Vanderbilt Journal of Entertainment & Technology Law

Volume 14
Issue 3 *Issue 3 - Spring 2012*

Article 3

2012

Virtual Blinds: Finding Online Privacy in Offline Precedents

Allyson W. Haynes

Virtual Blinds: Finding Online Privacy in Offline Precedents

Allyson W. Haynes[*]

ABSTRACT

A person in a building shows a desire for privacy by pulling her blinds shut or closing her curtains. Otherwise, she cannot complain when her neighbor sees her undressing from the window, or when a policeman looks up from the street and sees her marijuana plants. In the online context, can we find an analogy to these privacy blinds? Or is the window legally bare because of the nature of the Internet?

This Article argues that by analyzing the privacy given to communications in the offline context, and in particular, by analyzing case law recognizing privacy in an otherwise public place when the individual engages in affirmative efforts to ensure her privacy, the law can find a sensible foundation for recognizing privacy online. This Article proposes a framework that incorporates the following factors in the reasonable expectations of privacy context. First is the existence of a user agreement or employer policy governing the use of the specific communication mechanism or providing for monitoring of that use. Second is the extent to which third parties have access to or protect the communications. Third is the notice given to the user of the user agreement, employer policy, or practice of giving access to or protection from third parties. Finally, the fourth factor is the availability and use of privacy-enhancing controls which increase the likelihood of the communication being protected from disclosure to people other than the chosen recipient(s), including but not limited to (a) passwords, (b) encryption technology, (c) network configuration, and (d) privacy settings limiting disclosure to certain people.

Courts can adapt this test to a civil tort or Fourth Amendment context, to employment and non-employment cases, and to statutory

---

 Associate Professor of Law, Charleston School of Law. The Author wishes to thank Daniel J. Solove for his helpful comments and insights. The Author also would like to thank Elizabeth Moore, Charleston School of Law, JD 2011, for her valuable research assistance.

privacy claims. It is a logical evolution from the practical factors that courts have looked at in offline cases—like closing doors and securing lockers—and it is consistent with the growing weight of authority that finds a reasonable expectation of privacy in online communications where the Internet user avails herself of privacy-ensuring measures.

TABLE OF CONTENTS

Communication and socializing in general in our society now take place largely on the Internet. We send and receive email, post information to websites, share files, and use online social networks on a daily basis. These methods have replaced more traditional media. But privacy law has not kept pace with this technological trend. In Fourth Amendment, privacy torts, and federal statutory contexts, courts have struggled with the application of privacy concepts to online disclosures. This Article argues that, by analyzing the privacy given to communications in the offline context, particularly by analyzing case law recognizing privacy when the individual engages affirmative efforts to ensure her privacy, or denying such a right where the individual fails to do so, the law can find a sensible foundation for recognizing privacy online.

This Article proposes a framework that incorporates the following factors in the reasonable expectations of privacy context: (1) the existence of a user agreement or employer policy governing the use of the specific communication method or providing for monitoring of that use, (2) the extent to which third parties receive access to or protect the communications (whether part of a policy or not), (3) the notice given to the user of the user agreement, employer policy, or practice of giving access to or protection from third parties, and (4) the availability and use of privacy-enhancing controls (including but not limited to passwords, encryption technology, network configuration, and privacy settings limiting disclosure to certain people).

Part I discusses the tangled web of privacy law, as well as some of the rich scholarship describing privacy's importance to society. Because so much communication takes place via the Internet, some sense of online privacy is vital. While it is obvious that a person has no reasonable expectation of privacy in the contents of a comment, photograph, or video posted on the World Wide Web, there are contexts in which Internet communications should receive privacy protection. These contexts include communications via email and postings on limited-access websites and online social networks.

Part II looks at privacy offline, where the law has traditionally focused on the distinction between public and private communications. The precedent supports finding a limited reasonable expectation of privacy in both common law and Fourth Amendment contexts where disclosure occurs in a public place, but the individual makes affirmative efforts to ensure privacy. This is critical for the transition to the Internet, where the distinction between public and private is problematic for technical reasons, including the necessity of third-party disclosure.

Part III applies this precedent to the online context. Here, many courts have given too little privacy protection to

communications, finding waivers of protection based on entrenched notions of privacy as tantamount to secrecy. Instead, courts should give effect to individual efforts to ensure their privacy despite the Internet medium, as in the offline context. Many courts have applied this reasoning to cases involving email. While some cases have found otherwise, this Article argues that there should be a privacy interest in email even after it has arrived at its recipient's inbox. In addition, courts should extend privacy protection to other disclosures online, including some information disclosed on social networks, depending on the extent to which the user employs affirmative privacy-enhancing controls.

Part IV proposes a framework for analyzing reasonable expectations of privacy on the Internet. This framework balances factors including the existence of user agreements or employer policies providing for privacy of the communications, the notice of those policies given to the user, the availability of privacy-enhancing controls, and the user's affirmative engagement of such controls. Courts can adapt this test to a civil tort or Fourth Amendment context, to employment and non-employment cases, and to statutory privacy claims. It is a logical evolution from the factors that courts have looked at in offline cases, and it is consistent with the growing weight of authority that finds a reasonable expectation of privacy in online communications where the Internet user avails herself of privacy-ensuring measures—the digital equivalent of curtains, doors, and locks.

Part V looks ahead at the changes taking place within online social networks (OSNs) in terms of privacy settings and other user controls. Application of the proposed balancing framework to communications within online social networks will allow the law to keep pace with the evolution of the use of the Internet for communications and socializing purposes. It will also recognize that user-activated controls are an important element of the analysis of a reasonable expectation of privacy in online disclosures.

I. THE IMPORTANCE OF A RIGHT TO PRIVACY IN ONLINE DISCLOSURES

Underlying this Article's search for a coherent analysis of online privacy interests is the belief that some level of privacy in Internet communications is essential to contemporary society. The US Supreme Court noted in the recent case of *City of Ontario v. Quon* that, because new technology renders more pervasive certain methods of communication, it also increases the need for recognition of privacy

rights in those communications.[1] While the Court assumed without deciding that the plaintiff government employee had a reasonable expectation of privacy in text messages sent and received on a government-provided pager, the Court acknowledged that changes in technology and in society's use of that technology would affect "workplace norms, and the law's treatment of them"[2]:

> Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.[3]

The "pervasive" nature of Internet use is similarly pushing boundaries and societal norms in terms of privacy expectations. As online communications become ubiquitous, the law should revisit expectations of privacy.

Privacy is difficult to define,[4] but essential to society.[5] Professor Daniel J. Solove of George Washington University Law School refers to privacy as a "mosaic," as it underlies "tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law."[6] This Article focuses on the privacy of communications,[7] and how common-law tort theories, statutory provisions, and the Fourth Amendment protect them.[8] This analysis also includes some recent case law in the context of discovery of online communications, a new hotbed for privacy issues.[9]

---

1. City of Ont. v. Quon, 130 S. Ct. 2619, 2629-30 (2010).

2. *Id.* at 2623.

3. *Id.* at 2630.

4. *See* Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 424-25 (1980).

5. *See, e.g.*, Daniel J. Solove, *Conceptualizing Privacy*, 90 CALIF. L. REV. 1087, 1090-91 (2002) (noting the difficulties in conceptualizing privacy using common requisite denominators and instead advocating a concept based on "family resemblances").

6. Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393, 1430 (2001).

7. While remedying online invasions of privacy is very important, that is not the focus of this Article. Instead, it focuses on the necessity of individuals to be confident in the privacy of some communications, without the law deeming those communications necessarily public because they were made online.

8. While there are obvious differences between common-law tort principles, Fourth Amendment protections, and statutory provisions, the analysis of privacy overlaps. *See* Sanders v. Am. Broad. Cos., 978 P.2d 67, 74 n.3 (Cal. 1999) (citing Mancusi v. DeForte, 392 U.S. 364, 369 (1968)) (recognizing distinctions between employees' expectations of privacy in tort and Fourth Amendment contexts, but noting that the Supreme Court has analogized the situations as well).

9. *See* Ryan A. Ward, Note, *Discovery Facebook: Social Network Subpoenas and the Stored Communications Act*, 24 HARV. J.L. & TECH. 563 (2011).

As eminent scholars have established, privacy of communication is essential to free speech and self-expression,[10] to encouragement of diversity,[11] to facilitation of relationships,[12] and to the formation of personhood or personality.[13]

Many of the activities that privacy enables now take place via the Internet. Rather than regular mail, we use email. In fact, 92 percent of adult Internet users use email,[14] which translates to more than 225 million people,[15] or 71 percent of the entire US population.[16] Rather than telephone conversations or get-togethers, we have online chatting and Facebook. A recent survey shows that 65 percent of online adults, or half of all adults in the United States, use social networking sites.[17] That is more than double the percentage who

---

10. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 990-92 (2003); *see* Josh Blackman, *Omniveillance, Google, Privacy in Public, and the Right to Your Digital Identity: A Tort for Recording and Disseminating an Individual's Image over the Internet*, 49 SANTA CLARA L. REV. 313, 325-27 (2009) (arguing that privacy protections promote free speech and expression).

11. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2398 (1996) ("[S]trengthening privacy protections would seem to foster diversity, by reducing the private cost of 'abnormal' behavior."); *see id.* at 2416 ("There are also dynamic benefits to a legal regime that protects privacy, including the willingness of people to engage in activities that they would not in the absence of anonymity, the reduction of expensive extralegal precautions, and the reduction of wasteful expenditures on reputation-enhancement needed to correct misapprehensions caused by disclosure of true but incomplete information.").

12. JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 8 (2000) ("Privacy protects us from being misdefined and judged out of context in a world of short attention spans, a world in which information can easily be confused with knowledge. True knowledge of another person is the culmination of a slow process of mutual revelation.").

13. *See* Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 963 (1989) (suggesting privacy torts safeguard general "civility rules" and uphold "social personality" as opposed merely to individual injuries); *id.* at 1010 ("[W]e are thus led to attempt to rationalize the value of privacy, to discover its functions and reasons, to dress it up in the philosophical language of autonomy, or to dress it down in the economic language of information costs. But this is to miss the plain fact that privacy is for us a living reality only because we enjoy a certain kind of communal existence. Our very 'dignity' inheres in that existence, which, if it is not acknowledged and preserved, will vanish, as will the privacy we cherish." (footnote omitted)).

14. KRISTEN PURCELL, PEW RESEARCH CTR., SEARCH AND EMAIL STILL TOP THE LIST OF MOST POPULAR ONLINE ACTIVITIES 2 (2011), *available at* http://www.pewinternet.org/~/media//Files/Reports/2011/PIP_Search-and-Email.pdf.

15. *See Internet Users*, U.S. CENT. INTELLIGENCE AGENCY, https://www.cia.gov/library/publications/the-world-factbook/fields/2153.html (last visited Jan. 20, 2011) (noting that the United States had 245 million Internet users in 2009).

16. According to the latest US Government Census figures, there are over 313 million people in the United States. *U.S. World & Population Clocks*, U.S. CENSUS BUREAU, http://www.census.gov (last visited Feb. 28, 2012).

17. *65% of Online Adults Use Social Networking Sites*, PEW RESEARCH CTR. (Aug. 26, 2011), http://pewresearch.org/pubs/2088/social-networking-sites-myspace-facebook-linkedin.

reported social networking site usage in 2008.[18] Being online is a daily necessity for most Americans, both socially and economically, and the Internet's prevalence will continue to grow.[19]

The US Court of Appeals for the Sixth Circuit recently recognized that, "like the telephone earlier in our history, email is an ever-increasing mode of private communication, and protecting shared communications through this medium is as important to Fourth Amendment principles today as protecting telephone conversations has been in the past."[20] Also, the rapid rise of online social networking (among older adults as well as young people)[21] as a means to keep up with both close ties and more distant ones,[22] suggests that OSNs, too, are an ever-increasing mode of shared communications.[23]

Thus, it is essential that the law allow some kind of private space for online communications, depending on the context. As in other areas of the law, the move to the online context is better understood by a close examination of the offline context.[24] Part II

---

18. *Id.*

19. Janna Quitney Anderson & Lee Rainie, *Millennials' Likely Lifelong Online Sharing Habit*, PEW RESEARCH CTR. (July 9, 2010), http://pewresearch.org/pubs/1660/internet-experts-say-aging-millennials-will-continue-per ("In a survey about the future impact of the internet, a solid majority of technology experts and stakeholders said the Millennial generation will lead society into a new world of personal disclosure and information-sharing using new media. These experts said the communications patterns 'digital natives' have already embraced through their use of social networking technology and other social technology tools will carry forward even as Millennials age, form families and move up the economic ladder.").

20. Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) (en banc), *vacated*, 532 F.3d 521 (6th Cir. 2008).

21. Lee Rainie et al., *Social Networking Sites and Our Lives*, PEW RESEARCH CTR. (June 16, 2011), http://pewresearch.org/pubs/2025/social-impact-social-networking-sites-technology-facebook ("[T]he average age of adult-SNS [social networking service] users has shifted from 33 in 2008 to 38 in 2010."). More than "half of all adult SNS users are now over the age of 35." *Id.*

22. *Id.* ("Social networking sites are increasingly used to keep up with close social ties.").

23. *See* Patricia Sanchez Abril, Perspective, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 74 (2007). Professor Abril argues that the protection of privacy on online social networks is necessary for four reasons. *Id.* at 83. First, "social networking profiles serve an important identity-building function," by "provid[ing] a unique . . . forum for identity creation and exploration." *Id.* Second, privacy is necessary for individuals to preserve dignity and develop personality. *Id.* at 84-85. Third, voluntary disclosures online promote intimacy and socialization. *Id.* at 85-86. And fourth, privacy is necessary to encourage free discourse on OSNs. *Id.* at 86-87. Surveillance and unwanted sharing of personal communications stifle this free discourse. *Id.*

24. *See* Allyson W. Haynes, *The Short Arm of the Law: Simplifying Personal Jurisdiction Over Virtually Present Defendants*, 64 U. MIAMI L. REV. 133 (2009) (analyzing the exercise of personal jurisdiction over defendants based on Internet contacts by examining precedent dealing with offline contacts); *see also* Allyson W. Haynes, *Online Privacy Policies: Contracting Away Control Over Personal Information?*, 111 PENN. ST. L. REV. 587 (2007) (analyzing contract formation in the context of online privacy policies by analogizing to offline contract formation).

looks to offline precedent for guidance regarding how to define this space.

II. OFFLINE PRIVACY: MOVING TOWARD INDIVIDUALS' PRIVACY-ENHANCING EFFORTS

The distinction between "public" and "private" space underlies many aspects of US privacy law. The Fourth Amendment protects against searches and seizures where a person has a "reasonable expectation of privacy," which he will not have in a public place.[25] State tort law protects against the "public" disclosure of "private" facts, but does not protect against the dissemination of information already in the public sphere.[26] And tort law also protects against unwanted "intrusion upon seclusion," which a person will not have in a "public" place.[27] Underlying all of these areas[28] is the traditional idea that what is public and private is a function of both physical space and conscious exposure to others.[29]

Privacy has traditionally been defined using a binary distinction between public and private communications.[30] Also described as the "secrecy paradigm,"[31] some courts view privacy as an all-or-nothing attribute.[32] Professor Solove has been an effective critic of this notion of privacy as secrecy, where "once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private."[33] This narrow theory of privacy ignores the concepts of autonomy and choice—"individuals want to keep things

---

25. *See* Katz v. United States, 389 U.S. 347, 353-54 (1967).

26. *See* RESTATEMENT (SECOND) OF TORTS § 652D (1977).

27. *See id.* § 652B.

28. In addition, there are distinctions between speech on matters of public concern, protected by the First Amendment, and "matters of purely private concern." Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 758-59 (1985) ("We have long recognized that not all speech is of equal First Amendment importance."). This First Amendment concept underlies the rules that the media may not be punished for a privacy violation where it has lawfully obtained certain information. Fla. Star v. B. J. F., 491 U.S. 524, 541 (1989). This Article does not address the "public concern" aspect, focusing instead on the intrusion and disclosure aspects of the public/private distinction. *See Dun & Bradstreet*, 472 U.S. at 758-59.

29. *See* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 497 (2006).

30. *Id.*

31. Professor Daniel J. Solove coined this term in his article, *A Taxonomy of Privacy*. *See id.*; *infra* Part II.A.3

32. *See infra* Part II.A.1.

33. Solove, *supra* note 5, at 1107; *see also* Solove, *supra* note 29 ("Under the secrecy paradigm, privacy is tantamount to complete secrecy, and a privacy violation occurs when concealed data is revealed to others. If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information. In many areas of law, this narrow view of privacy has limited the recognition of privacy violations.").

private from some people but not others."[34] As Professor Solove explains:

> [C]ourts generally find no privacy interest if information is in the public domain, if people are monitored in public, if information is gathered in a public place, if no intimate or embarrassing details are revealed, or if no new data is collected about a person. . . . For disclosure, the secrecy of the information becomes a central dispositive factor; this approach often misses the crux of the disclosure harm, which is not the revelation of total secrets, but the spreading of information beyond expected boundaries.[35]

One contrasting theory considers privacy to include control over information and disclosure.[36] While this theory, like the binary secrecy paradigm, is too narrow in some respects,[37] it acknowledges that privacy includes the right not just to determine whether certain information will be disclosed, but the extent to which it will be disclosed, and the uses to which it will be put.[38]

By analyzing how the traditional binary distinction has been made and rejected in some offline instances, this Article analogizes to more modern privacy issues. Online as offline, privacy should be recognized as more complicated than simply black and white.

A. Common Law

Most scholars trace state common-law privacy to Samuel D. Warren and Louis D. Brandeis's famous law review article published in 1890.[39] Warren and Brandeis advocated for "the right 'to be let alone'" and a remedy for invasions of "the sacred precincts of private and domestic life."[40] They argued that the changes in technology and

---

34. Solove, *supra* note 5, at 1108.

35. Solove, *supra* note 29, at 563.

36. Solove, *supra* note 10, at 1113.

37. *Id.* at 1113-15 (noting that privacy-as-control omits the freedom to engage in certain activities, as opposed to disclosure of information alone, and excludes many decisional aspects of privacy, such as abortion and sexual freedom).

38. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967) (defining 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"); Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is not simply an absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves.").

39. Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 124 (2007) ("According to the oft-told legend, the right to privacy was born when Samuel Warren and Louis Brandeis penned *The Right to Privacy* in 1890."). *See generally* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

40. Warren & Brandeis, *supra* note 39, at 195.

industrialization made protection of "the domestic circle" even more important.[41]

Warren and Brandeis found seeds of privacy protection that extended beyond intellectual and artistic property within existing case law and that in fact "secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others."[42] This right to privacy necessarily has limits, including that it "ceases upon the publication of the facts by the individual, or with his consent."[43] But they recognized that "a private communication or circulation for a restricted purpose is not a publication within the meaning of the law."[44]

While the Warren & Brandeis article is considered the foundation of modern privacy law, William Prosser, in 1960, first delineated the privacy torts as we know them today.[45] The Restatement (Second) of Torts then recognized these torts collectively under an "Invasion of Privacy" category.[46] This category includes Publicity Given to Private Life (or "publication of private facts"),[47] Appropriation of Name or Likeness,[48] Intrusion upon Seclusion,[49] and False Light.[50] Now, fifty states have recognized some or all of these torts, either as part of their common law or by legislation.[51] The relevant privacy torts for purposes of this Article are publication of private facts and intrusion upon seclusion.

---

41. *Id.* at 196 ("The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.").

42. *Id.* at 198.

43. *Id.* at 218.

44. *Id.*

45. *See generally* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960).

46. RESTATEMENT (SECOND) OF TORTS § 652A-I (1977).

47. *Id.* § 652D ("One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.").

48. *Id.* § 652C. This tort provides a remedy against "[o]ne who appropriates to his own use or benefit the name or likeness of another." *Id.*

49. *Id.* § 652B ("One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other [person] for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.").

50. *Id.* § 652E. This tort prohibits the knowing or reckless public disclosure of a matter that places a person "in a false light" that "would be highly offensive to a reasonable person." *Id.*

51. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 31 (3d ed. 2008).

1. The Binary Approach: Public or Private

There is no privacy in public communications—that is, in anything a person himself makes public.[52] For example, under the Restatement's view of the tort of publication of private facts, a plaintiff will not receive protection for facts he shared with the public:

> There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public. . . . Similarly, there is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye. Thus he normally cannot complain when his photograph is taken while he is walking down the public street and is published in the defendant's newspaper.[53]

Rather, the law protects those facts or communications that the plaintiff "does not expose to the public eye, but keeps entirely to himself *or at most reveals only to his family or to close personal friends*."[54] Similarly, the tort of intrusion upon seclusion requires "intrusion into a place in which the plaintiff has secluded himself."[55] The invasion may include "opening his private and personal mail, searching his safe or his wallet, [or] examining his private bank account,"[56] but will not include investigation into public matters.

As applied by the courts, a third party cannot invade a person's privacy when that third party views, photographs, films, or overhears the person on public streets or thoroughfares.[57] In addition, courts have found no privacy violation when the following photographs or videotapes were taken: a couple at a farmers' market,[58] people standing in line in a government building to collect unemployment compensation,[59] a student in a classroom and hallway of a school

---

52. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b; WILLIAM L. PROSSER, LAW OF TORTS § 117 (4th ed. 1971).

53. RESTATEMENT (SECOND) OF TORTS § 652D cmt. b.

54. *Id.* (emphasis added). The Comment's language itself provides some relief from a view of privacy as utter secrecy. *See id.*

55. *Id.* § 652B cmt. b.

56. *Id.*

57. Jackson v. Playboy Enters., Inc., 574 F. Supp. 10, 11 (S.D. Ohio 1983) (holding that there was no invasion of privacy by publication of photograph of policewoman with three minors on a public sidewalk); Forster v. Manchester, 189 A.2d 147, 150 (Pa. 1963) (stating that there is no right to privacy based on surveillance "in the open on public thoroughfares where appellant's activities could be observed by passers-by"); Swerdlick v. Koch, 721 A.2d 849, 859 (R.I. 1998) (holding that there was no privacy violation when a neighbor photographed and documented activity taking place in full view of a public street).

58. Gill v. Hearst Publ'g Co., 253 P.2d 441, 444 (Cal. 1953) (stating that there is no right to privacy based on plaintiffs' "voluntary assumption of [a] particular pose in a public place," where the defendant published a picture of plaintiffs at their place of business in a busy farmers' market).

59. Cefalu v. Globe Newspaper Co., 391 N.E.2d 935, 939 (Mass. App. Ct. 1979) ("The appearance of a person in a public place necessarily involves doffing the cloak of privacy which the law protects.").

building during regular school hours,[60] a person in a courtroom,[61] in a restaurant,[62] on a cruise ship,[63] or in a church during a service open to the public.[64] Courts have found no privacy interest at a public spa,[65] health club,[66] or in a college's office space that was visible to employees and participants in the college program.[67] There is little gray area in the case law: typically, a space is open to the public or not.

2. Exceptions to the Traditional Rule

Courts have recognized two primary exceptions to the rule that a person lacks a right to privacy in a "public" place. First, privacy yields to security when the invasion rises to the level of harassment. Second, some activities are considered inherently private, thereby privatizing an otherwise public space.

a. Harassment or "Overzealous Surveillance"

First, a right to privacy will be implicated even in public when it rises to the level of harassment, particularly where children are involved.[68] Thus, the US Court of Appeals for the Second Circuit in *Galella v. Onassis* upheld an injunction prohibiting a paparazzo from

---

60. Jarrett v. Butts, 379 S.E.2d 583, 584-85 (Ga. Ct. App. 1989).

61. Berg v. Minneapolis Star & Tribune Co., 79 F. Supp. 957, 958-59, 963 (D. Minn. 1948) (finding no invasion of privacy when photographer took picture of plaintiff in courtroom and used it to illustrate a story about plaintiff's divorce and custody proceedings, which were of legitimate interest to the public).

62. Dempsey v. Nat'l Enquirer, 702 F. Supp. 927, 931 (D. Me. 1988); Wilkins v. NBC, 84 Cal. Rptr. 2d 329, 336 (Ct. App. 1999).

63. Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 483 (D. Me. 1987) (finding no invasion of privacy based on photographers taking pictures and harassing passenger on cruise ship, although plaintiff stated a claim for intentional infliction of emotional distress), *aff'd in part, rev'd in part*, 845 F.2d 347 (1st Cir. 1988).

64. Creel v. I.C.E. & Assocs., 771 N.E.2d 1276, 1281 (Ind. Ct. App. 2002) (holding that videotaping in a courtroom did not violate privacy where it "simply captured activity that was open to the public, observed by many, . . . which [anyone attending] could have testified to witnessing at trial").

65. Garmley v. Opryland Hotel Nashville, LLC, No. 3:07-0681, 2007 WL 4376078, at *3 (M.D. Tenn. Dec. 13, 2007) (rejecting claim for publication of private facts where the facts involve plaintiff's conduct with a member of the public, a massage therapist at a commercial spa); *see also* Wigginess, Inc. v. Fruchtman, 482 F. Supp. 681, 689-90 (S.D.N.Y. 1979), *aff'd*, 628 F.2d 1346 (2d Cir. 1980).

66. Foster v. Livingwell Midwest, Inc., No. 88-5340, 1988 WL 134497, at *2 (6th Cir. Dec. 16, 1988) (affirming lower court's finding of no privacy claim where plaintiff was filmed while exercising at the health spa where she was a member).

67. Nelson v. Salem State Coll., 845 N.E.2d 338, 346-47 (Mass. 2006).

68. *See* Galella v. Onassis, 487 F.2d 986, 998-99 (2d Cir. 1973); Tompkins v. Cyr, 995 F. Supp. 664, 684 (N.D. Tex. 1998); Wolfson v. Lewis, 924 F. Supp. 1413, 1433-34 (E.D. Pa. 1996). *But see* Valenzuela v. Aquino, 853 S.W.2d 512, 513-14 (Tex. 1993).

approaching the defendant Onassis within twenty-five feet or touching her, from blocking her movement in public places and thoroughfares, from any act that would place her life and safety in jeopardy, and from harassing, alarming, or frightening her.[69] Similarly, in *Wolfson v. Lewis*, the court ordered an injunction against surveillance and harassment of a family of healthcare executives, finding the tort of intrusion to protect against "[c]onduct that amounts to a persistent course of hounding, harassment and unreasonable surveillance, even if conducted in a public or semi-public place."[70]

b. Inherently Private Activity

Second, courts find a right to privacy in locations that are open to the public when the nature of the activity is inherently private; that is, activities involving bodily functions, health, reproduction, or nudity. Thus, in *Huskey v. National Broadcasting Co., Inc.*, a prisoner filmed in an "exercise cage" wearing only gym shorts who alleged that he was engaged in "private activities" stated a claim for invasion of privacy.[71] An employer violated employees' right to privacy by installing a hidden camera in a nurse manager's office where medical examinations took place.[72] A tanning salon owner violated a customer's privacy by secretly watching and photographing her while she undressed and tanned in the tanning room.[73] A hospital violated a patient's right to privacy when a nurse's husband viewed her delivery of a baby.[74] And a breast cancer patient's privacy was invaded when a drug salesman was allowed to observe her breast exam.[75] Courts have likewise found a right to privacy in a hospital room with respect to non-hospital personnel,[76] and in the emergency room.[77] They have found a right to privacy in public restrooms[78] and changing rooms.[79]

---

69. *Galella*, 487 F.2d at 998.

70. *Wolfson*, 924 F. Supp. at 1420-21, 1435 (emphasizing that such a cause of action in Pennsylvania would require substantial, offensive, and intentional intrusion upon the plaintiffs' seclusion).

71. Huskey v. NBC, 632 F. Supp. 1282, 1285 (N.D. Ill. 1986).

72. Acuff v. IBP, Inc., 77 F. Supp. 2d 914, 921 (C.D. Ill. 1999).

73. Sabrina W. v. Willman, 540 N.W.2d 364, 369 (Neb. Ct. App. 1995).

74. Knight v. Penobscot Bay Med. Ctr., 420 A.2d 915, 916-17 (Me. 1980).

75. Sanchez-Scott v. Alza Pharm., 103 Cal. Rptr. 2d 410, 418-20 (Ct. App. 2001).

76. People v. Brown, 151 Cal. Rptr. 749, 754-55 (Ct. App. 1979).

77. Castro v. NYT Television, 851 A.2d 88, 96-97 (N.J. Super. Ct. App. Div. 2004) (noting that defendants concede plaintiffs stated a cause of action for unreasonable intrusion).

78. Harkey v. Abate, 346 N.W.2d 74, 76 (Mich. Ct. App. 1983) (finding invasion of privacy based on installation of hidden viewing devices in public restroom at skating rink). *But see* Daly v. Viacom, Inc., 238 F. Supp. 2d 1118, 1123-25 (N.D. Cal. 2002) (finding plaintiff had no privacy claim in a film of her kissing a man in a bathroom stall).

79. Bevan v. Smartt, 316 F. Supp. 2d 1153, 1158, 1161-62 (D. Utah 2004).

And they have found a right to privacy in an otherwise public place where an inadvertently embarrassing or revealing pose is captured.[80] This exception is, however, a narrow one.[81]

3. Movement Away From the Binary Approach

In addition to the traditional exceptions noted above, some courts have embraced a more nuanced view of the privacy torts than the binary distinction between public and private communications or activities. These courts, in effect, recognize that privacy is not equivalent to secrecy, but should be viewed in context. And importantly, many courts find determinative individuals' own efforts to preserve the area as private.

In *Nader v. General Motors Corp.*, the New York Court of Appeals found sufficient allegations of invasion of privacy based on "overzealous" surveillance and recognized that a person's own actions in maintaining privacy—even in public—are relevant:[82]

> A person does not automatically make public everything he does merely by being in a public place, and the mere fact that Nader was in a bank did not give anyone the right to try to discover the amount of money he was withdrawing. On the other hand, if the plaintiff acted in such a way as to reveal that fact to any casual observer, then, it may not be said that the appellant intruded into his private sphere.[83]

The US Court of Appeals for the Sixth Circuit similarly found an invasion of privacy when a supervisor secretly recorded the conversations of four employees who worked in an open area.[84] The court concluded that the employees' expectation of privacy was objectively reasonable because, despite the open workspace, "the employees took great care to ensure that their conversations remained private" and the office was a "small, relatively isolated space," where "[t]he employees could be sure that no one was in the building without their knowledge."[85]

Other courts have also looked beyond the fact that a place is open to the public when an employee alleges a violation of privacy on company property. In *K-mart Corp. Store Number 7441 v. Trotti*, the Texas Court of Appeals upheld a claim by an employee for intrusion

---

80. Daily Times Democrat v. Graham, 162 So. 2d 474, 476, 478 (Ala. 1964).

81. *See* McNamara v. Freedom Newspapers, Inc., 802 S.W.2d 901, 905 (Tex. App. 1991) (finding no invasion of privacy when picture was taken in public place and genitals were accidentally exposed).

82. Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

83. *Id.* at 771.

84. Dorris v. Absher, 179 F.3d 420, 423-25 (6th Cir. 1999).

85. *Id.* at 425 ("The conversations took place only when no one else was present, and stopped when the telephone was being used or anyone turned onto the gravel road that was the only entrance to the office.").

upon seclusion when the employer searched a locker on company premises.[86] The court found it important that, while the lockers were the property of the employer, the employer allowed employees to purchase and use their own locks to secure personal belongings in the lockers.[87] Therefore, the employee "demonstrated a legitimate expectation to a right of privacy in both the locker itself and those personal effects within it."[88]

Likewise, the California Supreme Court found that an employee of a telepsychic marketing company, whom an undercover reporter had surreptitiously recorded, had a claim for intrusion upon seclusion despite the fact that other employees could hear the conversation.[89] The court held that, even though the plaintiff may have lacked "a reasonable expectation of *complete* privacy in a conversation because it could be seen and overheard by coworkers (but not the general public)," there was still a basis for a privacy claim.[90] While the court acknowledged that its holding in *Shulman v. Group W Productions, Inc.* required "an objectively reasonable expectation of seclusion or solitude in the place, conversation or data source,"[91] it rejected the notion that privacy was an all-or-nothing concept: "neither in *Shulman* nor in any other case have we stated that an expectation of privacy, in order to be reasonable for purposes of the intrusion tort, must be of *absolute* or *complete* privacy."[92]

Instead, videotaping in public may intrude on privacy even when the events are visible and audible to others. The court referred to its holding as "an expectation of limited privacy":

> [P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: the

86. K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637 (Tex. App. 1984) ("Where . . . the employee purchases and uses his own lock on the lockers, with the employer's knowledge, the fact finder is justified in concluding that the employee manifested, and the employer recognized, an expectation that the locker and its contents would be free from intrusion and interference.").

87. *Id.*

88. *Id.* at 638.

89. Sanders v. Am. Broad. Cos., 978 P.2d 67, 71 (Cal. 1999).

90. *Id.* (emphasis added).

91. Schulman v. Grp. W Prods., Inc., 955 P.2d 469, 491 (Cal. 1998). The court reversed the finding of the Court of Appeals that "plaintiffs had no reasonable expectation of privacy at the accident scene itself because the scene was within the sight and hearing of members of the public." *Id.* Rather, the court found that "[f]rom the tapes it appears unlikely the plaintiffs' extrication from their car and medical treatment at the scene could have been observed by any persons who, in the lower court's words, 'passed by' on the roadway." *Id.* The Court continued: "[a] patient's conversation with a provider of medical care in the course of treatment, including emergency treatment, carries a traditional and legally well-established expectation of privacy." *Id.* at 491-92.

92. *Sanders*, 978 P.2d at 71-72.

> fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law. Although the intrusion tort is often defined in terms of "seclusion," the seclusion referred to need not be absolute. "Like 'privacy,' the concept of 'seclusion' is relative. The mere fact that a person can be seen by someone does not automatically mean that he or she can legally be forced to be subject to being seen by everyone."[93]

The recognition that privacy involves interests beyond secrecy or seclusion underlies the Supreme Court's decision in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, where the Court found that the privacy exemption of the Freedom of Information Act precluded the release of FBI "rap sheets" despite the fact that those records constituted compilations of information previously publicly disclosed.[94] The Court noted that few facts are completely undisclosed, and that there is a salient distinction between "scattered disclosure of the bits of information contained in a rap sheet" and divulgence of the rap sheet itself.[95]

Since Professor Solove published his *Conceptualizing Privacy* article in 2002, two Circuit Courts of Appeals have recognized the salience of his distinction between privacy-as-secrecy and privacy-as-control, both in the context of analyzing conflicts between privacy interests and First Amendment protection. First, in 2009, in *National Cable & Telecommunications Ass'n v. FCC*, the District of Columbia Court of Appeals considered the validity of the Federal Communications Commission's 2007 order implementing the Telecommunications Act of 1996 specifying how telecommunications carriers are to obtain their customers' approval for the sharing of personal information.[96] Rejecting the approach of the US Court of Appeals for Tenth Circuit in *U.S. West, Inc. v. FCC*,[97] the court found that the Commission's order did not violate the First Amendment rights of the carriers under the balancing required by *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*.[98] While the Tenth Circuit believed that the government interest at

93. *Id.* at 72 (citations omitted) (quoting 1 J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.10(A)(2) (1998)).

94. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989).

95. *Id.* at 764; *see also* Solove, *supra* note 5, at 1109.

96. Nat'l Cable & Telecomms. Ass'n v. FCC, 555 F.3d 996, 997-1000 (D.C. Cir. 2009) (construing Implementation of the Telecomms. Act of 1996: Telecomms. Carriers' Use of Customer Proprietary Network Info. and Other Customer Info.; IP-Enabled Servs., 22 F.C.C. Rcd. 6927 (2007)).

97. U.S. W., Inc. v. FCC, 182 F.3d 1224, 1235, 1239 (10th Cir. 1999).

98. *Nat'l Cable*, 555 F.3d at 1000-02 (citing Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557 (1980)).

stake was preventing the disclosure of embarrassing information,[99] the DC Circuit found that the privacy interest was of a different sort:

> [W]e do not agree that the interest in protecting customer privacy is confined to preventing embarrassment as the Tenth Circuit thought. There is a good deal more to privacy than that. It is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others. The Supreme Court knows this as well as Congress: "both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[100]

A year later, the US Court of Appeals for the Fourth Circuit in *Ostergren v. Cuccinelli* rejected the secrecy paradigm in determining whether the application of a Virginia law prohibiting the publication of social security numbers would be unconstitutional as applied to the posting of Virginia land records on a privacy advocate's website.[101] The court noted that the privacy interest in preventing disclosure of social security numbers involved "a different conception of privacy not predicated on secrecy."[102] Unlike the release of the name of a rape victim or juvenile defendant's identity, disclosure of a social security number is not potentially embarrassing or compromising; rather, this case involved "a particular conception of privacy whereby one does not mind publicity itself but nonetheless would prefer to control how personal information will be used or handled."[103] The court quoted the US Court of Appeals for the D.C. Circuit in rejecting the limitations of the secrecy paradigm: "Under this conception, privacy does not hinge upon secrecy but instead involves 'the individual's *control* of information concerning his or her person.'"[104]

Thus, many courts have moved away from the binary view of privacy as secrecy, and toward recognition that privacy includes a right to control disclosure.[105] The extent to which the individual tries to wield that control is determinative.

---

99. *U.S. W., Inc.*, 182 F.3d at 1235.

100. *Nat'l Cable*, 555 F.3d at 1001 (quoting U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989)) (citing Solove, *supra* note 5, at 1109-10).

101. Ostergren v. Cuccinelli, 615 F.3d 263, 290 (4th Cir. 2010).

102. *Id.* at 282.

103. *Id.* at 282-83.

104. *Id.* at 283 (quoting *Nat'l Cable*, 555 F.3d at 1001).

105. *See* Cook v. WHDH-TV, Inc., No. 941269, 1999 WL 1327222 (Mass. Super. Ct. Mar. 4, 1999). The court found that the plaintiff stated a claim for intrusion upon seclusion under a Massachusetts's statute prohibiting "unreasonable, substantial or serious interference with his privacy," despite the fact that the intrusion at issue occurred while plaintiff was approached in his car, with his son, and in line at a Burger King drive-through. *Id.* at *5 (quoting MASS. GEN. LAWS ch. 214, § 1B (2011)). In doing so, the court rejected the argument that plaintiff voluntarily assumed the risk of being observed by being in a public place. *Id.* The plaintiff "was entitled to have a jury consider such factors as the defendant's motive for the intrusion; the extent or invasiveness of the intrusion; whether the plaintiff had a reasonable expectation of being free from such an intrusion; and whether the plaintiff consented." *Id.* The court explained that "the

B. The Fourth Amendment

Fourth Amendment analysis also shows a move from privacy as a binary or all-or-nothing concept toward a focus on context. The Fourth Amendment prohibits government agents from engaging in unreasonable searches and seizures.[106] Fourth Amendment searches are relevant here in two contexts: searches for criminal wrongdoing, and searches in a government-employment setting.[107] In both areas, courts have analyzed the existence of a person's reasonable expectations of privacy to determine whether a search has in fact occurred.[108] If there is no reasonable expectation of privacy, then there is no search at all.

The Supreme Court originally held that only physical trespasses into private spaces qualified as searches under the Fourth Amendment.[109] Thus, the quintessential protection of the Fourth Amendment was against searches of private homes.[110] Fourth Amendment analysis underwent a significant change after the landmark case of *United States v. Katz*.[111] There, the Court abandoned the "trespass" requirement, and indeed any focus on the specific "place" intruded upon by the government,[112] and instead found that a search may in fact take place even in a public place, so long as the person "seeks to preserve [that place] as private."[113] As Justice

---

rigid application of invasion of privacy tort law to invasions occurring in public places ought not deprive Mr. Cook of the judgment of a jury of his peers as to whether defendants unreasonably and substantially or seriously invaded his privacy." *Id.* The US Court of Appeals for the Sixth Circuit also found a possible invasion of privacy despite the fact that the invasion occurred in a public restaurant. Evans v. Detlefsen, 857 F.2d 330, 338 (6th Cir. 1988).

> The short answer to the defendant's argument [that there could be no intrusion into the plaintiff's seclusion in a public restaurant] is that the privacy which is invaded has to do with the type of interest involved and not the place where the invasion occurs. . . . Although the place of the occurrence is relevant to a determination of the sufficiency of the evidence of intrusiveness, it is not determinative of whether an intrusion into one's 'solitude and seclusion' has occurred.

Id.; *see also* Y.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488, 501 (Mo. Ct. App. 1990) (finding invasion of a couple's privacy by the publication of a video showing them at an in vitro fertilization gathering, where they were assured the event would remain private, they refused to be interviewed, and they made every effort to remain off-camera).

106. U.S. CONST. amend. IV; Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

107. *See* Leventhal v. Knapek, 266 F.3d 64, 73 (2d Cir. 2001) (noting that the Fourth Amendment protects against unreasonable searches and seizures by the government even when the government acts as an employer).

108. Katz v. United States, 389 U.S. 347, 353-54 (1967); *Leventhal*, 266 F.3d at 73.

109. Olmstead v. United States, 277 U.S. 438, 465-66 (1928).

110. *Id.* at 473 (Brandeis, J., dissenting).

111. *See Katz*, 389 U.S. at 347.

112. *Id.* at 353; *see also id.* at 351 ("[T]he Fourth Amendment protects people, not places.").

113. *Id.* at 351.

Harlan reasoned in his concurrence, the Fourth Amendment's protections require "first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[114] Thus, despite the fact that the government in *Katz* did not trespass inside the public telephone booth while wiretapping the defendant's conversations, "[t]he critical fact [was] that 'one who occupies it . . . shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume' that his conversation is not being intercepted."[115] In other words, the existence of an expectation of privacy does not depend on the place searched being completely "public" or "private"—rather, "it is a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable."[116]

Even privacy in the home, which has historically received prototypical protection, can be lost if the home is open to "plain view."[117] Courts look at the "effort on the part of the occupants to make [a] room secret and protect their privacy,"[118] and a person's "actual attempts to safeguard his private affairs."[119] Since *Katz*, the Supreme Court has found a reasonable expectation of privacy to exist in the interior of a car,[120] and in the interior of a person's purse or luggage,[121] even though the car or the luggage is in a public place. Also, like the temporary privacy a person has in a public telephone booth when he enters and shuts the door, a person has a limited

114. *Id.* at 361 (Harlan, J., concurring).

115. *Id.* (quoting *id.* at 352 (majority opinion)).

116. *Id.*

117. *Id.* ("Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.").

118. People v. Walker, 80 Cal. Rptr. 531, 533 (Ct. App. 1969).

119. State v. Morris, 961 P.2d 653, 657 (Idaho Ct. App. 1998) (noting that the defendant "took no steps to cover the window in order to shield his activities from the view of passersby"); *cf.* State v. Fortmeyer, 37 P.3d 223, 226 (Or. Ct. App. 2001) (noting that "defendants took extra measures to try to protect their privacy in their home").

120. United States v. Ross, 456 U.S. 798, 825 (1982).

121. United States v. Place, 462 U.S. 696, 707 (1983).

expectation of privacy in a public restroom,[122] hospital room,[123] changing room,[124] and hotel room.[125]

The Supreme Court has also recognized that a public employee can have an expectation of privacy in his place of work.[126] In *O'Connor v. Ortega*, the Court "delineate[d] the boundaries of the workplace context," which include "those areas and items that are related to work and are generally within the employer's control."[127] Whether an employee has a reasonable expectation of privacy within those boundaries will depend on context.[128] Some "offices may be so open to . . . the public" that the employee lacks any reasonable expectation of privacy there.[129] In addition to looking at how the particular office space is used, the Court noted that it would be relevant if the employer had a policy in place regarding the use of offices and the privacy that might be expected therein.[130]

One important doctrine limiting reasonable expectations of privacy in Fourth Amendment cases is the third-party doctrine, which finds that a person has no expectation of privacy in communications voluntarily provided to a third party.[131] In *Smith v. Maryland*, the Supreme Court found that the use of a pen register, which records numbers dialed from a telephone line, is not a search under the Fourth Amendment.[132] The Court found that people do not have a reasonable expectation of privacy in the numbers they dial because they "realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed."[133] In addition, the Court distinguished pen registers from more intrusive surveillance on the basis that "pen registers do not acquire the *contents* of communications."[134]

---

122. United States v. White, 890 F.2d 1012, 1015 (8th Cir. 1989); Barron v. State, 823 P.2d 17, 20 (Alaska Ct. App. 1992); State v. Powers, 991 So. 2d 1040, 1041 (Fla. Dist. Ct. App. 2008).

123. Ferguson v. City of Charleston, 532 U.S. 67, 78 (2001).

124. People v. Diaz, 376 N.Y.S. 2d 849, 854-55 (1975); State v. McDaniel, 337 N.E.2d 173, 177 (Ohio Ct. App. 1975).

125. Stoner v. California, 376 U.S. 483, 490 (1964).

126. O'Connor v. Ortega, 480 U.S. 709, 717 (1987).

127. *Id.* at 715.

128. *Id.* at 717 ("Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures, or by legitimate regulation.").

129. *Id.* at 717-18.

130. *Id.* at 717.

131. *See* United States v. Miller, 425 U.S. 435, 442 (1976).

132. Smith v. Maryland, 442 U.S. 735, 742 (1979).

133. *Id.*

134. *Id.* at 741.

An analogous aspect of the third-party doctrine is the "misplaced trust" doctrine used by the Supreme Court in *Hoffa v. United States*.[135] Under this rule, a person lacks a reasonable expectation of privacy in communications made to another party if the other party turns out to be a government informant.[136] Similarly, there is no protection against that other party to the communication then turning the information over to the authorities.[137]

Thus in common law and Fourth Amendment offline contexts, expectations of privacy can exist in limited circumstances despite the fact that communications occurred in a public context or were disclosed to third parties. The important question is whether the person has sought to preserve the area as private, and whether his expectation of privacy is one that society is prepared to recognize as reasonable.[138]

C. Statutory Privacy Law

In addition to tort law and Fourth Amendment issues, there are many federal and state statutes dealing with privacy interests. The statutes invoked most in the context of invasions of privacy online are Title I and Title II of the Electronic Communications Privacy Act (ECPA).[139] Title I, or the Wiretap Act, prohibits the interception of electronic communications in transit.[140] Title II, or the Stored Communications Act (SCA), regulates accessing of stored electronic communications and records.[141] When claims are brought under these statutes, they raise the issue of whether a party has intercepted an electronic communication or accessed a stored communication without authorization.[142] There is no protection for communications that are "readily accessible to the public."[143] Thus, the question of authorization and ready accessibility to the public often overlaps with

135. Hoffa v. United States, 385 U.S. 293, 302 (1966); *see also* Lewis v. United States, 385 U.S. 206, 210 (1966).

136. *Hoffa*, 385 U.S. at 302 (holding that there is no protection under the Fourth Amendment for "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it").

137. *See, e.g.*, United States v. King, 55 F.3d 1193, 1195 (6th Cir. 1995) (finding no expectation of privacy in letters provided to the government by a private individual).

138. *See* United States v. Jacobsen, 466 U.S. 109, 122 (1984).

139. Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510-2522, 2701-2712 (2006).

140. *Id.* §§ 2510-2522.

141. *Id.* §§ 2701-2712.

142. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879-80 (9th Cir. 2002); *see also* United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996).

143. *Konop*, 302 F.3d at 875 (quoting H.R. REP. NO. 99-647, at 41, 62-63 (1986)).

the existence of a protected privacy interest in the intercepted communications.[144]

III. ONLINE PRIVACY: RECOGNIZING USER CONTROLS AS "PRIVACY-ENHANCING EFFORTS"

As courts' analyses of reasonable expectations of privacy have shifted to the online context, courts have used analogies to previous communication methods like first-class mail and the telephone.[145] They have struggled with the public versus private distinction in a nonphysical context,[146] and with the fact that some Internet communications necessarily involve disclosure to third parties.[147] Some courts have mistakenly resorted to an over-simplified view of privacy interests.[148] But there is also a line of authority finding a reasonable expectation of privacy in the content of online communications, depending upon an analysis of the user controls, or the equivalent of shutting virtual doors or covering virtual windows.[149]

A. Brief Description of Online Communications and User Controls

In offline contexts, as discussed above, courts have given effect to people's efforts to ensure privacy by closing doors and blinds, employing locks, and otherwise conforming their activity to increase

144. *See* Shefts v. Petrakis, 758 F. Supp. 2d 620, 633 (C.D. Ill. 2010) (finding notice of monitoring of communications in employee manual defeated claims based on ECPA and reasonable expectation of privacy under Illinois Eavesdropping Statute); *see also* City of Ont. v. Quon, 130 S. Ct. 2619, 2632 (2010) (noting respondents' argument that the existence of a statutory protection under the SCA renders a search *per se* unreasonable under the Fourth Amendment, and stating that "the precedents counsel otherwise").

145. *See* United States v. Forrester, 512 F.3d 500, 509, 511 (9th Cir. 2007).

146. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1012 (2010) (describing the difficulty in applying the Fourth Amendment to the Internet, where the traditional inside/outside distinction "no longer works").

147. *See* Patricia Sanchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 25 (2007) ("In cyberspace, the complete secrecy requirement of privacy torts is difficult, if not impossible, to satisfy. Total secrecy is difficult offline; this difficulty is magnified online. No information placed on OSNs is completely secret, even if a profile is set to private. . . . Any information posted on OSNs–even if never actually transmitted to another—is not completely secret. This is because anything posted on OSNs is accessible to a third party—the OSNs themselves.").

148. *See infra* Part III.B.2.i.

149. *See* United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 875 (9th Cir. 2002); *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1083-84 (N.D. Cal. 2011); Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 449-50 (D. Conn. 2009); United States v. Long, 64 M.J. 57, 64-65 (C.A.A.F. 2006).

its private nature.[150] Online, analogous privacy measures include passwords, encryption techniques, privacy settings, and other methods of controlling the privacy of communications.[151] This Article focuses on four categories of Internet communication: email, websites, files shared via the Internet, and online social networks. The following Sections provide a brief description of how user controls may operate in each of those communication technologies.

1. Email

In our society, people typically use either workplace email or private email systems.[152] In the case of workplace email, the employer will typically have a policy governing the use of that email and the privacy given to it.[153] An employee whose employer monitors his email and notifies him of that monitoring via, for example, banner warnings each time she logs onto the computer, will not receive as much privacy protection as an employee whose employer does not monitor or access employee email.[154] Also important is whether the employee has a password that is unknown to the employer, and whether the employer has a right of access to the employee's email.[155] With private email, the relevant policy is between the user and the email service or Internet service provider (ISP) to which that user subscribes.[156] Some subscriber agreements provide for the ISP's provision of subscriber information to third parties, while others emphasize that they will not share subscriber information without a warrant.

Whatever system provides the email, the privacy of its component parts may be treated differently. As discussed further

---

150. *See* Dorris v. Absher, 179 F.3d 420, 425 (6th Cir. 1999); Nader v. Gen. Motors Corp., 255 N.E.2d 765, 770-71 (N.Y. 1970); K-Mart Corp. Store No. 7441 v. Trotti, 677 S.W.2d 632, 637 (Tex. App. 1984).

151. *See infra* Part III.B.

152. "More than half of working adults (53 [percent]) have both personal and work email accounts." Mary Madden & Sydney Jones, *Networked Workers*, PEW RESEARCH CTR. (Sept. 24, 2008), http://pewresearch.org/pubs/966/. "And while 22 [percent] say they maintain only a personal account, just 5 [percent] say that their email use is limited to a work account. . . . Personal email spills over to the cell phone and Blackberry, too . . . ." *Id.*

153. *See, e.g.*, *Brown-Criscuolo*, 601 F. Supp. 2d at 449-50 (describing employer's "Acceptable Use Policy" controlling the use of its computer system).

154. *Cf. id.* at 449 (listing factors to determine reasonable privacy expectations, such as whether the company monitors the employee's computer or email use and whether the employee is aware of company policy).

155. *See id.* at 449-50.

156. *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (describing AOL's contractual agreement with its email subscribers and policies in terms of reading or disclosing subscribers' emails).

below, the "to" and "from" addressing or "envelope" information is considered "non-content" information, while the actual message within the email is considered "content."[157] As with postal mail, courts have generally found no right to privacy in non-content information, while being more amenable to such a right in content information.[158] An employee's choice to either use an email system that his employer monitors and can access or a system that promises not to disclose information to third parties greatly affects the privacy of the email's "content."

2. Files Shared Via the Internet

Another way in which Internet users exchange information is through peer-to-peer sharing of computer files via Internet networks.[159] One example of a service that allows file-sharing is LimeWire.[160] A person who signs up for the software service and shares files on the service makes those files available to any other user of the software.[161] Another example is iTunes, the Apple software that enables users to share some of the content they maintain in their own iTunes files with other iTunes users.[162] The particular software or service will govern the specifics of when and how it allows such sharing. The user of open file sharing—whereby any user of the service may view the files shared by another user—will receive less protection from disclosure than the user of a file-sharing service that limits access to others.[163] In the wireless context,

157. *See* Kerr, *supra* note 146, at 1019-20 ("The addressing (or 'envelope') information is the data that the network uses to deliver the communications to or from the user; the content information is the payload that the user sends or receives.").

158. *Id.* at 1021-29.

159. *Cf.* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008); United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007); United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *6 (D. Or. Jan. 28, 2010).

160. LIMEWIRE, http://www.limewire.com (last visited Jan. 26, 2012). LimeWire was forced to shut down in 2010 due to copyright complaints. Edward Moyer, *Little Juice Left in Lime Wire*, CNET NEWS (Dec. 4, 2010), http://news.cnet.com/8301-1023_3-20024651-93.html.

161. *See* United States v. Borowy, 595 F.3d 1045, 1046-47 (9th Cir.) (describing LimeWire as "a publically [sic] available peer-to-peer file-sharing computer program"), *cert. denied*, 131 S. Ct. 795 (2010). In *Borowy*, a FBI agent, who was monitoring trafficking in child pornography, accessed LimeWire to download pornography files shared on the service by the defendant. *Id.*

162. *iTunes*, APPLE, http://www.apple.com/itunes/?cid=OAS-US-DOMAINS-itunes.com (last visited Jan. 26, 2012); *see Ahrndt*, 2010 WL 373994, at *6.

163. *See infra* Part III.B.3. *Compare Heckenkamp*, 482 F.3d at 1146-47 (finding a reasonable expectation of privacy in computer files despite the computer's connection to the employer's network, where the employer's policy did not provide for active monitoring of the employee's computer usage), *with* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (finding no reasonable expectation of privacy in files downloaded from the Internet where the

encrypted or secure networks will lead to privacy protection more than unsecured, open-access networks.[164]

3. Information Posted on a Website

This category includes an Internet user's decision to post a message on a website's message board or discussion forum, or in a chat room.[165] A message board or discussion forum is a feature that allows users to post and read messages, much like a virtual "bulletin board."[166] Chat rooms are webpages in which Internet users have "real-time" conversations with each other by posting and receiving instantaneous messages.[167] This category also includes a user posting information, photographs, videos, or other data onto a website, including data created by the specific user.[168] Relevant to the privacy of such postings are, again, any subscriber agreement between the ISP and the Internet user, in addition to whether a password or other method protects the website from access.[169] Like the email addressing information, information provided to ISPs is considered "non-content," while actual pages viewed would be considered "content."[170] A person who posts information on a website or chat room may control the

---

user's employer policy provided for auditing, inspecting, and monitoring of employees' Internet use).

164. *See infra* Part III.B.3. *Compare Ahrndt*, 2010 WL 373994, at *6 (finding no reasonable expectation of privacy where the defendant used an unsecured wireless network and set his iTunes software preferences to allow sharing of his files with any other user of the network), *with In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1083 (N.D. Cal. 2011) (finding a claim under the Wiretap Act where Google accessed users' networks, which were configured to render communications unreadable and inaccessible without the use of special software).

165. *See* Guest v. Leis, 255 F.3d 325, 331-32 (6th Cir. 2001); United States v. Maxwell, 45 M.J. 406, 411 (C.A.A.F. 1996).

166. United States v. Riggs, 739 F. Supp. 414, 417 n.4 (N.D. Ill. 1990) ("A computer bulletin board system is a computer program that simulates an actual bulletin board by allowing computer users who access a particular computer to post messages, read existing messages, and delete messages."). Note that the more modern use of the term "bulletin board system" refers to a service with considerably more functionality. *See Guest*, 255 F.3d at 331-32 (describing one bulletin board system that allows users to send email to subscribers, participate in chat room conversations or online games, or post or read messages on many topics).

167. Chat rooms have different levels of privacy. *See Maxwell*, 45 M.J. at 411 (describing chat conversations on AOL that take place in either a "public room" or a "private room").

168. *See* J.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 415 (Pa. Commw. Ct. 2000) (describing a website created by student that "consisted of several web pages that made derogatory comments about Student's algebra teacher [and principal]"), *aff'd*, 807 A.2d 847 (Pa. 2002).

169. *See id.* at 425 (describing student-created website that was "not a protected site, meaning that only certain viewers could access the site by use of a known password" and was accessible by links from other sites or by a user "stumbl[ing] upon" it when using certain search terms).

170. *See* Kerr, *supra* note 146, at 1029-30.

privacy of that posting by ensuring that the website is not open to the public but is protected by passwords or other techniques.

4. Online Social Networks

While the communications and information shared on OSNs overlap with some of the above descriptions, this Article treats OSNs separately because these activities occur under a single network in an OSN, and because OSNs are tremendously popular. Nearly half of all adults, or 50 percent of Internet users, say they use at least one OSN.[171] The most popular OSN is Facebook, boasting a membership of 92 percent of OSN members.[172] The second most popular is MySpace with 29 percent.[173] On an OSN, a user can send email messages to another user or "chat" in real time similar to the online chats discussed above.[174] A user creates his own "profile," where he can post information, photographs, or other data—and users may post such items on each other's profiles.[175] The user chooses the intended audience for these posts by enabling privacy settings that control who has access to the user's posts within the website.[176] Such settings can be as broad as "public," allowing viewing by anyone on the Internet, or as narrow as the user chooses.[177] Every OSN has a subscriber agreement with the specific user governing the terms of use and setting out privacy provisions.[178] The user controls include the user's choice to share information with a limited audience versus sharing with the public at large.

B. The Law's Treatment of Online Privacy

Applying traditional notions of privacy is problematic when it comes to the Internet, which is not a "place" at all,[179] and where some disclosure to a third party is a necessary predicate to communication thereon.[180] Under a strict application of the law, there is by definition

---

171. *65% of Online Adults Use Social Networking Sites*, *supra* note 17.

172. Rainie et al., *supra* note 21.

173. *Id.*

174. *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 976-77 (C.D. Cal. 2010).

175. *Id.* at 977.

176. *See, e.g.*, Abril, *supra* note 147, at 14-15.

177. *Id.*

178. *See, e.g.*, Romano v. Steelcase Inc., 907 N.Y.S. 2d 650, 656-57 (Sup. Ct. 2010).

179. *See* Kerr, *supra* note 146 (describing the lack of an "inside/outside distinction" on the Internet).

180. *See* United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. 2007) (finding no reasonable expectation of privacy in subscriber information, length of stored files, and other non-content information provided to ISPs), *vacated*, 648 F.3d 1 (1st Cir. 2011).

no right of privacy on the Internet, either because it is seen as "public" and not "private,"[181] or because communicating via the Internet necessitates sharing with a third party.[182] Therefore it is critical in the online context that courts employ the broader, non-binary view of privacy that includes controlling the extent of disclosure, as opposed to the focus on preventing any disclosure at all. As noted above, information posted or communications divulged on the Internet are, out of necessity, divulged to third parties. And secondly, in a binary world, the Internet is clearly more likely to be viewed as public than private.

This Article asks whether the exceptions made by courts in the offline context to the rule of no privacy in a "public" place can be extended to the online sphere. There are two problems with the online application of these exceptions. First, Internet privacy cases are not easily analogized to the exception made offline for cases involving harassment or overzealous surveillance in a public place.[183] Also problematic is the exception for inherently private activity, because the Internet has no equivalent of a restroom or changing room.[184] Instead, the best analogy to offline privacy in an otherwise public place is the recognition of individuals' privacy-ensuring measures. Courts should look at evolving custom and social mores in determining the reasonableness of online privacy expectations, and to the one tool that exists both offline and online for those seeking to preserve privacy expectations, the affirmative use of available privacy controls. Recognition of such "user controls" is essential for allowing some privacy in the online context.[185]

---

181. *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 863 (Ct. App. 2009) ("By posting the article on MySpace.com, Cynthia opened the article to the public at large. Her potential audience was vast.").

182. *D'Andrea*, 497 F. Supp. 2d at 120.

183. The closest analogy may be to cases alleging harassment in the context of "virtual worlds." *See* Michael J. Bugeja, *Second Thoughts About Second Life*, CHRON. HIGHER EDUC. (Sept. 14, 2007), http://chronicle.com/article/Second-Thoughts-About-Secon/46636 (describing allegations of virtual sexual harassment and even rape in Second Life).

184. There could be special protection for communications or postings concerning or displaying inherently private activity in Internet spaces set up specifically for that activity, although the court would have to find the disclosure was not purposeful. *See* RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977) (noting that a person has no claim for violation of privacy in a matter purposefully revealed to the public). In an early Internet case, *Michaels v. Internet Entertainment Group, Inc.*, the court rejected the argument that the plaintiffs had no reasonable expectation of privacy in the contents of a sex tape, despite the fact that part of the tape had been leaked on the Internet. Michaels v. Internet Entm't Grp., Inc., 5 F. Supp. 2d 823, 840-41 (C.D. Cal. 1998).

185. *See D'Andrea*, 497 F. Supp. 2d at 121 (arguing that individual privacy-enhancing measures such as password-protection should, like "locks, bolts, and burglar alarms," evidence a person's reasonable expectation of privacy in the contents of that website (quoting 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.6, at 721 (4th ed. 2006)) (internal quotation marks omitted)).

1. Non-Content Addressing and Subscriber Information

One area where courts have consistently found no expectation of privacy is with respect to email to and from addresses, including Internet protocol (IP) addresses. Here, the courts analogize to the content versus non-content distinction made in *Smith v. Maryland* with respect to pen registers. As the US Court of Appeals for the Ninth Circuit stated in *United States v. Forrester*:

> *Smith* based its holding that telephone users have no expectation of privacy in the numbers they dial on the users' imputed knowledge that their calls are completed through telephone company switching equipment. Analogously, e-mail and Internet users have no expectation of privacy in the to/from addresses of their messages or the IP addresses of the websites they visit because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of the information.[186]

In contrast, the underlying contents of email addresses or webpages visited are protected: "[T]he Court in *Smith* and *Katz* drew a clear line between unprotected addressing information and protected content information."[187]

Courts have looked at the agreement between the subscriber and ISP "to assess whether a subscriber's subjective expectation of privacy in his non-content subscriber information was one that society would be willing to accept as objectively reasonable."[188] Thus, the court in *United States v. Hambrick* found no reasonable expectation of privacy in subscriber information because the agreement between the defendant and the ISP "did not proscribe MindSpring from revealing defendant's personal information to nongovernmental entities."[189] Likewise, in *Freedman v. America Online, Inc.*, the court found that an AOL user had no expectation of privacy when his subscriber agreement "expressly informed Plaintiff that it may, in limited circumstances, reveal his subscriber information."[190]

186. United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007) (citation omitted) (citing Smith v. Maryland, 442 U.S. 735, 742, 744 (1979)); *see also* Freedman v. AOL, Inc., 412 F. Supp. 2d 174, 182-83 (D. Conn. 2005); United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

187. *Forrester*, 512 F.3d at 510.

188. *Freedman*, 412 F. Supp. 2d at 182.

189. *Hambrick*, 55 F. Supp. 2d at 508.

190. *Freedman*, 412 F. Supp. 2d at 183.

2. Content of Email

a. Following the Misguided Approach of Privacy as Secrecy

In addition to finding a waiver of privacy based on voluntary provision of non-content information to third parties, courts have also followed the analogous "misplaced trust" doctrine to find no expectation of privacy where third parties forward emails or chat room communications to law enforcement officials.[191] Certainly if the recipient of an email or chat room communication either is a government agent or in fact provides the communication to a government agent, there is no privacy violation.[192] But some courts have taken that doctrine beyond a user accepting the risk that a recipient of a communication will disclose it to the police. These courts find no expectation of privacy to exist in email once the user sends it simply because the email could be forwarded to others.[193]

In the 1996 case *United States v. Maxwell*, the FBI obtained a search warrant for AOL's computer bank in an investigation of child pornography, and uncovered emails from the defendant's account.[194] After his conviction, Maxwell appealed, challenging the search.[195] Because it found the search warrant to be invalid, the important issue before the court was whether Maxwell had a reasonable expectation of privacy in his email to necessitate the warrant.[196] The court found that, even though a person may have a limited privacy interest under the Fourth Amendment in email transmissions, that privacy expectation disappears once the email is received and opened: "[T]he transmitter of an e-mail message enjoys a reasonable expectation that police officials will not intercept the transmission without probable cause and a search warrant. However, once the transmissions are received by another person, the transmitter no longer controls its destiny."[197]

---

191. *See* United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (finding no expectation of privacy in contents of an email once it is received, just as there is no privacy in the contents of a letter "once the letter is received and opened" (quoting United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996)) (internal quotations omitted)); Commonwealth v. Proetto, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) (finding no reasonable expectation of privacy in communications via email and chat room forwarded by the victim to the police).

192. *See* United States v. Hoffa, 385 U.S. 293, 302 (1966) (discussing the "misplaced trust" doctrine).

193. *See* United States v. Maxwell, 45 M.J. 406, 418-19 (C.A.A.F. 1996).

194. *Id.* at 413-14.

195. *Id.* at 415.

196. *Id.* at 419-24.

197. *Id.* at 418.

A few other cases have favorably cited *Maxwell*'s reasoning, but without much analysis.[198] The court in *Commonwealth v. Proetto* followed the reasoning of the *Maxwell* decision, but in *Proetto* the email conversations were actually forwarded by their recipient to police.[199] Therefore, there was no reasonable expectation of privacy in those emails (or in recorded chat room conversations provided to the police) for purposes of the defendant's claims based on the Fourth Amendment and the ECPA.[200] The court did not need to employ the broad reasoning in *Maxwell* because the case fell neatly within the misplaced trust doctrine. But instead, the *Proetto* court stated that, because the recipient of the email messages could forward them to anyone, the defendant had no reasonable expectation of privacy in them.[201]

Other cases applying a rigid view of the third-party doctrine include *McLaren v. Microsoft Corp.*,[202] and *Smyth v. Pillsbury Company*.[203] In *McLaren*, the court found no legitimate expectation of privacy in an employee's email for purposes of analyzing his intrusion upon seclusion claim, despite the fact that the emails were stored under a private, personal password with Microsoft's consent: "Even so, any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third-party."[204] Similarly, in *Smyth*, the court found no reasonable expectation of privacy in emails sent over a company email system and intercepted by company management, despite company statements that all such email would remain private:

> [W]e do not find a reasonable expectation of privacy in e-mail communications voluntarily made by an employee to his supervisor over the company e-mail system notwithstanding any assurances that such communications would not be intercepted by management. Once plaintiff communicated the alleged unprofessional comments to a

198. *See, e.g.*, United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004) (noting that an individual may not have an expectation of privacy in email that has reached its recipient and upholding the computer monitoring condition of probation, but remanding on issue of whether the condition was overbroad); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding, *inter alia*, no reasonable expectation of privacy in email that had already reached its recipient, although there was a question as to whether email had been accessed at all); United States v. Valdivieso Rodriguez, 532 F. Supp. 2d 332, 339 (D.P.R. 2007) (finding that officers had probable cause for a warrant seeking email subscriber information, and citing in passing authority for the proposition that a person has no reasonable expectation in email already received).

199. Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001).

200. *Id.*

201. *Id.*

202. McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999).

203. Smyth v. Pillsbury Co., 914 F. Supp. 97 (E.D. Pa. 1996) (dismissing the employee's claims for termination in violation of public policy and intrusion upon seclusion).

204. *McLaren*, 1999 WL 339015, at *4.

> second person (his supervisor) over an e-mail system which was apparently utilized by the entire company, any reasonable expectation of privacy was lost.[205]

The reasoning that finds email content no longer private once received, or no longer private simply because the emails must be transmitted over a network, is an unduly broad view of the misplaced trust and third party doctrines. Instead, courts should not find such a waiver of privacy simply because an email is received by its recipient. Those messages should instead remain private as against third parties, just as a conversation does not lose its privacy simply because a party to it could have—but did not—share that communication with another,[206] and just as an opened letter may remain private in the hands of its recipient.[207]

b. The Better Approach of Privacy As Control

The better line of authority finds no such waiver simply because email has been sent and received. A growing number of courts find a limited expectation of privacy in email, depending upon the method of storage and privacy protection given to the email by the specific email provider, as well as any representations made to the email user about the privacy with which the messages will be treated.[208]

First, in the employment context, courts have begun to look at whether the employer owns the computer or monitors the email system.[209] In *Brown-Criscuolo v. Wolfe*, the court considered four factors:

> (1) does the corporation maintain a policy banning personal or other objectionable use, (2) does the company monitor the use of the employee's computer or e-mail, (3) do third

---

205. *Smyth*, 914 F. Supp. at 101.

206. The wiretapped conversation in *Katz* did not lose its privacy simply because the other party to Katz's conversation could have shared its contents with the police. *See* Katz v. United States, 389 U.S. 347 (1967).

207. *Ex parte* Jackson, 96 U.S. 727, 732-33 (1878). The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers, and effects." U.S. CONST. amend. IV. The Supreme Court has noted in the context of the exclusionary rule that "[i]f letters and private documents can thus be seized and held and used in evidence against a citizen accused of an offense, the protection of the Fourth Amendment . . . is of no value." Mapp v. Ohio, 367 U.S. 643, 648 (1961) (quoting Weeks v. United States, 232 U.S. 383, 393 (1914)).

208. *See* Brown-Criscuolo v. Wolfe, 601 F. Supp. 2d 441, 449 (D. Conn. 2009); United States v. Long, 64 M.J. 57, 62-65 (C.A.A.F. 2006); United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000); Hoff v. Spoelstra, Nos. 272898, 275979, 276054, 276257, 2008 WL 2668298, at *9 (Mich. Ct. App. July 8, 2008).

209. *See Brown-Criscuolo*, 601 F. Supp. 2d at 449.

> parties have a right of access to the computer or e-mails, and (4) did the corporation notify the employee, or was the employee aware, of the use and monitoring policies?[210]

In *Brown-Criscuolo*, the court found that the employee had an expectation of privacy in her email based on these factors.[211] She had a password to her account known only to her and the computer system's administrator. [212] Moreover, the school district's computer use policy confirmed that employees had a limited privacy interest in their email, subject to routine maintenance and monitoring.[213] In addition, it was not, in fact, the practice of the school to monitor users' email accounts.[214] Finally, the school superintendent accessed the employee's email for a specific reason that was not pursuant to routine maintenance and monitoring.[215]

Courts have looked at similar factors where the employer is the government. In *United States v. Monroe*, the court found no reasonable expectation of privacy in a US Air Force Staff Sergeant's email on a government computer, when IT personnel discovered the emails, and a banner warned the user at log-on that monitoring could occur.[216] Also in *Hoff v. Spoelstra*, the court found no reasonable expectation of privacy in emails on a city's computer system, where the city's information systems policy stated that the emails were considered public property, subject to Freedom of Information Act requests, and that users should not expect any degree of privacy in their email messages.[217] Thus, banner warnings and policy statements can render unreasonable any expectation of privacy in an employer email.

Even where the employer does monitor email, courts have found a privacy interest to exist in some circumstances. Six years after deciding *Monroe*, the same court found in *United States v. Long* that the defendant retained a privacy interest in emails sent from and stored on a government computer, despite a log-on banner warning

---

210. *Id.* (quoting *In re* Asia Global Crossing, Ltd., 322 B.R. 247, 257 (Bankr. S.D.N.Y. 2005)). *In re Asia Global Crossing* found the record inadequate to determine whether employees had a reasonable expectation of privacy in emails on the company's server, where the company had access to the emails, because the parties disputed whether the company's policy—which limited email use to company business and warned of little privacy protection—was communicated to employees. *Asia Global Crossing, Ltd.*, 322 B.R. at 260-61.

211. *Brown-Criscuolo*, 601 F. Supp. 2d at 450.

212. *Id.* at 449.

213. *Id.*

214. *Id.* at 450.

215. *Id.*

216. United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000).

217. Hoff v. Spoelstra, Nos. 272898, 275979, 276054, 276257, 2008 WL 2668298, at *9 (Mich. Ct. App. July 8, 2008).

that the computer was subject to monitoring.[218] In this case, the defendant had her own personal password that was not known to the system administrator.[219] Furthermore, it was the administrator's general policy not to search emails, and the search was not work related but was for law-enforcement purposes.[220]

When the case does not involve an employer-owned or monitored email system, courts willing to consider user controls will look at the policy of the private email provider, including the method of storage of emails and the policy of the service provider concerning reading or disclosing users' emails.[221] Thus, in *Maxwell*, while the court ultimately found that the defendant's expectation of privacy in his email was lost when the email was received, the court found a reasonable expectation of privacy against interception of the email.[222] In doing so, it found persuasive the fact that AOL had a policy "not to read or disclose subscribers' email to anyone except authorized users, thus offering its own contractual privacy protection."[223]

3. Files Shared Via the Internet

In the context of computer files shared over networks, courts have looked at the employer's or ISP's policy, as well as the nature of the software and any protective measures taken by the user.[224] In *United States v. Heckenkamp*, the court found that the defendant had a reasonable expectation of privacy in computer files despite the fact that the computer was attached to the network of the university where he was a student and former employee. [225] "[T]here was no

---

218. United States v. Long, 64 M.J. 57, 64-65 (C.A.A.F. 2006).

219. *Id.* at 64.

220. *Id.* at 64-65.

221. *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996) (finding a limited reasonable expectation of privacy in emails transmitted on the AOL computer subscription service, where that system provided a level of privacy to users' emails, stored them on a centralized and privately owned computer bank, and followed a policy of not reading or disclosing those emails without a court order); *see also* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding a disclaimer on a website bulletin board system defeated any claim to privacy).

222. *Maxwell*, 45 M.J. at 417-18.

223. *Id.* at 417. This is similar to the subscriber information context. *Compare id.*, *with* Freedman v. AOL, Inc., 412 F. Supp. 2d 174, 183 (D. Conn. 2005) (discussing AOL subscriber agreement, which expressly permitted AOL to reveal account information in certain circumstances), *and* United States v. Hambrick, 55 F. Supp. 2d 504, 509 (W.D. Va. 1999) ("[T]here is nothing in the record to suggest that there was a restrictive agreement between the defendant and MindSpring that would limit the right of MindSpring to reveal the defendant's personal information to nongovernmental entities."), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

224. *See generally* United States v. Heckenkamp, 482 F.3d 1142, 1146-47 (9th Cir. 2007); United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *3-6 (D. Or. Jan. 28, 2010); United States v. Larson, 66 M.J. 212, 216 (C.A.A.F. 2008).

225. *Heckenkamp*, 482 F.3d at 1146.

announced monitoring policy on the network," and the university's policy stated that, "[i]n general, all computer and electronic files should be free from access by any but the authorized users of those files."[226] The defendant's computer was also password protected and located in his dormitory room.[227]

In contrast, in *United States v. Simons*, the court found no reasonable expectation of privacy in files downloaded from the Internet at the defendant's government workplace, where the public employer had a stated policy allowing it to audit, inspect, and monitor employees' Internet use.[228] Likewise, in *United States v. Larson*, the court found the defendant to have no reasonable expectation of privacy in pornographic material or web browser history stored on a government computer provided to him for official use, where a banner appeared at each log-on putting him on notice that the computer was "not to be used for illegal activity" and that it was subject to third-party monitoring.[229]

Also relevant is the type of network being used to share files. In *United States v. Ahrndt*, the court found that a police officer's access to an unsecured wireless network, where he was able to download the defendant's shared iTunes library folder containing child pornography, was not a search.[230] Analogizing to the expectation of privacy in cordless phones, the court found a diminished expectation of privacy in data transferred over unsecured wireless networks: "As a result of the ease and frequency with which people use others' wireless networks, I conclude that society recognizes a lower expectation of privacy in information broadcast via an unsecured wireless network router than in information transmitted through a hardwired network or password-protected network."[231]

Similarly, in *United States v. Borowy*, the court found that the FBI's actions in accessing shared files on the peer-to-peer file-sharing service LimeWire did not violate the defendant's Fourth Amendment rights, even though the defendant had attempted (unsuccessfully) to

---

226. *Id.* at 1147 (second alteration in original).

227. *Id.* (concluding the search was justified by the special-needs exception).

228. United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000).

229. *Larson*, 66 M.J. at 215-16; *see also* United States v. Barrows, 481 F.3d 1246, 1248-49 (10th Cir. 2007) (finding government employee lacked reasonable expectation of privacy in his personal computer (PC) where he brought the PC to work and connected it to the city network, but took no measures to password-protect it, limit other employees' access to it, or protect it from public inspection).

230. United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *9 (D. Or. Jan. 28, 2010).

231. *Id.* at *5.

engage a feature that would have prevented others from downloading or viewing file names.[232]

Nevertheless, at least one court has found a legitimate privacy interest in files shared via the Internet, based in part on the presence of a secure network configuration, albeit in a statutory, rather than tort or Fourth Amendment, context.[233] In *In re Google Street View Electronic Communications Litigation*, the plaintiffs brought a class action against Google based on its interception of data packets from plaintiffs' wireless networks using software installed on its Google Street View vehicles.[234] Google moved to dismiss the claims for violation of the Wiretap Act based on its argument that the WiFi broadcasts were "readily accessible to the general public" under the Act.[235] The court disagreed, noting that the plaintiffs pled that their networks were "configured to render the data packets, or electronic communications, unreadable and inaccessible without the use of rare packet sniffing software; technology allegedly outside the purview of the general public."[236]

The court distinguished *Google*'s facts from those in *Ahrndt*.[237] While both networks were unencrypted, the conduct of the defendant in *Ahrndt* "in operating his iTunes software with the preferences set to share, in conjunction with maintaining an unsecured wireless network router, diminished his reasonable expectation of privacy to the point that society would not recognize it as reasonable."[238] In contrast, the *Google* plaintiffs pleaded that, "although the networks themselves were unencrypted, the networks were configured to prevent the

232. United States v. Borowy, 595 F.3d 1045, 1048-49 (9th Cir.), *cert. denied*, 131 S. Ct. 795 (2010); *see also* United States v. Ganoe, 538 F.3d 1117, 1127 (9th Cir. 2008) (holding that there is no reasonable expectation of privacy in files on a computer, where defendant installed and used LimeWire file-sharing software, "thereby opening his computer to anyone else with the same freely available program," and where "he was explicitly warned before completing the installation that the folder into which files are downloaded would be shared with other users in the peer-to-peer network").

233. *In re* Google Inc. St. View Elec. Commc'ns Litig., 794 F. Supp. 2d 1067, 1070 (N.D. Cal. 2011).

234. *Id.*

235. *Id.* at 1073 (citing statutory definition of "readily accessible to the general public" in 18 U.S.C. § 2510(16) (2006)).

236. *Id.* at 1083; *see also id.* at 1082-83 ("Unlike in the traditional radio services context, communications sent via Wi-Fi technology, as pleaded by Plaintiffs, are not designed or intended to be public. Rather, as alleged, Wi-Fi technology shares a common design with cellular phone technology, in that they both use radio waves to transmit communications, however they are both designed to send communications privately, as in solely to select recipients, and both types of technology are architected in order to make intentional monitoring by third parties difficult." (citing S. REP. NO. 99-541, at 6 (1986))).

237. *Id.* at 1083-84 (citing United States v. Ahrndt, No. 08-468-KI, 2010 WL 373994, at *1, *8 (D. Or. Jan. 28, 2010)).

238. *Id.* at 1084 (quoting *Ahrndt*, 2010 WL 373994, at *8).

general public from gaining access to the data packets without the assistance of sophisticated technology."[239] Therefore, the user's affirmative action in using networks configured to render the data unreadable made the privacy expectation a reasonable one.[240]

4. Information Posted on a Website

In contrast to the limited protection for email and file-sharing content, courts have given little privacy protection to postings on an internet forum or chat room,[241] or to other information posted to a website.[242] As in the email context, these courts have given significance to language appearing in website policies or banner announcements indicating that such material is not private.[243] One court has found a reasonable expectation of privacy to exist in communications posted to a website, and that finding was based on the website creator's explicit privacy-ensuring measures.[244]

---

239. *Id.*

240. *Id.* at 1083. While the plaintiffs in *Google* did not allege that their Fourth Amendment rights had been violated, the court's analysis of the ECPA is still instructive in a reasonable expectation of privacy context. *See generally id.* Indeed, the defendant in *Ahrndt* argued that his expectation of privacy was *per se* unreasonable because the search was illegal under the ECPA. *Ahrndt*, 2010 WL 373994, at *3.

241. *See* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding that users of a bulletin board system lacked a reasonable expectation of privacy in messages they posted, where a disclaimer stated "that personal communications were not private"); United States v. Maxwell, 45 M.J. 406, 418-19 (C.A.A.F. 1996) (denying a privacy expectation to transmissions like chat room conversations that are "sent to the public at large").

242. *See* BidZirk, LLC v. Smith, No. 6:06-109-HMH, 2007 WL 3119445, at *5 (D.S.C. Oct. 22, 2007) (finding no invasion of privacy where defendant's blog included a link to another website that posted, with permission, a picture of the plaintiffs); Four Navy Seals v. AP, 413 F. Supp. 2d 1136, 1145 (S.D. Cal. 2005) (finding no claim for publication of private facts based on newspaper's publication of photographs a reporter copied from "smugmug," a non-password protected website where the wife of a Navy Seal, erroneously believing the website was private, had posted photographs); United States v. Gines-Perez, 214 F. Supp. 2d 205, 225-26 (D.P.R. 2002) (finding that police officers' use of a photograph downloaded from the Internet to identify a suspect did not violate the suspect's Fourth Amendment rights, where the website was "under construction" but not password-protected or located on a secure network and contained no warnings or other protective measures controlling access to the web page or the photograph), *vacated*, 90 F. App'x 3 (1st Cir. 2004); *see also* Stern v. O'Quinn, 253 F.R.D. 663, 682 (S.D. Fla. 2008) (denying work-product protection for information voluntarily disclosed to the author of a book and in Internet chat rooms, as there was no evidence the defendants "did not purposefully and voluntarily" make those disclosures, but the evidence showed that "the types of disclosures made (*i.e.*, to the author of a book and on the Internet) [were] entirely inconsistent with a desire to maintain the privacy of the information disclosed" because "books are published and statements are posted on the Internet precisely for the purpose of making them accessible to anyone and everyone"); McMann v. Doe, 460 F. Supp. 2d 259, 268 (D. Mass. 2006) (finding no invasion of statutory right to privacy where defendant publicized on his website the plaintiff's posting on a public message board).

243. *See, e.g.*, *Guest*, 255 F.3d at 333.

244. Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 872 (9th Cir. 2002).

In *Konop v. Hawaiian Airlines, Inc.*, an airline pilot "maintained a website where he posted bulletins critical of his employer."[245] The pilot had set up the website to allow only certain people to register for access to it.[246] The airline's vice president received permission from two of the pilots on the list to create accounts in their names and thereby gain access.[247] When the plaintiff pilot learned of these actions, he brought claims against the airline, including claims based on the Wiretap Act and the SCA.[248] First, the court noted that "[t]he legislative history of the ECPA suggest[ed] that Congress wanted to protect electronic communications that are configured to private, such as email and private electronic bulletin boards."[249] In this instance, the Act also protected the plaintiff's website since, by its configuration, it was not readily accessible to the public.[250] Second, the court reversed the district court's finding that the airline was exempt from liability under the SCA because the vice president had used the name of an authorized "user" to gain access to the site.[251] Instead, that access was not authorized because the pilots included in the list were not the ones signing up as the user.[252]

Affirmative user controls will fail to secure a privacy interest where the court finds them ineffective. In *Snow v. DirecTV, Inc.*, the court found no violation of the SCA based on the defendants' accessing a website that required registration, password creation, and a statement affirming that the registrant was not associated with DirecTV.[253] The court reasoned that the ECPA specifies that its provisions should not be construed to prohibit access to "an electronic communication system that is configured so that such electronic

245. *Id.*

246. *Id.* at 872-73. The language displayed on the home page of the website also warned that only certain people—not airline management—were allowed to access the site and that users were required to abide by the site's confidentiality requirement and other terms and conditions. *Id.* at 875 n.3.

247. *Id.* at 873.

248. *Id.*

249. *Id.* at 875.

250. *Id.*

251. *Id.* at 879-80.

252. *Id.* at 880.

253. Snow v. DirecTV, Inc., 450 F.3d 1314, 1321-22 (11th Cir. 2006). The plaintiff in *Snow* created his website in response to DirecTV's "nationwide effort to stop the pirating of its encrypted satellite transmissions" by bringing thousands of anti-piracy actions in court. *Id.* at 1316. Snow's website—a "private support group" for "'individuals who have been, are being, or will be sued by any Corporate entity'"—contained language "expressly forbid[ding] access by DIRECTV [sic] and its agents." *Id.*

communication is *readily accessible to the general public.*"[254] Despite the fact that the website required a user to register, create a password, and affirm his non-association with DirecTV, the court stated, "[n]othing inherent in any of these steps prompts us to infer that access by the general public was restricted."[255] The court distinguished these facts from those in *Konop*, and indicated that the "self-screening methodology" employed by the defendant was "insufficient to draw an inference that the website is not readily accessible to the general public."[256]

In a challenge to a school district's decision to expel a student based on his creation of a website that was highly derogatory toward his principal and one of his teachers, the court in *J.S. v. Bethelehem School District* reviewed the school district's finding that the student had no expectation of privacy in the website.[257] Prior to accessing the website, a visitor "had to agree to a disclaimer" that indicated that the "visitor was not a member of the [school's] faculty or administration and . . . did not intend to disclose the identity of the web-site creator."[258] When the school's principal learned of the site from an anonymous email sent to a faculty member, the principal contacted the local police and eventually expelled the student.[259] The court found that the school district had not violated the student's right to privacy when it accessed the website, noting that the site was not "protected," so "any user who happened upon the correct search terms could have stumbled upon" it.[260] So, while the website creator had attempted to employ privacy controls, those controls were not effective; therefore, the website creator could not reasonably expect privacy.[261]

---

254. *Id.* at 1320 (quoting 18 U.S.C. § 2511(2)(g) (2006)) (internal quotation marks omitted).

255. *Id.* at 1321-22.

256. *Id.* at 1322.

257. J.S. v. Bethlehem Area Sch. Dist., 757 A.2d 412, 415 (Pa. Commw. Ct. 2000), *aff'd*, 807 A.2d 847 (Pa. 2002). While the case involved a student, which could implicate different legal issues, the court's analysis made no reference to that fact. *Id.*

258. *Id.* (failing to clarify whether that agreement was via clicking or otherwise).

259. *Id.* at 417.

260. *Id.* at 425. The court analogized to a person's lack of privacy rights in email once it is received:

> Likewise, the creator of a web-site controls the site until such time as it is posted on the Internet. Once it is posted, the creator loses control of the web-site's destiny and it may be accessed by anyone on the Internet. Without protecting the web-site, the creator takes the risk of other individuals accessing it once it is posted.

Id.

261. *Id.* The school district's findings of fact during the expulsion hearings included that "[t]here was no password required to access the Website and although a 'disclaimer' appears, the custom on the Internet is to ignore disclaimers," and that "[t]he Website was not 'password

Finally, in *United States v. D'Andrea*, the court found that the defendants had no reasonable expectation of privacy with respect to the content of a password-protected website, where an anonymous person told the police about the website (which contained images of child abuse and child pornography), and provided the police with the log-in name and password.[262] The court properly found the case to fall within the "assumption of the risk" exception whereby "when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs, the Fourth Amendment does not prohibit government use of that information."[263] So while the user employed privacy controls, those controls were circumvented when a third party gave police his passwords. [264]

5. Online Social Networks

Courts have yet to find any reasonable expectation of privacy under tort law or the Fourth Amendment for information shared on an OSN.[265] Most decisions finding a lack of privacy in these contexts are correct, since the user did not employ any privacy-ensuring measures.[266] But as explained further below, such privacy settings are on the rise, and courts should give them effect.[267]

---

protected' and could be found by 'links'—there was access from other sites." *Id.* at 416 (citation omitted).

262. United States v. D'Andrea, 497 F. Supp. 2d 117, 122-23 (D. Mass. 2007), *vacated*, 648 F.3d 1 (1st Cir. 2011).

263. *Id.* at 123 (quoting United States v. Jacobsen, 446 U.S. 109, 117 (1984)). The court also found the case to be governed by the rule that a person has "no reasonable expectation of privacy in matters voluntarily disclosed or entrusted to third parties." *Id.* at 120. This third-party waiver includes "subscriber information, the length of their stored files, and other noncontent data to which service providers must have access." *Id.* The *D'Andrea* court discussed at length the scholarship of Professor Warren LaFave, who argues that individual privacy-enhancing measures such as password-protection should, like "locks, bolts, and burglar alarms," evidence a person's reasonable expectation of privacy in the contents of that website. *Id.* at 121 (quoting 1 WAYNE R. LAFAVE, SEARCH AND SEIZURE § 2.6, at 721 (4th ed. 2006)) (internal quotation marks omitted); *see also* Warshak v. United States, 490 F.3d 455, 470-71 (6th Cir.), *vacated*, 2007 U.S. App. Lexis 23741 (6th Cir. 2007).

264. *D'Andrea*, 497 F. Supp. 2d at 122-23.

265. *See* Sandler v. Calcagni, 565 F. Supp. 2d 184, 197 (D. Me. 2008) (holding there was no claim for invasion of privacy based on publication of plaintiff's revelation found on her publicly-accessible Myspace.com webpage concerning "her decision to seek psychological help during college"); Dexter v. Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 n.4 (Ohio Ct. App. May 25, 2007) (finding no reasonable expectation of privacy in writings on MySpace account open to public view).

266. *See, e.g.*, *Dexter*, 2007 WL 1532084, at *6 n.4 (affirming that a party could not exclude from evidence statements about her drug usage made on Myspace).

267. *See, e.g.*, Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 991 (C.D. Cal. 2010) (finding that webmail and private messaging "are inherently private such that stored

Scholars have noted that OSN users expect more privacy in what they divulge on social networking sites than the law provides, and consider information to be private "as long as it is not disclosed outside of the network to which they initially disclosed it."[268] Furthermore, OSNs themselves are responding to users' concerns about privacy by implementing user controls that further that belief. Recently, Facebook renamed the broad setting allowing disclosure to any viewer from "Everyone" (which might have suggested "Everyone on Facebook" as opposed to "Everyone with an Internet Connection") to "Public," an explicit warning that the setting allows public viewing beyond Facebook users.[269] Facebook also has enabled its users to further control the extent their information is accessible to friends and sub-groups of friends, specifying that certain groups are "Open," "Closed," or "Secret."[270]

Facebook's latest user agreement gives the user a basis for believing some communications will remain private: "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."[271] In addition, Facebook makes a clear distinction between using public and private settings: "When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)."[272] Unfortunately, application of the law often outright contradicts such representations.[273]

a. OSNs in the Law

One case that has received a lot of attention from privacy scholars is *Moreno v. Hanford Sentinel, Inc.*[274] In that case, a young woman posted to her "online journal on MySpace.com" an entry titled "An [O]de to Coalinga," which was a derogatory article about her

---

messages are not readily accessible to the general public" under the SCA, but remanding for further evidentiary findings on the issue of whether Facebook wall postings and Myspace comments are given restricted access under the plaintiff's privacy settings).

268. *See* Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1002 (2009) (presenting results of an empirical study regarding personal information protection and expectations of privacy on online social networks).

269. *See Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php (last updated Apr. 26, 2011).

270. *Id.*

271. *Id.*

272. *Id.*

273. *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656-57 (Sup. Ct. 2010).

274. Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858 (Ct. App. 2009).

hometown.[275] The woman removed the "ode" from her journal six days later.[276] In the meantime, however, the principal at the high school in Coalinga, where the young woman's sister still attended, submitted the ode to the local paper, which published it in the letters to the editor section.[277] The community response to the letter was extreme: the young woman's family received death threats, someone fired a shot at their home, the father had to close his family business, and the family was forced to move away.[278] They then brought suit against the newspaper for invasion of privacy, specifically public disclosure of private facts.[279]

The court noted that "a crucial ingredient of the applicable invasion of privacy cause of action is a public disclosure of *private facts*."[280] Because the young woman published the ode on MySpace.com, which the court referred to as a "hugely popular Internet site," the posting was open to the "public eye" and she could not have had a reasonable expectation of privacy with respect to its contents.[281] While acknowledging that a fact may be private even when the expectation of privacy is not absolute, the court rejected the plaintiffs' claim that the ode was not meant to be made "public" and was taken down after a short time.[282] The court did not discuss the issue of privacy settings or other affirmative ways of making information posted online less "public."[283]

In contrast, in *Romano v. Steelcase Inc.*, the OSN disclosures at issue were designated as private under the OSN guidelines, but the New York Supreme Court still found no privacy interest.[284] The defendant sought access to the plaintiff's current and historical Facebook and MySpace pages and accounts, believing such information to be inconsistent with the plaintiff's claims for injuries and loss of enjoyment of life.[285] The defendant based this argument in part on what the court referred to as the "public portions" of the

275. *Id.* at 861.
276. *Id.*
277. *Id.*
278. *Id.*
279. *Id.*
280. *Id.* at 862.
281. *Id.*
282. *Id.* at 863; *see also* Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 43-45 (Minn. Ct. App. 2009) (finding the posting of information to a non-password protected or otherwise restricted website constitutes "publicity" for purposes of invasion of privacy, even though the information was taken down within two days).
283. *Moreno*, 91 Cal. Rptr. 3d at 863.
284. Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 656-57 (Sup. Ct. 2010).
285. *Id.* at 651.

plaintiff's MySpace and Facebook pages.[286] The plaintiff argued that such disclosure would violate her right to privacy.[287]

In considering whether to grant the disclosure, the court noted the broad scope of discovery under New York law.[288] The court also explained that the plaintiffs should not be permitted to shield necessary information from discovery when they have put their physical condition at issue.[289] The court noted that both social networking sites are geared toward the facilitation of sharing of information,[290] and both sites allow the user to implement privacy settings to restrict shared information.[291] Agreeing with the defendant that the information sought was "both material and necessary to the defense," the court required disclosure:

> In light of the fact that the *public* portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the *private* portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action.[292]

In rejecting the plaintiff's argument that disclosure would violate her right to privacy, the court reasoned that "neither Facebook nor MySpace guarantee complete privacy," and their user agreements warn users that profiles are "public spaces."[293] Moreover, Facebook's privacy policy cautions users that "[a]lthough we allow you to set privacy options that limit access to your pages, . . . no security measures are perfect or impenetrable" and information posted or shared with third parties "may become publicly available."[294] The court thus found no distinction between the public and private portions of the plaintiff's accounts: "[W]hen Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her

---

286. *Id.* at 654.

287. *Id.* at 652-53 (indicating that the court had reviewed the parties' submissions "as well as the applicable federal statutory law, specifically the Stored Communications Act, which prohibits an entity, such as Facebook and MySpace from disclosing such information without the consent of the owner of the account," but failing to address the SCA in its opinion (citation omitted)).

288. *Id.* at 652.

289. *Id.*

290. *Id.* at 653-54.

291. *Id.* at 654.

292. *Id.* (emphasis added).

293. *Id.* at 656. While the discovery context is distinguishable from the context of other privacy case law, the court here used Fourth Amendment and common law privacy precedents to determine whether the plaintiff had an expectation of privacy in the material sought in discovery. *Id.* at 655-57.

294. *Id.* at 656-57.

personal information would be shared with others, notwithstanding her privacy settings."[295]

The court failed to give any weight to the plaintiff's affirmative action in restricting her disclosures via her privacy settings.[296] To the court, disclosure on an OSN was equivalent to public disclosure, regardless of her efforts to limit her audience.[297] This traditional view of privacy as secrecy fails to recognize any right to control the extent of that disclosure. While the court may have properly ordered discovery even if it had recognized a privacy interest in the online social networking posts,[298] the court's failure to differentiate based on the plaintiff's affirmative user controls is a failure to view privacy as the right to control disclosure in addition to the right to prevent disclosure.

The US District Court for the Central District of California took a better approach in *Crispin v. Christian Audigier, Inc.*[299] That case involved a discovery subpoena directed to Facebook, MySpace, and the web-hosting service Media Temple, Inc.[300] The defendant alleged that the plaintiff's communications on these media were relevant to his claims for copyright infringement and breach of contract and were significant to the measure of damages.[301] The plaintiff sought to quash the subpoenas on the basis that they violated the SCA and his privacy rights.[302]

The court quashed the subpoena requests for webmail and private messaging because "those forms of communications media are inherently private such that stored messages are not readily accessible to the general public" under the SCA.[303] With respect to the subpoenas seeking Facebook wall postings and MySpace comments, however, the court remanded to a magistrate judge for further evidentiary findings concerning the plaintiff's privacy settings. The court suggested that if privacy settings restricted access to plaintiff's postings, then a subpoena would be improper:

---

295. *Id.* at 657.

296. *Id.*

297. *Id.* at 656-57.

298. Courts have often found that the plaintiff has waived such a privacy right by bringing a lawsuit and putting her physical condition at issue. *See, e.g.*, Ledbetter v. Wal-Mart Stores, Inc., No. 06-CV-01958-WYD-MJW, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (ordering discovery of information from plaintiffs' Facebook, Myspace, and Meetup.Com accounts based in part on the finding that they waived their doctor-patient privilege concerning their injuries when they filed the lawsuit to recover based on those injuries).

299. Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965 (C.D. Cal. 2010).

300. *Id.* at 968-69.

301. *Id.* at 969.

302. *Id.*

303. *Id.* at 991.

> Given that the only information in the record implied restricted access, the court concludes that Judge McDermott's order regarding this aspect of the Facebook and MySpace subpoenas was contrary to law. Because it appears, however, that a review of plaintiff's privacy settings would definitively settle the question, the court does not reverse Judge McDermott's order, but vacates it and remands so that Judge McDermott can direct the parties to develop a fuller evidentiary record regarding plaintiff's privacy settings and the extent of access allowed to his Facebook wall and MySpace comments.[304]

The court thus viewed the privacy to be accorded to the plaintiff's Facebook and MySpace postings as dependent upon whether he used privacy controls.[305] While the discovery and SCA contexts are different from privacy torts, which are in turn different from the Fourth Amendment context, the courts' analyses in these cases is instructive in the consideration that the law should give to the use of privacy settings in various legal contexts.

IV. A FRAMEWORK FOR REASONABLE EXPECTATIONS OF PRIVACY IN ONLINE COMMUNICATIONS

This Article suggests that courts need to apply more analysis to questions of privacy online and exceed the bounds of the binary public/private distinction. Thus, in any case where a person claims a reasonable expectation of privacy based on a communication or disclosure online, the court should, in addition to traditional doctrine, consider four factors.

The first factor is the existence of a user agreement or employer policy governing the use of the specific communication mechanism or providing for monitoring of that use. While the user does not typically control the terms of such an agreement, she decides to communicate online subject to those terms, and conceivably users could shop for better privacy terms when choosing ISPs or employers. Acknowledging such agreements would also have the benefit of predictability for their users. The Supreme Court noted in dicta in *Quon* that the question of whether Quon had a reasonable expectation of privacy in messages sent from and received on his City-provided pager was in part governed by the City's Computer Policy, which provided for no such privacy.[306]

Second, regardless of any specific policy, the extent to which third parties are actually given access to the communications or the communications are protected from disclosure by third parties, such as employers or ISPs, can give rise to expectations of privacy. This

---

304. *Id.* (footnote omitted).

305. *See id.*

306. City of Ont. v. Quon, 130 S. Ct. 2619, 2629 (2010).

may include informal policies of not viewing employees' email or an ISP's unstated policy of sharing IP addresses with third parties. Again in *Quon*, the Court noted that City officers' written and oral statements and actions might "overr[i]de" the official policy concerning privacy of the text messages.[307]

Third, courts should only give policies or practices credence if the user has notice of those policies or practices. The importance is the user's choice to increase or decrease his security through such controls or lack thereof. Therefore, the notice given to the user of the user agreement, employer policy, or practice of giving access to or protection from third parties is critical. If the user is not given notice of these terms or practices, he should not be bound to them.[308]

Fourth, the court should consider the availability and affirmative use of privacy-enhancing controls that increase the likelihood of the communication being protected from disclosure to people other than the chosen recipient(s). Such controls include, but are not limited to, (1) passwords limiting access to email accounts or wireless networks, (2) encryption technology that inhibits translation of communications, (3) network configuration that does or does not allow access to the public, and (4) privacy settings limiting disclosure to certain people, such as those available to OSN users. The nature of these controls is limited only by technology, and they will continue to develop. Courts should consider the controls that are available and in use, their effectiveness, and the person's decision to employ or not employ such measures. In the Fourth Amendment context, the misplaced trust doctrine will still influence the legal effect of using these controls; so that if a third party gives police a person's password, then the privacy of that password disappears. But the mere possibility that a third party could access the password or forward an email should not defeat privacy protections.

These factors can apply to various contexts in which privacy issues arise, and they are consistent with the growing weight of authority with respect to cases involving email and file sharing.[309] The biggest change that will result from the application of these factors is in the case of OSNs, where most courts have yet to give any effect to user-generated controls.[310] This analysis will result in a different outcome in email cases like *McLaren v. Microsoft*, where the

307. *Id.*at 2629, 2631.

308. *See id.* at 2630 ("[E]mployer policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated.").

309. *See supra* Parts III.B.2.b-III.B.3.

310. *See supra* Parts III.A.5-III.B.

court found no legitimate expectation of privacy in the employee's email despite his decision to store those emails under a private, personal password.[311] Also, it will change the analysis in a case like *Romano*, where the plaintiff restricted the public nature of her OSN disclosure via her privacy settings.[312]

V. CONCLUSION

Because online communications are ubiquitous and increasing in importance, some privacy is necessary. A number of courts have correctly found protection for email content, online file sharing over protected networks, and website postings, where the user enables privacy-enhancing measures. Courts are correct to reject the argument that a person lacks a reasonable expectation in email content simply because it is capable of being recorded and forwarded to others.

In addition, courts are correct to take into consideration the stated and unstated policies of employers, websites, and online social networks with respect to the privacy given to content to which they have access. They are correct to fault Internet users who claim privacy despite forgoing any privacy-enhancing measures. But where, as in *Romano*, the plaintiff did employ available privacy settings,[313] the courts should acknowledge those measures. The affirmative choice of OSN users to set their privacy settings reflects their reasonable expectations of the privacy given those communications, and should not be ignored by the law.

Increasingly more often, OSN users are posting information with the expectation that the OSN will keep that information private. When Facebook tells its users that some disclosures are "Closed" or "Secret," and that the user can control how content and information she posts is shared "through [her] privacy and application settings,"[314] courts should ensure that such promises are more than empty words. In applying the framework proposed in this Article, courts will give the same deference to user controls on OSNs that they have begun to do offline and in other online contexts. The extent of that protection will depend upon the availability and effectiveness of those controls, as well as courts' interpretations of societal interests in recognizing the reasonableness of privacy expectations on the Internet.

---

311. *See* McLaren v. Microsoft Corp., No. 05-97-00824-CV, 1999 WL 339015 (Tex. App. May 28, 1999); *supra* text accompanying notes 202-207.

312. *See* Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (Sup. Ct. 2010).

313. *See supra* Part III.B.5.