2012

Expectations of Privacy in Social Media

Stephen E Henderson, *University of Oklahoma College of Law*

EXPECTATIONS OF PRIVACY IN SOCIAL MEDIA

*Stephen E. Henderson**

This Article, which largely tracks my remarks at the Mississippi College School of Law Social Media Symposium, examines expectations of privacy in social media such as weblogs (blogs), Facebook pages, and Twitter tweets. Social media is diverse and ever diversifying, and while I address some of that complexity, I focus on the core functionality, which provides the groundwork for further conversation as the technology and related social norms develop. As one would expect, just as with our offline communications and other online communications, in some we have an expectation of privacy that is recognized by current law, in some we have an expectation of privacy that should be recognized by current law, and in some we have no legitimate expectation of privacy. The Article begins with a short (and personal) history of social media and then discusses the theory of information privacy, after which follows an explanation of, and then application of, the governing constitutional law. This is an area in which statutes should, and to some extent do, expand upon the constitutional floor, and the Article ends with a consideration of those statutes and needs for improvements therein, including via statutory frameworks like that recently adopted by the American Bar Association.

I. A BRIEF (AND PERSONAL) HISTORY OF SOCIAL MEDIA

For most of my life, I suppose I have been a relatively early adopter of computer technology, and because my personal history is relevant to that of social media and provides a bit of perspective and color, I comment briefly upon it here. If you are a reader who could not care less, however, you can safely skip this introduction and move immediately to the next section introducing information privacy.

I was nine years old when my father, a physicist at a national laboratory, purchased our first home computer. The Heathkit/Zenith Z-100 cost an outrageous sum compared to computers today, but I was dutifully impressed with its three-color display on which he programmed a card matching game in Z-Basic, and on which I began programming more ballistic alternatives.[1] Of course, nine seems positively old compared to my two-year-old son taking to my BlackBerry and iPad, but just as school used to

* Professor of Law, The University of Oklahoma College of Law. Yale Law School (J.D., 1999); University of California at Davis (B.S., 1995). I am grateful to the Mississippi College Law Review, and in particular to Editor-in-Chief Justin Ponds, for the invitation to participate in the Social Media Symposium and for the exceptional hospitality during that event.

1. For information on the Heathkit system, see Herb Johnson, *Intro to Heath/Zenith Z-100 Systems*, RETROTECHNOLOGY.COM, http://www.retrotechnology.com/herbs_stuff/z100.html (last updated Aug. 30, 2011); *Heathkit/Zenith Z-100/110/120*, OLD-COMPUTERS.COM, http://www.old-computers.com/museum/computer.asp?c=261 (last visited May 15, 2012).

be uphill both ways, in my youth it was hard work to make a computer do something fun.

Indeed, at times it was work to make a computer function at all. When I was fourteen and programming for my Pascal course, it could be a bit noisy. The fan on my dad's "laptop," an orange-screened Toshiba T3100, had failed, and so we resorted to using the fan from a hair blow dryer to cool the computer.[2] It is hard to imagine similarly resuscitating an electronic device in today's "replace it" culture. The following summer, I was programming as New Mexico's representative at the Department of Energy's High School Science Student Honors Program in Supercomputing, and I have a wonderful picture of myself as a young-looking fifteen-year-old leaning on a Cray-2 at Lawrence Livermore National Laboratory in outrageously loud shorts and a t-shirt. The processing power of that computer is now matched by that of an iPad 2,[3] but it was the fastest computer in the world between 1985 and 1990.[4] That same summer I began programming fluid flow simulations at Los Alamos National Laboratory in Fortran on networks of Sun computers, and also began to participate in social media.

Of course, the social media of the 1980s and early 1990s—known as Bulletin Board Systems (BBSes)—bears little resemblance to the social media of today.[5] Because the network connections, topping out with 28.8 thousand bit-per-second modems, were thousands, or tens of thousands, times slower than those we currently enjoy, the purpose was not to download significant content. But like the modern fare, BBSes allowed interactive online dialogue and entertainment. There were good jokes posted on the local BBS humor message board and a respectable multi-user text game in which you were permitted one move a day, and I was duly impressed with the graphics some folks created using only ASCII characters.[6] I, not being so creative, just stole someone's Bart Simpson likeness as my own signature, foreshadowing in a microcosm the "sharing" that would come with the World Wide Web (hereinafter "WWW").

During college I interacted with the nascent WWW, which we accessed via the first browser. Called Mosaic, it was the forerunner of today's

2. For information on the Toshiba system, see *T3100 Series*, OLD-COMPUTERS.COM, http://www.old-computers.com/museum/doc.asp?c=917&st=1 (last visited May 15, 2012); *Toshiba T-Series T3100*, TOSHIBA-EUROPE.COM, http://www.toshiba-europe.com/bv/computers/products/notebooks/t3100/index.shtm (last visited May 15, 2012).

3. *See* John Markoff, *The iPad in Your Hand: As Fast as a Supercomputer of Yore*, N.Y. TIMES (May 9, 2011, 3:45 PM), http://bits.blogs.nytimes.com/2011/05/09/the-ipad-in-your-hand-as-fast-as-a-supercomputer-of-yore/.

4. *See Cray-2*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Cray-2.

5. For more information, see *Bulletin Board Systems*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Bulletin_board_system (last updated June 12, 2012).

6. ASCII stands for American Standard Code for Information Interchange, and includes ninety-five printable characters that one would expect to find on a computer keyboard. *See ASCII*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/ASCII.

Firefox, Internet Explorer, Safari, and their kin.[7] And then came the heyday of America Online, and there were the first massively multiplayer games in MUDs and MOOs.[8] So I suppose my reliance upon computers and computer networking has been gradual, but today, I—like most of us—am an addict. I rely heavily upon the Internet for communication, for learning, for banking and other commerce, and for entertainment. I still love the feel of a paper book but also love being able to look up words with a single tap and to quickly explore their derivation and nuance. And it is hard to imagine consulting a paper encyclopedia or dictionary. I expect my dictionary to be able to speak to me, so I can get by without ever learning just how an upside-down "e" is to be pronounced.

Not only does this establish that online social media is not quite as new as it might seem, but, hopefully, that I have a little bit of geek credibility. Not as much as some, of course, but nor am I a Johnny-come-lately when it comes to communications and interactions via computer networks. Unfortunately, that is where my "good news" ends. I do not post any pictures to flickr. I do not have videos on YouTube. I lack a profile on LinkedIn. I do not blog. I do not tweet. Most distressing, perhaps, is that it was not until being invited to participate in a social media symposium that I finally joined the 845 million of you who have a Facebook page.[9] And even then, being a privacy nut I immediately turned off most all of the features, so I cannot claim the full experience. So I am fairly conversant with, but not a full participant in, social media.[10] But hopefully being conversant, and having spent considerable time in the last ten years thinking about privacy, merits something to say.

II. INFORMATION PRIVACY

There is some presumably small segment of society that at least claims not to care for privacy, perhaps best represented by Scott McNealy's famous (or infamous) words: "You already have zero privacy—get over it."[11]

7. *See Mosaic (web browser)*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/Mosaic_(web_browser) (last updated May 30, 2012).

8. *See MUD*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/MUD (last updated May 15, 2012); *see also MOO*, WIKIPEDIA.ORG, http://en.wikipedia.org/wiki/MOO (last updated June 16, 2012).

9. *See The Value of Friendship*, THE ECONOMIST, Feb. 4, 2012, at 23. As THE ECONOMIST points out, were Facebook a country, it would be the world's third most populous, behind only China and India. *Id.* It is astounding that fully one seventh of the world's population could soon be on Facebook. Its usage statistics are similarly impressive: "Every day 250m photos are uploaded to the site. One out of every seven minutes spent online is on Facebook, according to comScore, a research firm." *Id.*

10. According to a recent survey of more than 1,000 pregnant women, over half planned to record the birth via social media as it takes place. *See* Heidi Stevens, *Social Media Giving Birth to New Generation of Parents-to-Be*, CHI. TRIB., Dec. 28, 2011, *available at* http://articles.chicagotribune.com/-28//fam-1227-pregnant-trend-20111227_1_social-media-social-networking-healthy-pregnancy. A part of me has to wonder how many of them have given birth before, because there are things said in the delivery room that are best left in the delivery room. In all seriousness, whatever the merits, tweeting a birth just is not my world.

11. Jeffrey Rosen, *The Eroded Self*, N.Y. TIMES, April 30, 2000, *available at* http://www.nytimes.com/library/magazine/home/20000430mag-internetprivacy.html.

And there is some segment of commerce that seems to regularly disrespect privacy, perhaps best captured by Conan O'Brien's December 7, 2011, dig at Facebook founder and CEO Mark Zuckerberg: "Someone hacked into Facebook and leaked Mark Zuckerberg's private photos. When Zuckerberg realized someone had showed a blatant disregard for his privacy, he hired them."[12] But for most, privacy is an important value, and that has been true historically, at least in representative governments.

Studies by Alan Westin have confirmed a relationship between political philosophy and privacy throughout Western civilization:

> In classic or contemporary authoritarian societies, where public life is celebrated as the highest good and the fulfillment of the individual's purpose on earth, the concept of legally or socially protected privacy for individuals, families, social groups, and private associations is rejected as hedonistic and immoral. It is also seen as politically dangerous to the regime. Thus traditional authoritarian societies create procedures to watch and listen secretly to elite groups, and modern totalitarian governments keep extensive records on individuals, families, and all associational activities.
>
> In contrast, both classic republics and modern democracies regard the private sector as a valuable force for social progress and morality and thereby seek to foster individualism and freedom of association. In the modern constitutional democracies, the public order, government, is seen as a useful and necessary mechanism for providing services and protection; but constitutional governments are expressly barred by bills of rights and other guarantees of civil liberty from interfering with the citizen's private beliefs, associations, and acts, except in extraordinary situations and then only through controlled procedures.[13]

12. *The Best of Late Nite Jokes*, NEWSMAX.COM, (Dec. 7, 2011), http://www.newsmax.com/Jokes/644.

13. Alan F. Westin, Historical Perspectives on Privacy: From the Hebrews and Greeks to the American Republic 4-5 (unpublished manuscript, on file with the author) (presented and distributed at the 2009 Privacy Law Scholars Conference and quoted with permission). Westin later summarizes as follows:

> In the authoritarian tradition—exemplified by Sparta, the Roman Empire, 17–19th century European nation-state monarchies, and contemporary dictatorships—the exercise of extensive powers to compel disclosure and to conduct population-wide surveillance has been and remains an essential part of the political culture and governmental system.
>
> By contrast, in what I would call the constitutional tradition—typified by the Hebrews, Periclean Athens, the Roman Republic, the English parliamentary system, the American republic, and modern democratic nations—basic limits were and are placed on the powers of authorities to put individuals or groups under surveillance or to compel extensive disclosure of 'sensitive' personal information. . . .
>
> . . . [I]t is fair to say that no political system with a reputation for liberty in its time failed to provide important legal and social limits on surveillance by authorities. And, no regime that is judged to have been authoritarian and despotic failed to deploy forces of surveillance and enforced disclosure as regular instruments of state, or fails to do so today.

Similarly, privacy scholar Daniel Solove concludes that "[p]eople have cared about privacy since antiquity."[14]

As for America, Westin identifies the Republic of 1790–1820 as "the first 'modern' privacy system":

> Of course, the word "privacy" does not appear in the U.S. Constitution or the Bill of Rights. However, the Founding Fathers gave the American Republic all the key components of a broad-scale privacy regime—fundamental constitutional guarantees against unreasonable search and seizure; rejection of compulsory testimony and self-incrimination; and privacy for association and religion in the First Amendment. Privacy rights in first-class mail and in Census enumeration were written into early federal legislation or regulation, and the privacy of letters was given judicial protection against private publication against the wishes of the writer or recipient. And, by rejecting internal government passports, elaborate government record-keeping, government spy networks, and other apparatuses of late 18th and early 19th century royal surveillance, the American republic nurtured socio-political traditions of individual autonomy and non-surveillance that gave daily vitality to the early constitutional and legal rules.[15]

The First Amendment's freedom of speech protects privacy in the form of anonymous speech,[16] and the Supreme Court has interpreted the Bill of Rights to include substantive due process protection for private decisions.[17] A number of state constitutions explicitly protect privacy.[18] And the law has not been stagnant but instead in every category has adapted to the changing circumstances of over two hundred years.

Nonetheless, it can be difficult to define privacy, at least in part because we use the one term to describe multiple values.[19] There is surely a difference between the right of bodily autonomy on the one hand, and the right to private communications on the other, yet both are often described as rights of "privacy." When we are discussing social networking, we are

Id. at 9.

14. DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 4 (2011).

15. Westin, *supra* note 13, at 9–10.

16. *See* McIntyre v. Ohio Election Comm'n, 514 U.S. 334, 342 (1995).

17. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 485–86 (1965) (recognizing marital privacy); Whalen v. Roe, 429 U.S. 589, 599 (1977) (recognizing information privacy).

18. *See* ALASKA CONST. art. I, § 22; ARIZ. CONST. art. II, § 8; CAL. CONST. art. I, § 1; FLA. CONST. art. I, § 23; HAW. CONST. art. I, § 6; ILL. CONST. art. I, § 6; LA. CONST. art. I, § 5; MONT. CONST. art. II, § 10; S.C. CONST. art. I, § 10; WASH. CONST. art. I, § 7.

19. *See generally* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY (Ferdinand David Schoeman ed., 1984); DANIEL J. SOLOVE ET AL., PRIVACY, INFORMATION, AND TECHNOLOGY 35–36 (2006); Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087 (2002); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

not directly interested in bodily autonomy (what might be termed "decision privacy"); we are interested in "information privacy." But even with information privacy there are competing notions and definitions, and some argue it is impossible to encapsulate the right in any single formulation.[20] If so, perhaps privacy is essentially contested—most everyone agrees that we should have it, but has different ideas of just what it is. For the most part, however, I think the right to information privacy can be encapsulated by the ability to control what information about you is conveyed to others and for what purposes.

Such a "control" notion of information privacy is widely associated with Westin, whose seminal 1967 work defines privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[21] Similarly, Charles Fried described privacy as "that aspect of social order by which persons control access to information about themselves."[22] One of the key themes in Samuel Warren and Louis Brandeis's seminal 1890 article was an individual's "right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[23] So I consider information privacy the right to control what information about you is conveyed to others and for what purposes.

Andrew Taslitz has explained why this control matters:

> Identity is complex; different circumstances reveal different aspects of our nature. Each of us wears many masks wherein each mask reflects a different aspect of who we really are. We do not want our entire natures to be judged by any one mask, nor do we want partial revelations of our activities to define us in a particular situation as other than who we want to be. In short, we want to choose the masks that we show to others; any such loss of choice is painful, amounting almost to a physical violation of the self. When we are secretly watched, or when information that we choose to reveal to one audience is instead exposed to another, we lose that sense of choice.[24]

Similarly, Benjamin Goold explains as follows:

20. *See, e.g.*, SOLOVE, *supra* note 14, at 24 ("Privacy . . . is too complex a concept to be reduced to a singular essence. It is a plurality of different things that do not share one element in common but that nevertheless bear a resemblance to each other.").

21. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967). A Westlaw search for the latter half of Westin's quotation (beginning with "to determine for themselves") in the "allcases" database shows it has been relied upon in over thirty court decisions, including decisions by supreme courts. *E.g.*, U.S. Dep't of Justice v. Reporters Comm. for Freedom of Press, 489 U.S. 749, 764, n.16 (1989); Shaktman v. State, 553 So. 2d 148, 150 (Fla. 1989).

22. Charles Fried, *Privacy*, 77 YALE L.J. 475, 493 (1968).

23. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890).

24. Andrew E. Taslitz, *The Fourth Amendment in the Twenty-First Century: Technology, Privacy, and Human Emotions*, 65 LAW & CONTEMP. PROBS. 125, 131 (2002).

> Although it is possible to talk of privacy as simply the right to be "let alone," its status as a right derives primarily from its relationship to ideas of autonomy and self-determination. Privacy is valuable because it is necessary for the proper development of the self, the establishment and control of personal identity, and the maintenance of individual dignity. Without privacy, it not only becomes harder to form valuable social relationships – relationships based on exclusivity, intimacy, and the sharing of personal information – but also to maintain a variety of social roles and identities. Privacy deserves to be protected as a right because we need it in order to live rich, fulfilling lives, lives where we can simultaneously play the role of friend, colleague, parent and citizen without having the boundaries between these different and often conflicting identities breached without our consent.[25]

So information privacy is fundamental to our personhood. In the words of information security specialist Bruce Schneier, "Privacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect."[26] We develop as mature human beings by having many different zones of privacy: some thoughts we experiment upon only by ourselves, some we share only with spouses or very close confederates, some we share with church congregants, some with professional colleagues. Because who we are is a complex amalgamation of all of these different "masks," to use Taslitz's term, it is a very real harm to our personhood when this structure is betrayed. Information conveyed to an unintended recipient does not enjoy the context it would have with an intended recipient and thus is likely to be misunderstood or misconceived. Information privacy is therefore an important right, and the pithy "if you have nothing to hide, you have nothing to fear" is deeply flawed.[27] And privacy is not extinguished by the sharing of information with select others, as privacy is not secrecy. In the words of Justice Thurgood Marshall, "Privacy is not a discrete commodity, possessed absolutely or not at all."[28] Instead, the divisible nature of privacy is fundamental to its worth.

---

25. Benjamin Goold, *Surveillance and the Political Value of Privacy*, 1 AMSTERDAM L. FORUM 3, 3-4 (2009).

26. Bruce Schneier, *The Eternal Value of Privacy*,WIRED.COM, (May 18, 2006), http://www.wired.com/politics/security/commentary/securitymatters/2006/05/70886/. Schneier continues:

> For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that—either now or in the uncertain future—patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable.

Id.

27. *See* SOLOVE, *supra* note 14, at 21–32.

28. Smith v. Maryland, 442 U.S. 735, 749 (1979) (Marshall, J., dissenting). *See also* Lewis R. Katz, *In Search of a Fourth Amendment for the Twenty-first Century*, 65 IND. L.J. 549, 564–66 (1990) (explaining this concept); Burrows v. Super. Ct., 529 P.2d 590, 596 (Cal. 1974) (applying the concept to

Although perhaps not essential to the current project of examining privacy in social media, it is worth noting a common mistake, which is to consider "privacy versus security." This false dichotomy presents a unitary dial: if we turn up privacy, we get less security, and if we turn down privacy, we get more security.[29] Security and privacy are viewed as a zero-sum tradeoff. In the both humorous and telling words of Daniel Solove, this false dichotomy has become so ingrained "that people seem to associate being inconvenienced and being intruded upon with security. So if the government wants to make people feel more secure, all it needs to do is make them feel more uncomfortable and exposed."[30]

Bruce Schneier is a frequent critic of such "security theater,"[31] and he corrects this misperception: "Too many [people] wrongly characterize the debate as 'security versus privacy.' . . . Liberty requires security without intrusion, security plus privacy."[32] In other words, there is no doubt that there is a relation between security and privacy, in that a change to one will sometimes affect the other.[33] But sometimes it is possible to increase security without decreasing privacy, and sometimes a decrease to privacy leads to no meaningful increase in security. Our goal as a nation has always been not merely to be safe, but to be *secure*, and such security requires both safety and privacy. Thus, perhaps in this context it is most helpful to articulate that *safety* and privacy are related and can affect one another, but *security* requires an ample measure of both.

III. The Fourth Amendment and Social Media

There is no doubt that law enforcement finds relevant some of what we do online. The Electronic Privacy Information Center, or EPIC, has obtained information on a Department of Homeland Security initiative that would monitor social media, gathering information from "online forums, blogs, public websites, and messages boards" and disseminating it to "federal, state, local, and foreign government and private sector partners."[34] The Federal Bureau of Investigation has solicited proposals for

recognize privacy in a bank account); People v. Jackson, 452 N.E.2d 85, 89 (Ill. App. Ct. 1983) (same); State v. McAllister, 875 A.2d 866, 874 (N.J. 2005) (same); People v. Chapman, 679 P.2d 62, 67 (Cal. 1984) (applying the concept to recognize privacy in telephone dialing information); People v. Sporleder, 666 P.2d 135, 141 (Colo. 1983) (same); People v. DeLaire, 610 N.E.2d 1277, 1282 (Ill. App. Ct. 1993) (same); State v. Hunt, 450 A.2d 952, 955-56 (N.J. 1982) (same); State v. Boland, 800 P.2d 1112, 1117 (Wash. 1990) (applying the concept to recognize privacy in trash collection); State v. Morris, 680 A.2d 90, 95 (Vt. 1996) (same).

29. I believe it may have been from Marc Rotenberg, Executive Director of the Electronic Privacy Information Center, that I first heard this precise analogy.

30. Solove, *supra* note 14, at 35.

31. *See* Bruce Schneier, *Beyond Security Theater*, 427 New Internationalist 10 (2009), *available at* http://www.schneier.com/blog/archives/2009/11/beyond_security.html.

32. Schneier, *supra* note 26.

33. In the words of the Eleventh Circuit, "[T]he Fourth Amendment embodies a value judgment by the Framers that prevents us from gradually trading ever-increasing amounts of freedom and privacy for additional security." Bourgeois v. Peters, 387 F.3d 1303, 1312 (11th Cir. 2004).

34. *EPIC v. Department of Homeland Security: Media Monitoring*, epic.org, http://epic.org/foia/epic-v-dhs-media-monitoring/default.html (last visited May 15, 2012).

developing a similar system.[35] While perhaps merely the twenty-first century equivalent of the national security traffic analysis that has long taken place in communications networks, some will see echoes of THE ONION's humorous proposition that Facebook was a CIA creation.[36]

More specifically (and seriously), Google's "Transparency Report" chronicles how many data requests Google receives from government agencies and courts around the world.[37] In the first half of 2011, there were 5,950 American criminal justice requests for user data relating to 11,057 accounts, and Google complied with these requests 93% of the time.[38] So that is some 12,000 requests per year, or thiry-two per day, to this single—albeit enormous—online provider, and this does not include those requests made pursuant to a National Security Letter or Foreign Intelligence Surveillance Act court order.[39]

Such law enforcement requests are potentially governed by the Fourth Amendment, which provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[40] As Jed Rubenfeld has argued, that specific language—that we have a right to be *secure* in our persons, houses, papers, and effects—is indeed perhaps a particularly good way to describe the right, because government surveillance and other acquisition of information affects our sense of security.[41] But when the Supreme Court looks to whether there has been a search or seizure it does not define either by notions of "security."

The Court recently reaffirmed that there are two tests for what constitutes a search. The first is when "[t]he Government physically occupie[s] private property for the purpose of obtaining information."[42] Thus, the Fourth Amendment regulates police installation of a GPS device on a target's vehicle in order to track its movements,[43] and it would regulate the search of a target's computer. The second conception—relevant to obtaining information from a social media provider—is government conduct

35. *See* Jim Giles, *FBI Releases Plans to Monitor Social Networks*, NEWSCIENTIST, (Jan. 25, 2012), http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html.

36. *See CIA's 'Facebook' Program Dramatically Cut Agency's Costs*, THEONION.COM, http://www.theonion.com/video/cias-facebook-program-dramatically-cut-agencys-cos,19753/ (last visited May 15, 2012). In case you are wondering, Agent Mark Zuckerberg's codename is "The Overlord."

37. *Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/ (last visited May 15, 2012).

38. *Transparency Report: United States*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/ (last visited May 15, 2012).

39. *See* Ryan Singel, *U.S. Requests for Google User Data Spike 29 Percent in Six Months*, WIRED.COM, (Oct. 25, 2011 11:07 AM), http://www.wired.com/threatlevel/2011/10/google-data-requests (noting the report's limitations).

40. U.S. CONST. amend. IV.

41. *See* Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 119–122 (2008).

42. United States v. Jones, 132 S. Ct. 945, 949 (2012).

43. *See id.*

that intrudes upon a reasonable expectation of privacy.[44] There is much about this second definition that remains poorly defined,[45] but for our purposes there is instructive case law, as explained below.

The Court has also applied two conceptions of seizure. But unlike those for search, which can be seen as complementary, Paul Ohm has developed the contradiction in the Court's two lines of seizure jurisprudence.[46] In a series of eavesdropping cases in the 1960s and 1970s, the Court repeatedly asserted, essentially without analysis, that the capture of intangible communications constitutes both a Fourth Amendment search and seizure. First, in the false-friend case of *Hoffa v. United States*, the Court concluded that "the protections of the Fourth Amendment are surely not limited to tangibles, but can extend to oral statements."[47] But because it resolved the case on what would become the infamous third party doctrine, the *Hoffa* Court did not distinguish between search and seizure of such intangibles.[48]

The next year, in *Katz v. United States*, the Court held that recording one end of a telephone call implicates both rights.[49] But although the Court labeled the eavesdropping a "search and seizure" throughout its opinion, it never explained why seizure was implicated.[50] That same year, in *Berger v. New York*, the Court repeatedly described the capture of telephone conversations as constituting a seizure, again without analysis.[51] Ten years later, in *United States v. New York Telephone Company*, the Court articulated that recording the digits dialed on a telephone constitutes both a search of the telephone and a seizure of the information so obtained.[52] However, once again the Court made no justification for this assertion, and made no attempt to define "seizure."[53]

44. *See id.* at 950, 952 ("[A]s we have discussed, the *Katz* reasonable-expectation-of-privacy test has been added to, not substituted for, the common-law trespassory test.").

45. *See, e.g.*, Stephen E. Henderson, *Nothing New Under the Sun? A Technologically Rational Doctrine of Fourth Amendment Search*, 56 MERCER L. REV. 507, 517 n.54 (2005) [hereinafter *Nothing New*] (noting the Court's waffling between normative and empirical notions).

46. *See* Paul Ohm, *The Olmsteadian Seizure Clause: The Fourth Amendment and the Seizure of Intangible Property*, 2008 STAN. TECH. L. REV. 2, 17–31(2008).

47. 385 U.S. 293, 301 (1966).

48. *See id.* at 302–03; *Nothing New*, *supra* note 45, at 518–20.

49. 389 U.S. 347, 353 (1967) ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

50. *See id.* at 354–57. This lack of explanation is not too surprising when one considers that the entire *Katz* majority opinion is essentially devoid of careful legal analysis. It is from Justice Harlan's concurrence that we derive a legal standard, namely the "reasonable expectation of privacy criterion" for what constitutes a search. *See id.* at 361 (Harlan, J., concurring).

51. 388 U.S. 41, 59–60 (1967).

52. 434 U.S. 159, 169 (1977) ("[Federal Rule of Criminal Procedure 41(b)] is broad enough to encompass a 'search' designed to ascertain the use which is being made of a telephone suspected of being employed as a means of facilitating a criminal venture and the 'seizure' of evidence which the 'search' of the telephone produces.").

53. Instead, the Court limited itself to explaining why a Rule of Criminal Procedure authorizing a warrant to "search for and seize any . . . property" is broad enough to permit a warrant authorizing a

It is easy to see why the interception of private communications constitutes a search under the modern reasonable expectation of privacy framework: both empirically and normatively, persons have an expectation of privacy in their conversations, and when the government surreptitiously accesses those conversations, it invades that reasonable expectation. But while the Supreme Court interception cases consistently also label the recording a seizure, there is no meaningful consideration of why that is the case. Instead, in every opinion the Court focused solely on determining whether the government could undertake the challenged conduct which it had so quickly labeled a "search and seizure."

The modern definition of seizure is typically associated with *United States v. Jacobsen*, in which the Court defined a seizure as "some meaningful interference with an individual's possessory interest" in property.[54] At first glance, this might seem in conflict with the eavesdropping cases, as listening in upon a conversation or discovering the telephone digits dialed does not interfere with the conversants' possession of that information. The Supreme Court, without acknowledging the eavesdropping cases, took just such a view in *Arizona v. Hicks*.[55]

In *Hicks*, officers executing an emergency aid search of a home picked up stereo equipment and recorded the serial numbers thereon.[56] Although the Court determined that such movement did constitute a Fourth Amendment search, it concluded that recording the serial numbers was no seizure:

> We agree [with the government] that the mere recording of the serial numbers did not constitute a seizure. To be sure, that was the first step in a process by which respondent was eventually deprived of the stereo equipment. In and of itself, however, it did not "meaningfully interfere" with respondent's possessory interest in either the serial numbers or the equipment, and therefore did not amount to a seizure.[57]

Not only does this fail to address the contrary view in the eavesdropping cases, but it assumes a narrow definition of "possession." It may be that "[i]n the whole range of legal theory there is no conception more difficult than that of possession,"[58] but the first two definitions in Black's law dictionary are as follows:

> 1. The fact of having or holding property in one's power; the exercise of dominion over property.

pen register. *Id.* at 170 ("Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses recorded by pen registers as well as tangible items.").

54. 466 U.S. 109, 113 (1984).

55. 480 U.S. 321 (1987).

56. *Id.* at 323.

57. *Id.* at 324.

58. BLACK'S LAW DICTIONARY 1201 (8th ed. 2004) (quoting JOHN SALMOND, JURISPRUDENCE 285 (Glanville L. Williams ed., 10th ed. 1947)).

> 2. The right under which one may exercise control over something to the exclusion of all others; the continuing exercise of a claim to the exclusive use of a material object.[59]

The concept of "dominion" and "exclusive control" are just as relevant to intangible things as to tangible. Indeed, as explained above, the entire notion of information privacy arguably rests on the right and ability to control information. Thus, if the government obtains information that was previously in one's exclusive control, it seems it has meaningfully interfered with a possessory interest. It is unclear, however, whether the Court will so recognize.

Whatever the precise definitions of search and seizure, the Court has articulated this general principle:

> [T]he Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[60]

This limitation makes eminent sense, in that police should not have to be the only ones to avert their eyes. If you tape a message on a window visible from the street, or place a pie to cool or a plant to grow there, a police officer driving or walking by is free to give it a look. According to the control theory of information privacy, you have chosen to share that information. Whereas if you carry any of those items on your person in public, but in an opaque container, the item remains private, and police must act accordingly.

Some social media is exposed to the public, such as an open-to-the-world blog. It is not reasonable to expect privacy when one publishes something to all comers. So there would be no Fourth Amendment restraint on police obtaining the content of such a blog, either by bringing up the site themselves or via the third party hosting that content.[61] The same holds true for a Facebook wall which the user leaves open to the public, YouTube videos left open to the public, and flickr pictures left open to the public. And the same holds true for tweets from a public account, meaning one for which the user does not restrict followers. Since any private person can obtain these things without restraint, the police can as well.[62]

59. *Id.*

60. Katz v. United States, 389 U.S. 347, 351 (1967).

61. *See* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (finding no reasonable expectation of privacy in personal computer files accessible to anyone using the peer-to-peer file trading network); United States v. Gines-Perez, 214 F. Supp. 2d 205, 224–26 (D.P.R. 2002) (finding no reasonable expectation of privacy in a photograph available on a publicly accessible website).

62. Because such information is already public, there can similarly be no civil liability for republication under the privacy tort of public disclosure of private facts. *See* Moreno v. Hanford Sentinel, Inc., 172 Cal. App. 4th 1125, 1129–30 (2009). On the other hand, if private information is placed online in

On the other end of the spectrum, there are functions on social media sites that are the antithesis of public, meaning it is immediately apparent that one retains a reasonable expectation of privacy.[63] For example, Facebook messages, in which one user communicates directly with another, are either analogous to a telephone conversation if in real time, or are analogous to e-mail and postal mail if asynchronous.[64] We retain a reasonable expectation of privacy in telephone conversations,[65] postal letters,[66] and e-mail,[67] and thus similarly retain an expectation of privacy in these messages.[68] Of course, once a physical letter is received, it is the recipient's expectation of privacy that becomes relevant, and no longer the sender's.[69] But as to a copy retained by an intermediary such as a social media service provider, both the sender and recipient should retain a reasonable expectation of privacy. If anything, a service provider's legitimate interest in a message decreases once it has reached its intended destination, as that transmission was the sole purpose of the bailment.

Thus, we have two poles: there is no reasonable expectation of privacy for public posts, but there is a reasonable expectation of privacy, and indeed a warrant requirement, for instant messaging and e-mail. What of information "between" these poles? We can classify that information into three categories. There is "subscriber information," which the social media provider requires in order to provide any service. This would include identifying information (subscriber name, contact information, method of payment, and screen name), account type, and the length of service. There is "transactional information," which the social media provider requires to facilitate desired communications. Transactional information would include to whom a subscriber communicates, and when, thus including a list of Facebook friends. Finally, there are "non-public communications," such

such a public format, it can constitute that tort even if not many persons actually peruse it. *See* Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 42–45 (Minn. Ct. App. 2009).

63. One could argue these functions are not, therefore, *social* media, but they are popular functions on some social media sites and therefore deserving of consideration.

64. *See Privacy for Messages*, FACEBOOK, http://www.facebook.com/help/?page=1680442699233 34 (last visited May 15, 2012) ("[Y]our conversations within Facebook [Messages] are absolutely private. Only you and the person you're messaging can view the contents and history of your conversation, and stories about your messages will never appear in the news feed.").

65. *See Katz*, 389 U.S. at 353; Berger v. New York, 388 U.S. 41, 51 (1967).

66. *See Ex parte* Jackson, 96 U.S. 727, 733 (1877) (protecting letter via warrant requirement); Walter v. United States, 447 U.S. 649, 654–55 (1980) (same where carried by private carrier); United States v. Jacobsen, 466 U.S. 109, 114 (1984) (same).

67. *See* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) ("Given the fundamental similarities between email and traditional forms of communication, it would defy common sense to afford emails lesser Fourth Amendment protection."). A panel of the Eleventh Circuit briefly held to the contrary but then withdrew that opinion. *See* Rehberg v. Paulk, 598 F.3d 1268, 1281–82 (11th Cir. 2010), *vacated*, 611 F.3d 828, 846–47 (2010).

68. For a contrary view that does not address my (or others') previous work on the limitations of the Fourth Amendment third party doctrine, see Junichi P. Semitsu, *From Facebook to Mug Shot: How the Dearth of Social Networking Privacy Rights Revolutionized Online Government Surveillance*, 31 PACE L. REV. 291, 329, 350–51 (2011).

69. *See* United States v. King, 55 F.3d 1193, 1196 (6th Cir. 1995).

as Facebook wall posts to a limited audience of friends,[70] YouTube videos to a limited audience,[71] flickr pictures to a limited audience,[72] and protected tweets to a limited following.[73] There are of course other features on Facebook and similar sites, and new ones being developed all of the time. But many merely provide various means of communicating some type of information to a limited audience, and thus can be analyzed within this simplified structure.

In order to determine the Fourth Amendment rule for these categories we require the so-called third party doctrine, a Supreme Court jurisprudence that grew out of a very stingy reading of the *Katz* language regarding disclosures to the public.[74] In a nutshell, "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by [the third party] 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."[75] In other words, you retain no reasonable expectation of privacy in information you convey to a third party, with respect to the government obtaining it from that third party. Thus, there is no Fourth Amendment restriction on law enforcement access to bank records residing with a bank[76] or to phone dialing records residing with a phone company.[77] I, like many others, think this doctrine is wrongheaded and especially destructive given modern social norms and technologies.[78] Encouraged by some recent developments, I have already written its obituary.[79] Most recently,

70. *See How Do I Control Who Can See and Post to My Wall*, FACEBOOK, http://www.facebook.com/help/?faq=163475490382977#How-do-I-control-who-can-see-and-post-to-my-Wall? (last visited May 15, 2012).

71. *See Private Videos and How to Share Them*, YOUTUBE, http://support.google.com/youtube/bin/answer.py?hl =en&answer=157177 (last visited May 15, 2012).

72. *See Public/Private*, FLICKR, http://www.flickr.com/help/privacy (last visited May 15, 2012).

73. *See FAQs About Following*, TWITTER, http://support.twitter.com/articles/14019-what-is-following (last visited May 15, 2012); *About Public and Protected Tweets*, TWITTER, http://support.twitter.com/articles/14016 (last visited May 15, 2012).

74. *See Nothing New*, *supra* note 45, at 518–21; Stephen E. Henderson, *Learning from All Fifty States: How To Apply the Fourth Amendment and Its States Analogs To Protect Third Party Information from Unreasonable Search*, 55 CATH. U.L. REV. 373, 376–79 (2006) [hereinafter *Learning*].

75. United States v. Miller, 425 U.S. 435, 443 (1976).

76. *See id.* at 437.

77. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

78. *See, e.g.*, *Nothing New*, *supra* note 45, at 521–44; *Learning*, *supra* note 74, at 379–86, 390–93; CHRISTOPHER SLOBOGIN, PRIVACY AT RISK: THE NEW GOVERNMENT SURVEILLANCE AND THE FOURTH AMENDMENT 151–64 (2007); Susan W. Brenner & Leo L. Clarke, *Fourth Amendment Protection for Shared Privacy Rights in Stored Transactional Data*, 14 J.L. & POL'Y 211 (2006); Russell D. Covey, *Pervasive Surveillance and the Future of the Fourth Amendment*, 80 MISS. L.J. 1289 (2011); Susan Freiwald, *Cell Phone Location Data and the Fourth Amendment: A Question of Law, Not Fact*, 70 MD. L. REV. 681 (2011) [hereinafter *Cell Phone Location*]; Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3 (2007) [hereinafter *First Principles*]; Jack I. Lerner & Deirdre K. Mulligan, *Taking the "Long View" On the Fourth Amendment: Stored Records and the Sanctity of the Home*, 2008 STAN. TECH. L. REV. 3 (2008); Katherine J. Strandburg, *Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change*, 70 MD. L. REV. 614 (2011); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 647 (2011).

79. Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. 39 (2011) [hereinafter *Timely Demise*].

Justice Sotomayor questioned the doctrine in her concurrence in *United States v. Jones*.[80] But unless and until five members of the Supreme Court so hold, it remains the federal constitutional law, and thus it is necessary to apply the doctrine to our categories of social media information.

For subscriber information and transactional information, there is no Fourth Amendment protection.[81] Just as with banking records and telephone dialing records, the third party service provider uses this information in order to provide the desired service, and thus it falls squarely within the third party doctrine. In order to determine the rule for friend wall posts and protected tweets, it is helpful to first return to our "protected" end of the spectrum—Facebook messages. I have asserted that there is a reasonable expectation of privacy by analogy to telephone conversations and postal mail, but how does this work with the third party doctrine? The Court has actually never made it clear, but the rule must be what I have termed a "limited" third party doctrine: one retains no reasonable expectation of privacy in information provided *for a third party's use*.[82] This is the only way to reconcile there being no protection for telephone dialing information (provided for the company's use in facilitating the calls) with there being protection for telephone conversations (for which the company is a mere conduit or bailee). Thus, as to friend wall posts, protected tweets, and similarly limited communications, there is a Fourth Amendment expectation of privacy.[83]

But there are further complications. What of information that was once publicly available but is no longer? A person might post something to a blog but then later remove it. Or a third party might post something to its public website but then remove it. According to the third party doctrine, law enforcement can access that information without restraint from any person who read the entry and chooses to reveal its content or who

80. United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotamayor, J., concurring).

81. *See* United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) (holding there is no reasonable expectation of privacy in e-mail transactional information and in Internet protocol addresses of websites visited); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) (same); United States v. Bynum, 604 F.3d 161, 164 (4th Cir. 2010) (holding there is no reasonable expectation of privacy in Internet subscriber information); United States v. Hambrick, No. 99–4793, 2000 WL 1062039, at *3–4 (4th Cir. Aug. 3, 2000) (same); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) (same), *vacated on other grounds*, 648 F.3d 1 (1st Cir. 2011); State v. Mello, 27 A.3d 771, 775 (N.H. 2011) (same under state constitution). *See also* United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008) (gathering cases and concluding that "[e]very federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation"). *Cf.* State v. Reid, 194 N.J. 386, 399 (2008) (holding there is a reasonable expectation of privacy in subscriber information under state constitution).

82. *See Nothing New*, *supra* note 45, at 526–27. Courts in other contexts have recognized a reasonable expectation of privacy in something left with a bailee. *See* United States v. Most, 876 F.2d 191, 198 (D.C. Cir. 1989) (bag left with store clerk); United States v. Barry, 853 F.2d 1479, 1481–84 (8th Cir. 1988) (luggage left with airline); United States v. Presler, 610 F.2d 1206, 1213–14 (4th Cir. 1979) (briefcase left with friend).

83. In the context of privacy torts, courts have recognized a privacy interest despite limited disclosure to a circle of friends. *See* Steven D. Zansberg & Janna K. Fischer, *Privacy Expectations in Online Social Media—An Emerging Generational Divide?*, 28-Nov Comm. Law. 1, 28 (2011).

retained a copy and chooses to hand it over. I agree with this result, because as Christopher Slobogin and Eugene Volokh have argued, that person has autonomy and free speech interests in choosing to share information that overrides the possible privacy interests of the original source.[84]

What of law enforcement access from an employee of the service provider who happens to recall its content or—much more likely—who can obtain it from company records? I think there is a reasonable expectation of privacy in this instance and, therefore, such access should be regulated by the Fourth Amendment. That something was once public does not necessarily defeat a claim of privacy. To use an analogy, criminal justice records are public, but when certain records are expunged, they are no longer publicly available and for good reason.[85] The European Commission's proposed data protection regulations thus include a "right to be forgotten" that would require third parties to assist in the removal of online information.[86] One can imagine an especially strong case for privacy: perhaps the post was in error and was taken down after only a few seconds, and the error was on the part of the service provider rather than the true party in interest with respect to privacy, the subscriber or customer.

Thus, I argue that there is a reasonable expectation of privacy in once-public, now deleted social media content. Would it then be appropriate to require law enforcement to obtain a warrant to access all such content? I think that might be appropriate where the content is very personal (e.g., health information), and it was only ever publicly accessible on account of service provider mistake. But I do not think that would be ideal where the content is less personal and was intentionally made publicly available by the user. So finding a reasonable expectation of privacy is only half the battle (if that). According to the Fourth Amendment, all government access must be reasonable, and a warrant can only issue upon probable cause. But the Amendment does not dictate that reasonable access must always be via a warrant.

A court might have to confront this—and other—difficult issues as a matter of Fourth Amendment law, but it would be much better for a legislature to make an initial attempt. Daniel Solove has explained that:

84. *See* Christopher Slobogin, *Transaction Surveillance by the Government*, 75 MISS. L.J. 139, 185–86 (2005); Stephen E. Henderson, *Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too*, 34 PEPP. L. REV. 975, 1011–1012 (2007) (expounding on Slobogin's principle); Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000). This same reasoning applies to content previously disclosed to only a limited number of persons.

85. My thanks to Christopher Slobogin for suggesting this analogy.

86. *See Commission Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) of 29 Nov. 2011,* EPIC.ORG, art. 15 at 47–48, http://epic.org/privacy/intl/EU-Privacy-Regulation-29-11-2011.pdf (last visited May 15, 2012).

> In an ideal world, government information gathering would be regulated by a comprehensive statutory regime. Courts would analyze whether the rules in this statutory regime met basic Fourth Amendment principles rather than craft the rules themselves. A pronouncement as short and vague as the Fourth Amendment best serves as a guidepost to evaluate rules, rather than as a source of those rules.[87]

This does not mean, however, that a court can dodge its constitutional responsibility if a legislature has failed to act. Solove continues:

> But a comprehensive statutory regime to regulate government information gathering does not yet exist. Statutes regulate government information gathering in isolated areas, but there is no all-inclusive regime. For better or worse, the Fourth Amendment has been thrust into the role of the primary regulatory system of government information gathering. Until there is a substitute, we should treat the Fourth Amendment as the regulatory system it has been tasked with being. If legislatures respond with rules of their own, courts should shift from crafting the rules to evaluating the rules made by legislatures.[88]

Justice Alito, writing in concurrence for himself and three others, made much the same point in *United States v. Jones*:

In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative. A legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way.

To date, however, Congress and most States have not enacted statutes regulating the use of GPS tracking technology for law enforcement purposes. The best that we can do in this case is to apply existing Fourth Amendment doctrine and to ask whether the use of GPS tracking in a particular case involved a degree of intrusion that a reasonable person would not have anticipated.[89]

Ideally, statutes will govern access to social media information, which statutes the courts will review for compliance with the requirements of the Fourth Amendment. Not only can legislatures more consistently approach the myriad of differing circumstances under which law enforcement accesses different types of information, but they can regulate the decisions of private social media providers. Whereas the Fourth Amendment limits only government conduct, and therefore places no limitation on disclosure

87. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1515 (2010).

88. *Id.*

89. United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring) (internal citations omitted).

by private entities on their own initiative, statutes can thoughtfully regulate both.

IV. Statutes and Social Media

As to legislation regulating law enforcement access to social media information, we are as unlucky as a person in luck could be. We are in luck, because there are such statutes, in particular three federal laws: the Wiretap Act (Title III),[90] the Pen Trap Act,[91] and the Stored Communications Act.[92] We are unlucky, because when it comes to modern communications like social media, they are real dogs. The technologies and norms of social media have evolved rapidly, whereas the statutory structure—and much of the particular language—has remained constant. The Stored Communications Act ("SCA") was enacted in 1986, during the era of the Bulletin Board System.[93] The World Wide Web did not yet exist; it would be proposed in late 1990. And despite several rounds of amendments, the basic structure of the SCA has remained static.

The distribution of work between the three statutes is fairly clear if, remarkably, it has to be inferred in the case of the Wiretap Act.[94] If the issue is one of prospective, real time surveillance, then the place to look is the Wiretap Act for the contents of communications and the Pen Trap Act for non-content "dialing, routing, addressing, or signaling information."[95] If the issue is retrospective, historic surveillance, then the place to look is the Stored Communications Act. So if law enforcement wants to obtain Facebook wall posts or messages or Twitter tweets as you send or receive them, it is a Wiretap Act issue. If law enforcement wants to obtain that same information later via Facebook or Twitter records, it is a Stored Communications Act issue.

90. Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. §§ 2510–2522 (2006).

91. Pen Registers and Trap and Trace Devices, 18 U.S.C. §§ 3121–3127 (2006).

92. Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701–2711 (2006).

93. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 980–81 (C.D. Cal. 2010) (gathering precedent applying the SCA to bulletin board systems).

94. The Wiretap Act governs "intercepts," where intercept is defined as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). Since gaining possession or control can constitute an "acquisition," it would seem that an Internet Service Provider faxing or emailing content in response to a Title III warrant could constitute an "intercept." Courts interpret the statute, however, to regulate only acquisition contemporaneous with its transmission. *See, e.g.*, Fraser v. Nationwide Mut. Ins. Co., 352 F.3d 107, 113 (3d Cir. 2003) ("Every circuit court to have considered the matter has held that an 'intercept' . . . must occur contemporaneously with transmission."). Where the technology of the Internet, with its store and forward router delay, has potentially caused this to be less clear, courts have taken a practical interpretation rather than an overly technical one. *See, e.g.*, United States v. Councilman, 418 F.3d 67, 79–80 (1st Cir. 2005) (en banc) (finding provider's automatic forwarding of e-mail to constitute an intercept); O'Brien v. O'Brien, 899 So. 2d 1133, 1136–37 (Fla. Dist. Ct. App. 2005) (finding use of screen capture spyware on a home computer to constitute an intercept under an analogous Florida provision).

95. 18 U.S.C. § 3127(3). *See also* 18 U.S.C. §§ 2510(8), 2511(1)(c).

As a matter of privacy, this distinction makes no sense. Nowhere in the theory of information privacy as control over information is there a temporal limitation. Somebody who considers their Facebook messages to be private wants to control the messages dissemination as they are sent, the next day, the next week, and the next year. The right and ability to control what information about you is conveyed to others and for what purposes does not diminish in value over time. Indeed, in at least some instances the privacy interest may be greatest with respect to very old information that would be especially harmful given its lack of context and current relevance. As discussed above, it is privacy that allows us to mature and develop, and that ability is threatened by the "outing" of former selves. Hence, properly interpreted, the Fourth Amendment recognizes no such temporal difference. Unfortunately, the current statutory framework does.

Thus, the Sixth Circuit has held unconstitutional a provision of the Stored Communications Act that poorly protects the privacy of stored e-mail communications,[96] and many have called for increasing the relatively weak protections provided to historic information.[97] Moreover, the statutory protections depend upon confusing and often unhelpful distinctions such as whether information is deemed to be in "electronic storage,"[98] which is defined in a far from common-sense manner,[99] and whether a provider is an "electronic communication service" or "remote computing service."[100] As to opened Gmail (Google email), for example, Google might be neither since the provider accesses content to deliver targeted advertising.[101]

As for disclosure on private initiative, meaning without government involvement, employers and other service providers that do not provide service "to the public" are entirely unrestrained.[102] Since social media sites are available to all comers—meaning they do provide service "to the public"—they typically cannot disclose posts, tweets, and chats on pain of civil liability, including not being permitted to respond to civil subpoenas requesting such contents.[103] They face no similar restraint on disclosing

96. *See* United States v. Warshak, 631 F.3d 266, 283–88 (6th Cir. 2010).

97. *See, e.g.*, *Cell Phone Location*, *supra* note 78; *First Principles, supra* note 78; Lerner & Mulligan, *supra* note 78; Slobogin, *supra* note 84; Strandburg, *supra* note 78.

98. *See* 18 U.S.C. § 2703 (2006)

99. *See* 18 U.S.C. § 2510(17).

100. *See* 18 U.S.C. §§ 2703(a)–(b). Many will also fault the Stored Communications Act for failing to have a suppression remedy. *See* 18 U.S.C. § 2708. Even the Wiretap Act lacks a suppression remedy for intercepted "electronic communications." *See* 18 U.S.C. § 2515 (providing suppression only for "oral" and "wire" communications). But suppression of evidence is always controversial, even for constitutional violations. *See* JOSHUA DRESSLER & ALAN C. MICHAELS, UNDERSTANDING CRIMINAL PROCEDURE VOLUME 1: INVESTIGATION 354–366 (5th ed. 2010).

101. *See*18 U.S.C. § 2510(17) (providing a temporal limitation on "electronic storage"); 18 U.S.C. § 2703(b)(2)(B) (limiting protection to information held or maintained "solely for the purpose of providing storage or computer processing services.").

102. *See* 18 U.S.C. § 2702 (only restricting those providing service "to the public").

103. *See* 18 U.S.C. §§ 2702(a)–(b); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 976–91 (C.D. Cal. 2010); *In re* Subpoena Duces Tecum to AOL, L.L.C., 550 F. Supp. 2d 606, 609–12 (E.D. Va. 2008); *May I Obtain Contents of a User's Account from Facebook Using a Civil Subpoena?*, FACEBOOK,

transactional and subscriber information to anyone other than the government.[104]

While these specific statutes are entirely too confusing and require substantive reform, legislatures would also benefit from a greater perspective. Sectoral, content-specific regulations make sense, but they should be considered under a larger umbrella that promotes consistent and thoughtful regulation. Surely there are principles that are applicable whether a legislature is considering law enforcement access to bank records, social media records, or medical records. Rather than proceed in an entirely ad hoc fashion, decision makers should begin with a set of first principles that provide a framework for producing sensible and consistent sectoral legislation.

For five years, I have been part of an effort to develop such a framework, the first of its kind, and on February 6, 2012, the American Bar Association House of Delegates adopted our black letter standards on Law Enforcement Access to Third Party Records.[105] They will be published with detailed commentary, and hopefully much more will be written about them elsewhere. It is a very positive initial step. We now have a framework courts, legislatures, and administrative agencies can use in making the difficult determinations of how best to regulate law enforcement access to information in order to account for the needs of law enforcement and the interests of privacy, freedom of expression, and social participation.

V. Conclusion

As is typically the case, social media is not as novel as many think it to be. Its computer origins stretch back as long as several decades, and—as the original moniker of "bulletin board systems" makes clear—its offline equivalents extend far beyond that. It is nonetheless remarkable that a seventh of the world's population might soon be using a single online social media resource, and the amount of information that resides with third party social media providers is expanding dramatically, along with other types of third party information. Since information privacy is a fundamental principle of human development and dignity that has been acknowledged by all modern democracies, thoughtful and careful regulation of government access is a critical issue. On the one hand, access to such

http://www.facebook.com/help/search/?q=civil+subpoenas (last visited May 15, 2012). The Stored Communications Act has no bearing on access to emails residing on a personal computer and further does not prevent a court from ordering a party to litigation to either (1) him or herself request the information from his or her service provider, thereby falling under a § 2702(b) consent exception, or (2) provide his or her login information, such that an opposing party can look at the site. So long as the requested information is relevant, courts in civil discovery adopt one of these options. *See, e.g.*, Largent v. Reed, No. 2009-1823 (Pa. Ct. C.P. Nov. 7, 2011) (requiring plaintiff to disclose login information and to not change it for 21 days thereafter), *available at* http://www.theemployerhandbook.com/.pdf; Thayer v. Chiczewski, 2009 WL 2957317, at *6–7 (N.D. Ill. Sept. 11, 2009) (relying on party consent).

104. *See* 18 U.S.C. §§ 2702(a)(3), (c)(6).

105. *See Criminal Justice Standards on Law Enforcement Access to Third Party Records*, ABA, http://www.americanbar.org/groups/criminal_justice/policy/standards/law_enforcement_access.html (last visited May 15, 2012).

records is necessary not only for the prevention and detection of traditional crimes but also to prevent and detect private access that is itself harmful, such as identity theft and computer hacking. On the other hand, law enforcement access implicates information privacy and American norms of limited government and principles of freedom of speech and association.

Fortunately, even with the *unfortunate*—and hopefully temporary—limitations of the Fourth Amendment third party doctrine, there is constitutional privacy protection for social media contents that are not disseminated to the public. Constitutional protection of transactional information, however, does require reformulating that doctrine. This should be both a constitutional and legislative priority, because just as one reasonably expects privacy in telephone dialing records, one reasonably expects privacy in online transactional information such as the Internet protocol addresses involved in Web browsing and in records pertaining to online communications. Scholars have noted and considered the protection of such information under the First Amendment's freedom of association,[106] and courts have recognized that such First Amendment rights should inform the expectation of privacy analysis.[107]

There will be reasoned disagreements on precisely what restrictions should be required before law enforcement can access particular information, resulting in different rules in different jurisdictions. Subject to a federal constitutional floor, this makes good sense and is to be encouraged. But rather than rely entirely upon ad hoc sectoral consideration, legislatures and other decision makers can use the framework provided by the ABA Criminal Justice Standards on Law Enforcement Access to Third Party Records to coherently regulate access to different types of third party information, including social media information.

106. *See* Peter Swire, *Social Networks, Privacy, and Freedom of Association: Data Protection vs. Data Empowerment* __ N.C. L. REV. __ (forthcoming 2012); Katherine Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 (2008).

107. *See, e.g.*, Amazon.com, L.L.C. v. Lay, 758 F. Supp. 2d 1154 (W.D. Wash. 2010) (rejecting government subpoena of expressive records); *In re* Grand Jury Investigation of Possible Violation of 18 U.S.C. § 1461, 706 F. Supp. 2d 11, 16–23 (D.D.C. 2009) (same); *In re* Grand Jury Subpoena to Amazon.com Dated August 7, 2006, 246 F.R.D. 570, 572–74 (W.D. Wis. 2007) (same). For other sources courts look to in finding a Fourth Amendment reasonable expectation of privacy, see *Timely Demise*, *supra* note 79, at 42 n.26.