections currently applied to the data mining process are wholly insufficient. The acquisition of "complete" knowledge, without any form of underlying due process, creates the very risk of exposure against which the associational privacy doctrine is meant to protect.[282]

Another major privacy concern surrounding data mining is that data mining constitutes "a form of digital dragnet search," comparable in concept to the broad fishing expeditions that the Fourth Amendment's particularity requirement disallows.[283] A lack of particularity can frustrate the probable cause requirement by allowing the state indiscriminate entry into protected spheres without suspicion, effectively replicating the general warrants the Fourth Amendment was meant to bar.[284] The particularity requirement necessitates that, when a warrant is issued, it enumerates the location to be searched and items to be seized for which probable cause exists.[285] Beyond the text of the Fourth Amendment, however, reflections of the particularity requirement are also found in the case law governing protective frisks.[286] Yet

---

280. *Maynard*, 615 F.3d at 560.

281. In a similar vein, Tien argues that data mining, even when drawn from public data, is objectionable as a warrantless secondary search. Tien, *supra* note 233, at 409–13 (drawing comparisons to Walter v. United States, 447 U.S. 649 (1980); United States v. Jacobsen, 466 U.S. 109 (1984); and Bond v. United States, 529 U.S. 334 (2000) to illustrate the applicability of the secondary search doctrine).

282. *See infra* Part IV.D (explaining existing privacy expectations and how they can be protected).

283. Daniel J. Solove, *Data Mining and the Security-Liberty Debate*, 75 U. CHI. L. REV. 343, 357 (2008); *see also* Tien, *supra* note 233, at 391–92 (explaining that even though the Supreme Court has approved of privacy-intrusive government techniques, it has left open the possibility that overbroad use of such techniques would be treated differently).

284. Tien, *supra* note 233, at 402. *See also* Maryland v. Garrison, 480 U.S. 79, 84 (1987) ("The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

285. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . and particularly describing the place to be searched, and the persons or things to be seized."); *see also* Steele v. United States, 267 U.S. 498, 503 (1925) (requiring that the place to be searched be identified clearly enough that the reader can "with reasonable effort ascertain and identify the place intended.").

286. During a *Terry* stop (a stop based on a reasonable suspicion of criminal activity) police officers may frisk those being stopped for weapons if the officers have a reasonable suspicion that the individual is armed or dangerous. *See generally* Terry v. Ohio, 392 U.S. 1 (1968). The frisk is limited by a set of particularity requirements that limit where the officer may search (the outside of the individual's clothing) and what the officer may search for (a weapon). *See, e.g.*, Sibron v. New York, 392 U.S. 40, 65 (1968) (noting in dicta that

Fourth Amendment protections are focused on the initial acquisition of evidence; the Fourth Amendment renders few restrictions on how evidence may be examined after it is obtained, indicating that data mining should not be directly restricted by a particularity requirement.[287]

Although the Fourth Amendment does not explicitly restrict data mining on particularity grounds since data mining is the mere analysis of existing evidence, some scholars have nonetheless argued that the need for particularity can be inferred from Fourth Amendment jurisprudence.[288] Pattern-based data mining requires searching the information of millions of people with no particularized suspicion as to any of them.[289] Even link-analysis data mining, targeting the networks of known or suspected terrorists, suffers from a particularity problem in that it casts suspicion based solely on associational contact.[290]

The chilling effect of such broad searches has been clear since the elimination of the general warrant.[291] To allow the government such a broad sweep, absent particularized suspicion, is to allow it to ferret out the expressive associations of everyone, thus denying the security of privacy to unpopular groups. But that is not to say that all data mining is bad. Data mining (of a less invasive and comprehensive form) can be a valuable tool for academics and policymakers as they seek to understand societal needs and to better target government programs. Many of the difficulties in regulating data mining, in fact, arise from the legislative desire to regulate "bad" data mining while permitting "good" data mining, which can raise First Amendment issues.[292]

Data mining is a new concern on the privacy front, as it is still a technology in its infancy. Furthermore, due to the secrecy that surrounds its use and the fact that its results are not admissible evidence in criminal trials it is impossible to know the full extent of its use.[293] However, even the threat of

---

an officer engaged in a *Terry* frisk is limited to "patting of the outer clothing of the suspect for concealed objects which might be used as instruments of assault" and may not go through the suspects pockets unless the initial patdown leads to the discovery of concealed objects that might be used as weapons); Minn. v. Dickerson, 508 U.S. 366, 378 (1993) (holding officer's further searching of "lump" in suspect's pocket once object was determined not to be a weapon to be constitutionally invalid).

287. When restrictions on the examination of evidence after seizure exist, it is usually a result of a special aspect of the evidence. Computer searches, for instance, consist of two steps: the seizure of the physical computer and the subsequent execution of an electronic search of the data on the seized computer for evidence. *See* KERR, *supra* note 145, at 374–76 (explaining the two-step search process of computers).

288. Tien, *supra* note 233, at 402–03 (noting that in *Berger v. New York*, 388 U.S. 41 (1967), the Court required particularity safeguards of a general wiretap warrant due to the broad scope of the privacy intrusion involved).

289. *Id.*

290. Lee Tien points out that, per *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979), "[M]ere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause." Tien, *supra* note 233, at 403–04.

291. *See generally supra* notes 66–71 and accompanying text.

292. See *Sorrell v. IMS Health Inc.*, 131 U.S. 2653, 2668 (2011), a case addressing a Vermont statute that sought to bar private pharmaceutical companies from using data mining to guide their marketing strategy as to individual physicians, while allowing data-mining and use of the underlying information for "health care research" and by journalists, insurers, the State, and others. The Court held that this regulation constituted both a content-based and a speaker-based restriction on speech that could not survive heightened scrutiny. *Id.* at 2672.

293. *See, e.g.*, Illinois vs. Gillian, 670 N.E.2d 606, 620 (Ill. 1997) (citing Illinois v. Stewart, 473 N.E.2d

such invasive technology is sufficient to chill group membership given the technology's retrospective capabilities. Data mining has the potential to wholly strip the intended protections of *NAACP* by allowing the government to recreate a group's membership lists and attendance, thus circumventing the civil protections established by *NAACP*. Therefore, current theories of privacy protection in the technological context must take into account the specter of data mining, as well as the government interests underlying such use.

V. HOW TO PROTECT FIRST AMENDMENT ASSOCIATIONAL PRIVACY IN A DIGITAL ERA

The three core types of government surveillance discussed vary in their level of invasiveness and in the level of Fourth Amendment protection available. However, all three methods (recipient level access, transmitter level access, and reconstructive access) have a very real potential to chill First Amendment associational activity. This Article will now analyze possible solutions to the problem these methods pose for associational privacy concerns and consider which solution is likely to be the most viable.

A. Maintain the Status Quo

The easiest response to implement is the continued maintenance of the status quo. However, a failure to protect associational privacy from government exploitation of technology will have detrimental results beyond the obvious chilling effect on First Amendment exercise. Assuming that law enforcement use of the Internet continues to expand, this approach would have a clear cost to the perceived (if not legally recognized) privacy interests of the individual and would chill associational privacy. It is highly likely that the use of subpoenaed electronic evidence, such as that in the Malcolm Harris case, would continue to increase, as would the government's use of data mining.

However, as Judge Posner points out, "protected communications are valuable to the persons communicating, whether they are good people or bad people, and this duality is the source of both the costs and the benefits of intercepting communications for intelligence purposes."[294] Although the security of information would not change absent government disclosure, increased government use of electronic data would surely lead to increased concern about the fundamental lack of privacy of electronic communications.

In the short term, the privacy of expressive associations would be chilled, and terrorists would be confronted with the logistical challenges that Posner contends would be imposed. However, neither activists nor terrorists will remain idle while their private communications are intercepted and read, and anonymity-protecting tools are becoming increasingly mainstream. Examples

840, 859 (Ill. 1984) (holding that prior acts evidence is not admissible if used to show propensity, but is admissible for any other purpose)).

294. POSNER, *supra* note 241, at 133.

of such technology include Tor, an anonymous, encrypted web browser initially developed by the Naval Research Laboratory,[295] Anonymous's Annonaceae operating system,[296] and deep web browser Freenet,[297] among others.

In the technological context, there is an easy answer to invasive surveillance: increased security. If the government fails to protect the public sufficiently from chilling government surveillance, activists will instead reduce and secure their digital footprint.[298] This, in turn, will promote the development and further expansion of anonymizing tools, which serves the needs of criminals and terrorists as well as advocates and group members. When communications are encrypted, it is necessary to break the encryption before the underlying contents of the communication can be analyzed. As more parties encrypt their communications, it becomes increasingly costly and time-consuming to evaluate those communications for potential threats.

Another unfortunate impact of such an approach would be the potential concentration of extremism. While tools may exist to reduce online presence, to truly escape government monitoring requires more than a little fanaticism; it requires continuous use of secure communication channels and the (at least temporary) eschewing of many modern tools of daily life, such as cell phones, unencrypted Internet communications, and credit cards.[299] These high costs would drive off less committed members of unpopular expressive associations, with the result that only the most committed members would remain. Removing the more moderate elements from unpopular expressive associations, beyond the constitutional harm caused by chilled speech, would thus also create social harm by concentrating radicalism.

Doing nothing to protect associational rights may be acceptable to those in favor of granting the government broad powers during the war on terrorism in the short term, but in the long term, it will lead to the radicalization of unpopular expressive groups and the promulgation of methods to escape or hinder government attention. Furthermore, this method perpetuates harms against individual privacy rights. This course fails to balance First Amendment associational privacy needs with government interests, and as such, does not offer a viable long-term approach that will protect the speech of

---

295. *Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en (last visited Feb. 15, 2014) (billing itself as aiding individuals who want to prevent companies from tracking them, journalists who want to safely communicate with sources, NGO workers who do not want to be identified by hostile governments, and, ironically, law enforcement officers who do not want to be identified through their government IP addresses).

296. THE ANONOS PROJECTS, chiselapp.com/user/treeofsephiroth/repository/anonos/home (last visited Feb. 15, 2014) ("Oppressed people need a way to stay safe from tracking and bypass censorship, and our tools may be quite influential in future protests").

297. *What Is Freenet?*, FREENET: THE FREE NETWORK, https://freenetproject.org/whatis.html (last visited Feb. 15, 2014).

298. For instance, instead of communicating through e-mail lists, forums, and social media tools, groups could move their communications to invite-only, encrypted chat rooms and e-mail chains accessed through identity-masking software or browsers.

299. *See* Bruce Schneier, *How to Remain Secure Against the NSA*, BRUCE SCHNEIER (Sep. 15, 2013, 8:11 AM), https://www.schneier.com/blog/archives/2013/09/how_to_remain_s.html (illustrating an example of the extreme measures suggested for avoiding government surveillance).

associational groups such as Occupy Wall Street. Nonetheless, it is likely that, for the immediate future, this approach will prevail.

B. Expanded Fourth Amendment Protections

The need to strengthen Fourth Amendment protections is a common theme among those suggesting reforms to better protect association privacy and First Amendment rights more generally from government information-gathering.[300] A primary vehicle for this theme of enhanced privacy protection is a concerted effort to update the ECPA.[301] ECPA reform is an ongoing topic of debate within the Congress; in November 2012, the Senate Judiciary Committee approved a proposed substitution to H.R. 2471 that would have created a warrant requirement for access to stored communication contents, removing the 180-day standard after which stored data is considered "abandoned."[302] Some service providers, including Google, Microsoft, Yahoo, and Facebook, have already begun to implement this proposed reform through their internal policies, contending that a perceived Fourth Amendment warrant requirement for content data trumps the ECPA framework.[303]

The Senate proposal, though groundbreaking in that it addresses the privacy problems posed by the ECPA's outdated standards, falls far short of what is needed. It completely ignores the clear harms that access to transactional information can pose, especially when combined with data analysis software. While addressing the outdated 180-day standard is significant, this reform would leave intact many of the provisions and programs that have the potential to generate a chilling effect on association.

Another proposal for reform, put forth by Orin Kerr, argues for a statutory suppression remedy specific to the ECPA as a means to protect individual rights and to promote the stability and clear resolution of issues of Internet surveillance law, enabling more effective policing.[304] A broader suppression remedy such as Kerr proposes would help to reduce the chilling effect that

---

300. *See, e.g.*, Amar, *supra* note 18 (arguing that First Amendment concerns should be incorporated into the Fourth Amendment's constitutional reasonableness analysis); Christopher Slobogin, *Surveillance and the Constitution*, 55 WAYNE L. REV. 1105, 1106 (2009) (recognizing the need for a rejuvenated Fourth Amendment). *But see* Solove, *supra* note 266, at 116 (arguing that the proper nexus for reform is the incorporation of the First Amendment into criminal procedure and not the expansion of the Fourth Amendment).

301. *See, e.g.*, Kerr, *supra* note 136, at 859 (arguing that "legislative rule-creation offers significantly better prospects for the generation of balanced, nuanced, and effective investigative rules involving new technologies" than reliance on judicially created rules); *see also* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004) (analyzing the SCA and proposing how its standards should be reworked).

302. Leahy Substitute to H.R. 2471, 112th Cong. 3–7 (2012).

303. Dieter Bohn, *Google, Microsoft, Yahoo, and Facebook Say They Require Warrants to Give Over Private Content*, THE VERGE (Jan. 26, 2013, 6:57 AM), http://www.theverge.com/2013/1/26/3917684/google-microsoft-yahoo-facebook-require-warrants-private-content.

304. *See generally* Orin Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 807 (2003) (explaining how the lack of an exclusionary rule for electronic evidence leads to few challenges to Internet surveillance practices, which results in "[t]he law remain[ing] unusually obscure, and the rare judicial decisions construing the statutes tend[ing] to confuse the issues, not clarify them.").

Internet surveillance produces by minimizing the risk of police behavior beyond the limits of the ECPA. A suppression remedy, more importantly, would promote the development of clear precedents, which in turn would better enable those engaged in expressive associations to guard their own privacy. The provision of a suppression remedy, however, would only impact a very limited subset of cases: those where the government illegally obtained information that was later used in a criminal trial. Although protecting against wrongful use in the criminal context would offer some reassurance, it would not ensure against the misuse of data outside of criminal prosecutions or significantly check the government's acquisition of electronic data. As such, the application of an exclusionary rule would effect only a small improvement in the protection of associational privacy.

C. First Amendment Associational Privacy as Criminal Law

Within the privacy field, there is an ongoing "general attack on current Fourth Amendment doctrine."[305] One prong of this attack, generalized broadly, consists of the argument that the First Amendment and Fourth Amendment protect different things and that the current Fourth Amendment jurisprudence insufficiently protects First Amendment rights in the criminal procedure context. Proponents of this approach argue that the First Amendment did, at one time, supply procedural protections,[306] and that there are doctrinal, historical, and normative justifications for its reincorporation into criminal procedure. If an instance of government information gathering implicates First Amendment values[307] and has a chilling effect on speech,[308] Solove argues that it should only be allowed to occur if there is (1) a significant government interest in the information[309] and (2) the government is using a narrowly tailored manner of collection.[310] In many cases, these standards would require that the information be obtained pursuant to a warrant and with probable cause.[311]

Katherine Strandburg, in her extensive examination of network analysis

---

305. Strandburg, *supra* note 242, at 796.

306. *See* Solove, *supra* note 266, at 133 (highlighting the common origins of the First, Fourth, and Fifth Amendment in concerns about seditious libel); *id.* at 138 (noting that, though *Boyd v. United States* was decided on Fourth and Fifth Amendment grounds, it functioned to protect a significant amount of contemporary First Amendment activity).

307. *Id.* at 153 (suggesting the adoption of Robert Post's approach of looking to whether government activity implicates First Amendment values, instead of the much lower threshold of whether it implicates First Amendment activity).

308. *Id.* at 154–59 (noting the need for a cognizable chilling effect as opposed to a mere apprehension).

309. *Id.* at 160 ("[T]he government must be able to establish a substantial interest in the information . . . . [which] would root out government information gathering initiatives that lack a compelling purpose [and] would force the government to be more transparent about the reasons for its information gathering activities.").

310. *Id.* at 160–61 (noting the need for courts to "look to whether the information gathering effectively furthers the government's interest, and whether the procedural safeguards and judicial oversight available are sufficient to prevent abuse without rendering the investigation ineffective").

311. *Id.* at 161 (highlighting that a warrant and probable cause requirement would promote particularity, ensure judicial oversight, and guard against post hoc rationalizations for searches); *cf.* Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044 (Colo. 2002) (finding a traditional probable cause warrant insufficient to require a bookstore to turn over its sales records due to the First Amendment concerns implicated).

data mining, argues for a more direct application of the First Amendment.[312] Specifically, she argues that targeted link analyses must be properly justified and narrowly tailored in a First Amendment context.[313] This presents an easy proof for a suspected terrorist, but becomes more difficult for higher order (higher degree of separation) analyses of the individual's network.[314] However, Strandburg is firm that the present standard of mere "relevance," in light of the fact that more link data inevitably yields more accurate results, permits too great an intrusion on tenuously connected individuals.[315] Therefore, she proposes a balancing between the accuracy interest and the degree of imposition on associational rights.[316] Regarding pattern analysis, Strandburg similarly contends that the primary balancing should be between the tailoring of the pattern analysis and the extent of burden on expressive associations.[317]

Looking more generally at the acquisition of data from third-party sources, Strandburg echoes Solove's suggestion that a probable cause warrant be required where a chilling effect is evident.[318] She continues, however, to suggest that in all other cases a court order be required to allow a neutral judge to assess the First Amendment burdens. In agreement with Solove, she suggests that the FISA standard that an investigation not be "conducted solely upon the basis of activities protected by the First Amendment," is wholly insufficient.[319]

Critics, however, contend that expanding the First Amendment into criminal procedure in this manner will handicap criminal investigations that should be permissible. Professor Eugene Volokh points out that motive, an important element in criminal prosecutions, may be inexorably linked to a defendant's expressive associations.[320] Volokh also points out that in light of the prevalence of e-discovery, these protections may make it harder for criminal investigators to obtain information than it would be to obtain the

312. *See* Strandburg, *supra* note 242, at 777 ("Some showing of likelihood that the group is engaged in criminal or terrorist activities should be required for such acquisition in order to demonstrate the requisite government interest in the analysis.").

313. *Id.* at 806 ("[T]argeted link analysis can be employed to investigate the associations surrounding a particular individual or group of individuals who have aroused suspicion in some other way.").

314. *Id.* at 808 (noting that link analyses are unlikely to reveal the associational connections of all but the main suspect).

315. *Id.*

316. *Id.* at 809.

317. *Id.* at 810 (describing the importance of having "sufficient examples of traffic data associated with the particular type of association at issue" to ensure that the pattern can be matched, and the importance of that pattern being unique enough that it will not overlap with protected expressive associations).

318. *Id.* at 812.

319. *Id.* at 812 (describing the FISA standard as "utterly insufficient"); Solove, *supra* note 266, at 168 ("Law enforcement officials will invariably argue that their investigation is based at least in some part on criminal activity. The focus of the inquiry should . . . [be] on whether the investigations have a chilling effect on [First Amendment] activities.").

320. For instance, the most effective method to show the ideological motive of a defendant accused of bombing an abortion provider is probably to investigate the pro-life groups to which the defendant belongs and to speak to group members who know the defendant. *See* Eugene Volokh, *Deterring Speech: When Is It "McCarthyism"? When Is It Proper?*, 93 CALIF. L. REV. 1413, 1444–45 (2005) (discussing investigative techniques to reveal ideological motives).

information through a civil suit.[321]

Another potential problem with the First Amendment protections Strandburg and Solove propose is that they have the potential to create perverse incentives. If expressive associations have special First Amendment protections against criminal investigations, there is a strong likelihood that criminals and terrorists would seek to exploit those protections by communicating through reputable expressive associations.[322] Beyond the immediate harm to the government's interest in crime management, this would also result in the exact effect it tries to avoid: the chilling of speech. An increased presence of criminal elements in expressive associations would discourage membership by creating an apprehension that an individual will be wrongfully linked with, investigated with, and perhaps prosecuted with the criminal elements of the group. However, without implementation it is impossible to know whether the heightened standards Solove and Strandburg propose would provide a sufficient safe harbor to criminal elements to yield this eventuality or whether the harms they would impose would outweigh the benefits of increased protections.

The enforcement of this new First Amendment right would, according to Solove[323] and Strandburg,[324] require the extension of the exclusionary rule to the First Amendment. This expansion would serve as a deterrent to potential overreach during investigations concerning First Amendment activity,[325] and might serve to reduce the chilling effect of surveillance and investigations into First Amendment speech. However, both Strandburg and Solove also note that this approach has disadvantages. Solove readily admits that much of the chilling government surveillance he hopes to guard against occurs outside the criminal context, a problem he hopes will be remedied through the defendant's ability to challenge subpoenas or file civil rights suits.[326] However, such a system is ultimately impractical, because establishing access restrictions protecting First Amendment activity would likely result in increased executive branch efforts to covertly bypass the procedural restrictions.[327] Another

---

321. *Id.* at 1445 ("[I]n civil cases it's routine for litigants to demand a wide range of email and other records from the other side, hoping that these records may contain helpful evidence.").

322. *See* Lachlan Cartwright, *Sex, Drugs and Hiding From the Law at Wall Street Protests*, N.Y. POST (Oct. 10, 2011, 4:00 AM), http://nypost.com/2011/10/10/sex-drugs-and-hiding-from-the-law-at-wall-street-protests/ (explaining how, during Occupy Wall Street, a few criminals melded into the encampments assuming, correctly, that they would be better able to conduct criminal activity from within the crowd.).

323. Solove, *supra* note 266, at 163–64 ("[T]he lack of a textual basis under the First Amendment should not preclude importing warrants, probable cause, the exclusionary rule, and other concepts from the Fourth Amendment . . . . [I]n the event that the government seeks to use information obtained in violation of the First Amendment as evidence in a criminal trial, the exclusionary rule could serve as a viable way to enforce First Amendment protections.").

324. Strandburg, *supra* note 242, at 814 ("The basis for applying an exclusionary rule to evidence obtained in violation of the Fourth Amendment would seem to apply equally well to evidence obtained in violation of the First Amendment's freedom of association protections.").

325. Solove, *supra* note 266, at 164 (contending that the risk of exclusion will incentivize investigators to pursue a judicial determination of probable cause prior to investigating First Amendment activities).

326. *Id.*

327. The NSA's 2006 covert wiretap program readily illustrates that the existing protections are already considered constricting by the intelligence community.

inherent problem, highlighted by Strandburg, is that a First Amendment exclusionary rule could, like the Fourth Amendment exclusionary rule, cause courts to narrow the corresponding constitutional rights out of a desire to convict.[328]

Applied to real world expressive associations, it is unclear if any of these proposals will work. Solove's solution, an independent First Amendment rule of criminal procedure, is ideal from a theoretical perspective, but in reality it will likely have unforeseen consequences and will encourage covert surveillance. It is also unclear whether, as a matter of judicial economics, it is good practice to create a potential First Amendment issue in Fourth Amendment exclusion proceedings. Requiring a judicial inquiry into whether an act fits into the "values" of the First Amendment could well lead to courts narrowing the bounds of "First Amendment values" to secure convictions, especially in light of the fact that the groups most in need of these protections will be those that are the least popular.[329]

Furthermore, it is unlikely that the proposals by Solove and Strandburg would have made any difference for Occupy. Neither would have protected Carlos Miller, who seemingly was singled out for adverse treatment based on public postings. It is uncertain whether either proposal would have protected Malcolm Harris, given that the records sought allegedly pertained to low value speech encouraging actions contrary to police orders and the accompanying transactional data. Furthermore, it is unclear how far a First Amendment procedural rule would extend with regard to transactional data. Transactional data that are wholly unrelated to First Amendment activity can nonetheless chill it. For instance, the police can prove location based on cell phone and credit card records, even if neither device was directly relevant to the defendant's First Amendment activity. It is highly unlikely the government would allow constitutional protections to be applied so broadly.

D. A New Proposal: Recognizing "Unreasonable" Expectations to Create a Statutory Framework

Current Fourth Amendment doctrine (as embodied by the *Katz* reasonable expectation of privacy) and statutory protections governing network surveillance fail to account for the nuance of privacy. The bounds of our expectations of privacy vary based on how many people we tell our secrets to and who they are.[330] Obviously, a secret is the most private if no one knows it. But that does not mean it is not private if it is shared with a best friend. Nor, for that matter, does the secret stop being private if shared with a group of

328. Strandburg, *supra* note 242, at 816.

329. It is well established that First Amendment expression by unpopular groups is often targeted for prosecution. The names of unpopular groups such as the Ku Klux Klan, the Jehovah's Witnesses, the Communist Party, the NAACP, and now the Westboro Baptist Church frequently recur in First Amendment jurisprudence, because the speech of unpopular groups is inherently less valued by society and is therefore more likely to be restricted.

330. *See supra* Part IV.A.

friends, so long as the speaker expects those friends to keep it secret.[331] The more people who know a given fact, the less private that fact becomes until eventually it becomes public.

Associational privacy is similarly nuanced. Group members cannot expect absolute privacy in their associations, at least not the absolute privacy required by *Katz* to establish a "reasonable expectation" of privacy.[332] To be in a group requires other group members, which limits the availability of absolute privacy. Nonetheless, group members do have some expectation of privacy, which the Supreme Court acknowledges through its associational privacy doctrine.[333] The associational privacy doctrine recognizes privacy in membership, a privacy that exists between the extremes of the *Katz* dichotomy and embodies a relational approach to privacy.[334]

Society's reliance on technology and the government's growing access to network information increasingly challenges associational privacy. Although associational privacy has not traditionally been applied to government surveillance activities, technology allows such activities to reveal information—such as memberships, friendships, and attendance at specific events—that is central to associational privacy.[335] Unless checked, this government surveillance will undermine the protections of associational privacy, substantially chilling public discourse. To remedy the threats to associational privacy, it is necessary to understand where the problematic access occurs, what the privacy expectation in that context is, and how legislation can work to counteract the breach of those expectations. Although the *Katz* framework is flawed,[336] it is nonetheless the optimal framework for the proposed reforms to operate within.[337]

The types of access described in this Article result from privacy violations at three levels of a communication: the recipient, the transmitter, and the reconstruction. Access at the recipient level occurs when police examine public content and restricted content they gain access to via deceit. Access at

---

331. *See* Solove, *supra* note 54, at 1177 ("[A]s long as [information] is kept secret, it remains private.").

332. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) (limiting protection to expectations that "society is prepared to recognize as 'reasonable'" and stating that open conversations that may be overheard do not qualify for protection).

333. *See supra* Part II (discussing associational privacy).

334. For a more thorough discussion of relational privacy, see *supra* note 202 and accompanying text.

335. *See generally supra* Part IV.

336. Contemporary critics increasingly argue against the continued use of the "reasonable expectation of privacy" standard. *See, e.g.*, Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CALIF. L. REV. 1593, 1594–98 (1987) (critiquing the "narrow, individualistic conception of privacy" implemented under *Katz* and the resultant neglect of relational privacy considerations); Solove, *supra* note 54, at 1154–57 (arguing for a relational conception of privacy). Some, but not all of their critiques are based on some of the flaws that this Article seeks to address.

337. The breadth of alternatives to *Katz* makes it otherwise impossible to describe universally operable solutions to the problems addressed herein. Moreover, retaining the existing framework allows for gradual changes as opposed to sweeping reform, rendering the proposed solutions more immediately viable. The proposed changes, it should be noted, are shifts in the direction that many privacy scholars believe Fourth Amendment privacy law should move. Therefore, operating within the *Katz* framework is not adverse to the ultimate overhaul of Fourth Amendment privacy protections. *See, e.g.*, Solove, *supra* note 54, at 1151 (proposing the reversal of *Smith v. Maryland* and *United States v. Miller* and the restructuring of the government access to third party records doctrine).

the level of the transmitter occurs when the police demand that third-party service providers turn over content or transactional data. Finally, access at the reconstructive level occurs when the government uses data mining to glean patterns, actions, and associations that the individual has not yet shared with others. Each level involves a different privacy expectation with different theoretical bases, yet each is deserving of some protection under the law.

1. Recipient Level Access

Under *Katz* and the current statutory framework, neither public content nor restricted access content receive any privacy protection. Admittedly, the accessing of publicly available information implicates only a reasonable expectation of insignificance: that the data, though public, are only relevant to the intended audience and that few others will bother to find and view it. The access, via deceit, of a restricted access multi-user communication, however, implicates a different expectation of privacy. When individuals communicate via password-protected forum, restricted access listserv, or private Facebook group or post, they have an expectation of privacy. The privacy right invoked, in the terminology of *Katz*, can be described as a reasonable expectation of good faith: that the members of the limited-access group are all there for a valid purpose and that they will try to respect one another's privacy.[338] The protection of private information is far from absolute in such a setting, but it nonetheless still exists.[339] The traditional balancing between valid police interests and the interests of those engaging in such multi-user limited access venues (such as meetings at union halls) has traditionally been attained successfully due to the economic limits on undercover operations.[340] The Internet, however, removes that check, resulting in excessive usage of deceptive police practices online and, ultimately, the chilling of speech and association.[341]

The proper mechanism for regulating this new, modern phenomenon is one duly deferential to law enforcement purposes: a statutory requirement that before officers may assume a false online identity (except in exigent circumstances or delineated classes of cybercrime case that are investigated primarily via false identity), they be required to certify to a magistrate that they are likely to reveal information relevant to an ongoing criminal investigation and that the investigation is not based on protected First Amendment activities.[342] This standard, at first, appears to run counter to the existing

338. *See generally* Ethan J. Leib, *Friends as Fiduciaries*, 86 WASH. U. L. REV. 665, 687–92 (2009) (highlighting the importance of trust in friendships and fictive friendships).

339. To draw an analogy to a physical context, this expectation of privacy is akin to that which might be had at an Alcoholics Anonymous meeting: there is no absolute guarantee of privacy, but there is an expectation that no one will later use what is said to write a tell-all book.

340. *See* Richard H. McAdams, *The Political Economy of Entrapment*, 96 J. CRIM. L. & CRIMINOLOGY 107, 112 (2005) ("Aside from scandals, undercover operations impose significant costs.").

341. Michael W. Sheetz, *Cyberpredators: Police Internet Investigations Under Florida Statute 847.0135*, 54 U. MIAMI L. REV. 405, 430 (2000) (describing the low costs of Internet investigations).

342. If this standard appears familiar, it is because it is the same standard currently used to obtain a pen register court order.

Fourth Amendment jurisprudence, which makes clear that information wrongfully disclosed based on a false representation is not protected by the Fourth Amendment.[343] It is undisputed that the Fourth Amendment does not presently protect information willingly shared with an informant or an undercover officer.[344] However, search and seizure cases make equally clear that deceit cannot be used to enter private spaces (such as the home) under false pretense,[345] except when those spaces have been converted to criminal purpose and the invitation is extended to further that purpose (i.e., entering a drug den pretending to be a buyer).[346] And when undercover officers are investigating groups holding open meetings while engaged in protected First Amendment activities, they are only required to (1) conduct their investigation in good faith, and (2) adhere to the scope of the defendant's invitation to participation in the organization.[347] The issue, then, becomes a question of how a private online venue is to be treated for Fourth Amendment privacy purposes.

The unique nature of online interaction necessitates the use of a marginally more aggressive framework than that applied to physical surveillance. Access to an individual's friend-only Facebook content or an exclusive forum provides access, not to one conversation, but to all conversations that are occurring and that may occur. A restricted access forum is a semi-private space, much like a church or other association might be. But there are key differences between a church and a limited-access Internet forum.

---

343. *See supra* text accompanying note 195 (discussing the application of the misplaced trust doctrine).

344. *See, e.g.*, United States v. White, 401 U.S. 745, 752–54 (1971) (finding no Fourth Amendment violation in police electronically eavesdropping on a conversation inside the defendant's home through an informant wearing a wire); *but see* Lopez v. United States, 373 U.S. 427, 466 (1963) (Brennan, J., dissenting) (expressing, in a case in which an agent used a wire to record the defendant's attempts to bribe him, the fear that surveillance "makes the police omniscient; and police omniscience is one of the most effective tools of tyranny").

345. Although deception cannot be used to enter a private space where officers lack a warrant or probable cause, it can be used to affect an entry pursuant to a warrant or exigent circumstances where a traditional knock-and-announce entry is not viable.

346. *See, e.g.*, Lewis v. United States, 385 U.S. 206, 211 (1966) ("A government agent, in the same manner as a private person, may accept an invitation to do business and may enter upon the premises [of a home used for business purposes] for the same purposes contemplated by the occupant"); Dietemann v. Time, Inc., 449 F.2d 245, 249 (9th Cir. 1971) (finding that "one who invites another into his . . . office [for a commercial transaction] takes a risk that the visitor may not be what he seems, and that the visitor may repeat all he hears and observes when he leaves" but rejecting the notion that this risk extends to the surreptitious recording and transmission of audio and video footage by an undercover reporter); *see also* State v. Pi Kappa Alpha Fraternity, 491 N.E.2d 1129, 1132 (Ohio 1991) (finding that consent given to state liquor agents, who held themselves out as fraternity alums, to enter a fraternity house during a search for illegal alcohol sales was invalid because it was obtained through deception, and therefore could not have been freely and voluntarily given).

347. *See* United States v. Aguilar, 883 F.2d 662, 705 (9th Cir. 1989) (citing Reporters Comm. v. Am. Tel. & Tel., 593 F.2d 1030 (D.C. Cir. 1978), *cert. denied* 440 U.S. 949 (1979)) (the First Amendment does not afford protection against good faith criminal investigations); *Id.* (citing Pleasant v. Lovell, 876 F.2d 787, 803–04 (10th Cir. 1989)) (the First Amendment requires that undercover informers "adhere scrupulously" to the scope of the invitation). In *Aguilar*, which involved undercover surveillance of several churches by Immigration officials, the Ninth Circuit explicitly warned that "the Supreme Court unmistakably declared that persons have no expectations of privacy or confidentiality in their conversations or relations with other persons, no matter how secretive the setting . . . legitimate law enforcement interests require persons to take the risk that those with whom they associate may be government agents." *Id.* at 703.

Admittedly, the online gatekeeper has less personal contact than the physical gatekeeper, leading one to expect somewhat less privacy in the online sphere.[348] The economics of online surveillance, however, substantially change the calculus. The Supreme Court has made clear that those who choose to associate take the risk that those they associate with may be government agents.[349] But that risk is de minimus—the likelihood that any one person that an individual meets at church or a book club or an Alcoholics Anonymous meeting is a government agent is negligible. The governmental interests at play easily and vastly outweigh the chilling effect such a low likelihood event would impose. The economies of scale available to undercover online investigations greatly increase the likelihood of surveillance to the point where the chilling effect outweighs the governmental interest absent the imposition of minor regulatory measures designed to guard First Amendment activities.

The proposed certification requirement provides a middle ground between the misplaced trust doctrine and First and Fourth Amendment protections. It allows deception in entering Internet forums or restricted-access online venues, but requires a showing of relation to ongoing criminal investigations and good faith (in that the investigation is not based on First Amendment activities). This requirement, at a minimum, ensures that police use of deception to gain access to restricted venues is based on a known link to criminality and not merely on concerns about the sentiments expressed or individuals involved with that venue.[350] To ease some of the burden such a requirement would pose, an exception to the requirement could be made for certain classes of cybercrime cases in which undercover online activity constitutes a primary investigative technique, such as child exploitation cases.[351] This exception works because cybercrime prosecutions rarely overlap with groups at the heart of the associational privacy doctrine's protections and is required due to the necessity of using false identity in these sorts of investigations.[352] Such a standard keeps the increased burden on law enforcement low, but ensures there is a modicum of particularized suspicion and oversight of undercover activities online. Further, it prevents "preventative policing" from becoming a justification for the monitoring of unpopular groups, offering greater protection for their associational privacy.

2. Transmitter Level Access

A higher expectation of privacy exists with respect to access by transmitters. Access by transmitters, through second-degree data acquisition,

348. There are ways to compensate for this, however. It is common for privacy gatekeepers to ask those seeking access to identify themselves and explain why they should be allowed access.

349. *See supra* note 348 and accompanying text.

350. *See generally* Strandburg, *supra* note 242, at 758–61.

351. *See* McAdams, *supra* note 340, at 107–09 (noting that in certain cases it is not desirable to "[b]an all such operations because their benefits sometimes justify their costs").

352. *But see* Aaron J. Burstein, *Amending the ECPA to Enable a Culture of Cybersecurity Research*, 22 HARV. J.L. & TECH. 167, 171 (2008) (noting that "both Congress and the Executive Branch have recently become aware of the need to integrate privacy into cybersecurity policy").

involves third party carriers turning over content and non-content information they possess, an activity the existing statutory framework of the ECPA governs.[353] The ECPA framework, however, is insufficient: it allows far too much access to stored electronic communications and transactional information.[354] The privacy interest in this information also is not absolute, as there is always a risk of it being accessed for network maintenance purposes. But the general understanding of those using electronic resources is that their information is "private" in that it will not be disclosed to others.[355] Again adopting the *Katz* phrasing, this interest could be described as a reasonable expectation of justification in that consumers assume that their communications will only be accessed for valid network maintenance purposes. Thus, although not fully private, communications in this category can be considered fairly private. As has been shown, carrier access can have sizeable chilling effects on association, especially given the lesser requirements to obtain transactional data.[356] However, too high a bar to this kind of information can result, at least on the federal level, in the bypass of the legal framework altogether, which has a far more chilling effect on association.

The reform of the Stored Communications Act to eliminate the 180-day distinction and the incorporation of an exclusionary rule are strong first steps in reforming the problem of carrier access. However, associational privacy requires more: transactional records of non-public information, such as network address, call logs and web histories, and locational data should also be protected by the same standards as content data in all except cybercrime cases.[357] The need for this protection arises both from the wealth of information about one's associations that can be gleaned from this data and from the protections afforded against pre-textual searches by judicial determinations of probable cause. To avoid impeding legitimate law enforcement interests, an exception to the warrant requirement would allow for network address and transaction history to be obtained via subpoena where the request is sufficiently specific in time or scope. Such specificity could be ensured, for instance, by limiting the release of transactional information to a specified temporal window or by only disclosing confirmatory information, thus allowing the police to confirm suspicions but not to gain new information. A similar exception could be drafted to allow the use of relevant transactional information in network-based data mining, under the circumstances discussed infra.

---

353. *See generally supra* Part IV.B.

354. *See supra* Part II.

355. Under the ECPA, it would in fact be illegal to freely disclose to others. *See* 18 U.S.C. § 2511 (2012) (stating that it is unlawful to disclose any electronic communications that were intercepted or that should reasonably been known to have been intercepted).

356. *See generally supra* Part IV.B.

357. Cybercrime cases clearly require a different standard of access. Because the entirety of the crime may well be committed through the Internet, transactional data form the prime investigative tool. Thus, to allow the continued prosecution of cybercriminals, it is necessary to treat physical crimes and cybercrimes differently for purposes of electronic communications privacy.

3. Access at the Reconstructive Level

The most confounding threat to associational privacy comes from the reconstructive potential of data mining. On the one hand, if no wrongly obtained private information enters the data mining process; logic dictates that the output also should not be private. Conversely, the information produced by the data mining process could very well be private; data mining can reveal secretive association and attempts to predict people's future actions. Using the analysis of scattered bits of information, it reconstructs a naked image of the individual and their activities. Clearly, this implicates major concerns for associational privacy.

Each type of data mining requires a distinct approach to privacy protection. Network-based analysis, due to its reliance on transactional data, is best suited to clear regulation. However, network-based analysis is also a vital tool in the war on crime and terrorism, and absolute limits on it would be both unworkable and unenforceable.[358] The ideal system for such regulation would be a variant on the Title III super warrant requiring (1) probable cause to believe evidence of a predicate felony offense will be revealed, (2) that normal investigative techniques are not viable, and (3) that the data mining will be executed with the most possible protection for individual privacy before a suspect's social network could be analyzed. Once the super warrant issues, though, the subsequent acquisition of the data of individuals in the suspect's social network could be governed by subpoenas issued pursuant to the super warrant certifying that there is independent reason to believe the individual in question might be linked to the criminal activity under investigation.

Such a standard recognizes that traditional individualized suspicion is not present in a link-analysis for individuals beyond the target, but that those individuals are nonetheless vital to establishing the whole of the target's networks. Therefore, the standard substitutes the added protections of the super-warrant for individualized suspicions as to subsequent links, whose data would be obtainable via subpoena based on their link to the original target. The addition of the super-warrant's predicate felony requirement serves to balance privacy interests and law enforcement interests by ensuring that the privacy invasion inherent in link analysis only occurs for serious crimes. Although this standard takes the progressive step of treating data mining as a search, it also sacrifices relational privacy and some of the core principles of the Privacy Act of 1974 by providing reduced protection to those linked to a target through their associational ties. This sacrifice is necessary to ensure that, once suspicion as to a target exists, the government can obtain sufficient relational information to perform a link-analysis.[359]

Pattern-based analysis presents a different problem, because it requires

358. *See* POSNER, *supra* note 241, at 143 ("The government has a compelling need to exploit digitization in defense of national security.").

359. This solution is feasible because constitutional associational privacy doctrine does not yet extend to the criminal context. If associational privacy doctrines were expanded or the First Amendment incorporated into Fourth Amendment procedures, this trade-off might not remain viable.

sweeping data access.[360] Pattern-based analysis raises clear concerns under the mosaic theory, as well as a number of process-based concerns. At present, however, the publicly disclosed technology behind pattern-based analysis is still too incomplete to determine how secure or accurate such programs can be. Until such a program is implemented (and its details made public), it is impossible to accurately predict how it will work and what procedures the government will apply to its use. Therefore, despite the strong potential for privacy invasions that chill association, it is necessary to leave this potentially valuable tool (and the jurisprudence surrounding it) with room to mature and develop. Thus, data mining of public information should be allowed to continue with limited judicial constraints until its full scope and application are known.[361] However, statutory protection should exist in the form of mandated standards for accuracy, certainty, and security before data-mined information can be used for investigative purposes. Furthermore, statutory protections should require independent corroborating evidence before suspicion generated by data mining is used to justify an arrest, search, or detention.

These proposals offer one possible option to address the impact online law enforcement activities can have on associational privacy. The key is finding a sustainable balance between privacy and policing interests that will protect associational privacy in an era where, increasingly, technology is integral to association. To do this, it is necessary to look beyond *Katz* and consider the "unreasonable" expectations to constitutional privacy that individuals possess. Particularly, it is necessary to consider at what stage access to private information is gained. Access can originate in the recipient, in the transmitter, and in the individual, and at each stage different conceptions of privacy, and therefore different balances of privacy and security interests, will govern.

VI. CONCLUSION

The rise of networked technology has fundamentally changed the modern world. Technology is inseparably integrated into nearly every facet of our daily lives. This brave, new, and networked world is hailed as promoting the free exchange of ideas, but it also threatens to chill expressive association. It is no longer possible for an expressive association to avoid using technology or to try to restrict the technology use of its members. But technology use brings with it substantial risk of government investigation and surveillance, chilling associational activity and undermining the protections afforded by the right to associational privacy. If the values embodied in the associational privacy doctrine are to remain protected, more robust regulation of how and when the

360. *See generally supra* Part IV.C.

361. In light of the developing mosaic theory jurisprudence, however, it seems likely that the proper means of regulation will be the expansion of the Fourth Amendment to govern certain kinds of pattern-based data-mining. This would have the added benefit of preserving non-police uses of data mining under the special needs search exception to the Fourth Amendment, avoiding the First Amendment issue that selective regulation of data mining created in *Sorrell*.

government may gain access to network information will be needed. We must abandon our binary conception of privacy and instead embrace and protect "unreasonable" expectations of privacy.

Reforming the ECPA is a valuable first step in this direction, but more steps are needed. As a society, we must have a free and frank conversation about how to balance security interests, privacy interests, and constitutional rights. If the government's security interests are not sufficiently protected, the procurement of electronic data will occur extra-judicially and the harm will remain. If rights to privacy and association are not protected, speech will be chilled and valuable components of our civil discourse will be lost. The past years have demonstrated some ways that this chilling can occur. However, as new and novel technologies come into use, this impact can only worsen. If associational privacy is to endure, the standards governing electronic investigations must be modernized and revised with a specific focus towards protecting the communications of groups.

The question that truly highlights the importance of this issue is a simple one: could the Civil Rights movement have survived today? Would the conveniences of the Internet have facilitated its efforts, or would technology have better allowed the police departments of the American South to silence activists and quell protests? And ultimately, are we willing to risk the outcome of these questions? Technology has changed both society and the very nature of expressive association. If the concept of associational privacy, as boldly envisioned in *NAACP*, is to endure, its sweep must expand to guard against the chilling effect of government use of technology and electronic data. The Arab Spring and American Autumn showed that the Internet can amplify popular sentiments to the benefit of democracy. Without sufficient safeguards, this newfound tool of democracy will become a tool of suppression, and the voices of America's minority groups will be lost from the national discourse.