RETHINKING REASONABLE EXPECTATIONS OF PRIVACY IN ONLINE SOCIAL NETWORKS

By Bryce Clayton Newell*

Cite as: Bryce Clayton Newell, *Rethinking Reasonable Expectations of Privacy in Online Social Networks*, XVII RICH. J.L. & TECH. 12 (2011), http://jolt.richmond.edu/v17i4/article12.pdf.

I. INTRODUCTION

[1] In 1890, Warren and Brandeis "invented" the common law right to privacy in the United States.[1] They declared the need for a right to privacy – "to be let alone"[2] – because technological advancements

* Adjunct Instructor of Digital Media, Utah Valley University. B.S., Utah Valley State College; J.D., University of California, Davis School of Law; enrolling in the Ph.D. program in Information Science at University of Washington's Information School in Autumn 2011. I would like to extend special thanks to Dr. Eoin Carolan at University College Dublin for his supervision of the initial draft of this article and for his helpful advice; Coke Newell for his helpful insights and assistance throughout this process; my mother, Cindy Newell, and Aprille, Annalesa, Caden, and Aspen for their love and support. Finally, I'd like to thank the editors of the Richmond Journal of Law and Technology for their hard work and extremely helpful suggestions.

[1] *See* Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 1 (1979); *see also* DANIEL J. SOLOVE, THE DIGITAL PERSON 57 (Jack M. Balkin & Beth Simone Noveck eds., 2004).

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (quoting THOMAS M. COOLEY, COOLEY ON TORTS 29 (2d. ed. 1888)) (internal quotation marks omitted); *see also* William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

(photography) and business methods (yellow journalism) enabled the media to bring previously private details to the attention of a much larger audience.[3] Warren and Brandeis declared, "[i]nstantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[4] Because of the technological innovations of their day, the authors noted that, "solitude and privacy have become more essential to the individual" than in the past.[5] Concern over the sacredness of private and domestic life led to the conclusion that "[t]he law . . . must protect privacy on the principle of an 'inviolate personality.'"[6] In essence, Warren and Brandeis intended to introduce continental European privacy concepts into U.S. jurisprudence.[7]

[2] In the present day, new technologies continue to provide solid grounding for Warren and Brandeis' concerns. Internet technologies and various software platforms make it much easier to communicate and find information about others' online communication.[8] For many – especially the younger generation – the "sacred precincts" of private life have extended onto the information superhighway.[9] Individuals, both those with the right to do so and those without, increasingly post, upload, or share personal and private details, arguments and disputes, as well as

[3] *See* SOLOVE, *supra* note 1; Warren & Brandeis, *supra* note 2.

[4] Warren & Brandeis, *supra* note 2.

[5] *Id.* at 196; *see also* Avner Levin & Patricia Sanchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1012 (2009).

[6] Levin & Abril, *supra* note 5 (quoting Warren & Brandeis, *supra* note 2, at 205).

[7] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1204 (2004) ("[I]t is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant. For, though commentators have failed to recognize it, what the two authors set out to do was precisely to introduce the continental protection of privacy into America.").

[8] *See* Levin & Abril, *supra* note 5, at 1004.

[9] Warren & Brandeis, *supra* note 2; *see* Levin & Abril, *supra* note 5, at 1004.

intellectual property to public and private directories all over the Internet.[10] Indeed, as interpersonal communication itself has shifted increasingly to electronic media, the letter has transformed into multiple forms of e-mail, text messages, tweets, and posts on blogs, walls, forums, and chat rooms.[11] For some, yesterday's closet has become today's limited-access Facebook[12] or MySpace[13] profile.[14] Indeed, these services allow users to dictate whom they allow to access their posted content and online communication.[15] In fact, Facebook claims "[m]ore than 500 million active users," of whom fifty percent "log on to [the network] in any given day."[16] Despite the concerns put forth by Warren and Brandeis, recent judicial decisions have denied privacy protection in information posted to these online social networks ("OSNs").[17] These current privacy rulings have allowed personal information to be freely "proclaimed from the house-tops," despite what many feel are reasonable expectations to the contrary.[18] Law enforcement agencies have increasingly resorted to mining personal information posted to OSNs as a means to acquire information and identify individuals suspected of criminal activity.[19]

[10] *See* Levin & Abril, *supra* note 5, at 1004.

[11] *See* Charles N. Faerber, *Book Versus Byte: The Prospects and Desirability of a Paperless Society*, 17 J. MARSHALL J. COMPUTER & INFO. L. 797, 827 (1999).

[12] Facebook.com is a registered trademark of Facebook, Inc.

[13] MySpace.com is a registered trademark of MySpace, Inc.

[14] *See* Levin & Abril, *supra* note 5, at 1019.

[15] *See id.* at 1019-20.

[16] *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Apr. 9, 2011).

[17] *See, e.g.*, Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 864 (Cal. Ct. App. 2009); Leduc v. Roman, 2009 CarswellOnt 843, para. 27 (Can. Ont. Sup. Ct. J.) (WL); Murphy v. Perger, 2007 CarswellOnt 9439, para. 20 (Can. Ont. Sup. Ct. J.) (WL); *see also* Warren & Brandeis, *supra* note 2.

[18] Warren & Brandeis, *supra* note 2 (internal quotation marks omitted).

[19] *See, e.g.*, Matthew J. Hodge, Note, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 95-96 (2006);

OSNs have even played the stage for criminal confessions.[20] Often, robust privacy laws have failed to translate effectively when applied to these new technologies.[21]

[3] In an eighteenth century English case concerning copyright law, a dissenting Justice proclaimed: "[i]t is certain every man has a right to keep his own sentiments, if he pleases: he has certainly a right to judge whether he will make them public, or commit them only to the sight of his friends."[22] Regardless of how this right has developed in various jurisdictions, recent cases have not given it much weight where parties have tried to argue for privacy rights in information posted to online social networking profiles.[23] Recent cases have determined it irrelevant whether or not the profile is accessible to the public at large or only to the user's "friends."[24] These cases have involved intrusion by both private and public actors, therefore implicating both common law and constitutional theories of privacy protection in the United States.[25] Holding that there is

Autumn K. Leslie, Note, *Online Social Networks and Restrictions on College Athletes: Student Censorship?*, 5 DEPAUL J. SPORTS L. & CONTEMP. PROBS. 19, 33 (2008).

[20] *See, e.g.*, Press Release, U.S. Dep't of Justice, Myspace Confession Dooms North Augusta Bank Robber (May 28, 2009), *available at* http://columbia.fbi.gov/dojpressrel/2009/co052809.htm.

[21] SOLOVE, *supra* note 1, at 6-7.

[22] Millar v Taylor, (1769) 98 Eng. Rep. 201 (K.B.) 242; 4 Burr. 2303, 2379 (Yates, J., dissenting).

[23] *See generally* Sharon Nelson, John Simek & Jason Foltin, *The Legal Implications of Social Networking*, 22 REGENT U. L. REV. 1, 11-13 (2009) (noting several cases where police use information posted to social networking sites in their investigations).

[24] *See* Kathleen Elliot Vinson, *The Blurred Boundaries of Social Networking in the Legal Field: Just "Face" It*, 41 U. MEM. L. REV. 355, 375 (2010) ("Even if a user utilizes privacy settings, it may not protect her from blurred boundaries that result in subpoenas, discovery, ethical and legal issues, and private postings becoming public.").

[25] *See* Shawn C. Helms, *Translating Privacy Values with Technology*, 7 B.U. J. SCI. & TECH. L. 288, 313-14 (2001) (explaining that constitutional, common law, and legislative approaches to privacy only afford limited protection to private and public actors utilizing the Internet).

no reasonable expectation of privacy in Internet postings posits an unreasonable standard for those who view their limited-access posts on Facebook or MySpace as private, or at least quasi-private, where the number of "friends" who can access the information is high, and deserving of some sort of privacy protection.[26] However, some view these standards as dictated by individuals out of touch with the expectations of the millions of individuals using such online services.[27]

[4] Present United States privacy law – despite being made up of a patchwork of federal and state constitutional, statutory, and common law[28] – is predominantly based on the ideals of individual control, autonomy, and liberty from governmental intrusion,[29] despite the fact that its inspiration was an idea grounded on the importance of protecting human dignity and an "inviolate personality."[30] Comparatively, Europe has predominantly taken the second position – that privacy protects human

[26] *Cf.* David V. Richards, *Posting Personal Information on the Internet: A Case for Changing the Legal Regime Created by § 230 of the Communications Decency Act*, 85 TEX. L. REV. 1321, 1357 (2007) (explaining that it is necessary to revisit the law since much potential harm exists for Internet publication and the current law does not address online defamation or privacy invasion).

[27] *See* Leslie, *supra* note 19, at 34 ("Because online social networks are such a new media, originating less than five years ago, little public opinion as to the privacy interest expected therein is available since the Supreme Court has yet to deal with this issue." (footnotes omitted)).

[28] *See* SOLOVE, *supra* note 1, at 56 ("Information privacy law consists of a mosaic of various types of law: tort law, constitutional law, federal and state statutory law, evidentiary privileges, property law, and contract law."); Helms, *supra* note 25 ("Because there is no absolute right to privacy, constitutional claims, privacy torts, and federal statutes have created a patchwork of protection that protects privacy only within certain limited situations." (footnotes omitted)).

[29] *See* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 U. OTTOWA L. & TECH. J. 357, 360 (2005) (noting that Americans envision their privacy rights in terms of individual liberty, freedom and control).

[30] Warren & Brandeis, *supra* note 2, at 205.

dignity and fosters personal relationships.[31] The European view also promotes individual autonomy, although it does so in a different fashion and perhaps to a greater extent, as this Article suggests.[32] This view of privacy and individual autonomy embeds an element of human dignity into its analysis of an individual's reasonable expectation of privacy, rather than strictly tying reasonableness to ideas of control and waiver.[33] This conception is also more in line with the view that "[w]ithout our privacy, we lose 'our very integrity as persons' . . . ."[34] Privacy may signify a fundamental human right,[35] although this view has been challenged.[36]

[5] In the United States, the Fourth Amendment protects an individual's privacy interest in his person, home, and belongings from governmental intrusion when the individual has a subjective expectation of privacy that society is prepared to recognize as reasonable.[37] Similarly, courts in Canada and Europe have predicated privacy protection on a reasonable expectation standard by using the Canadian Charter of Rights and Freedoms ("Charter")[38] and the European Convention for the

[31] *See* Levin & Nicholson, *supra* note 29, at 390 (noting that European principles of privacy "guarantee the dignity of the individuals to whom the data belong").

[32] *See id*. ("What these principles do offer is protection of the public persona European citizens perceive themselves to have, protection of their image as they would like others to see it.").

[33] *See id*. at 388-89 (explaining that Europe is more concerned with preserving dignity protection among society's members than worrying about governmental intrusion).

[34] Whitman, *supra* note 7, at 1153 (quoting Charles Fried, *Privacy*, 77 YALE L.J. 475, 477 (1968)).

[35] *See* Charter of Fundamental Rights of the European Union, art. 7-8, 2000 O.J. (C 364) 10 [hereinafter European Charter]; Whitman, *supra* note 7, at 1153.

[36] *See* Whitman, *supra* note 7, at 1154-55.

[37] *See* Smith v. Maryland, 442 U.S. 735, 740 (1979); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[38] Canadian Charter of Rights and Freedoms, Part I of the Constitution Act, 1982, *being* Schedule B to the Canada Act, 1982, c.11 (U.K.) [hereinafter Canadian Charter], *available at* http://laws.justice.gc.ca/eng/charter/CHART_E.pdf.

Protection of Human Rights and Fundamental Freedoms ("ECHR")[39] to balance competing individual and public interests. This Article argues that the subjective expectation of privacy in information posted to limited-access social media websites – also described as the notion of "network privacy"[40] – is an expectation that society recognizes as reasonable in the twenty-first century.

[6] This Article furthers Professor Levin's and Professor Abril's reasoning to conclude that judges ought to adopt a more contemporary view of what constitutes a reasonable expectation of privacy in the context of digital communication and online "communities."[41] Implementing a more modern view is especially imperative when courts consider questions concerning limited-access information posted to online social media websites. Furthermore, this Article argues that European-based privacy laws focusing on the right to a private life, viewing privacy as a respected aid to relationship building and as a vehicle to protect personal dignity,[42] more accurately reflect the realities of the digital age and properly protect individual privacy on the Internet. By protecting autonomy through principles based on human dignity and recognizing that reasonable expectations can have their place in the context of online communities and digital communication, albeit often mediated and less private than some forms of offline communication, privacy laws would more effectively protect individuals and their constitutional concerns. Recent decisions of the European Court of Human Rights have laid the theoretical groundwork required for heightened protection of human dignity in online environments by espousing interpretations of reasonable expectations of privacy that, if applied to these online situations, would result in more protection for users posting information to OSNs.

---

[39] European Convention for the Protection of Human Rights and Fundamental Freedoms, art. 8, Apr. 11, 1950, 213 U.N.T.S. 221 [hereinafter ECHR], *available at* http://www.echr.coe.int/NR/rdonlyres/D5CC24A7-DC13-4318-B457-5C9014916D7A/0/EnglishAnglais.pdf (entered into force Sept. 3, 1953).

[40] Levin & Abril, *supra* note 5, at 1045.

[41] *See generally id.* at 1047 (arguing that privacy laws should change to focus more on the contemporary and informally recognized "notion of network privacy").

[42] *See* Levin & Nicholson, *supra* note 29, at 388.

II. DIVERGENT NOTIONS OF PRIVACY: DIGNITY, LIBERTY, OR CONTROL?

[7] Commentators around the world have debated the proper theoretical basis on which privacy ought to be protected.[43] The two most prevalent theories of privacy in the Western world are based on: 1) the right to control the release of personal information, and 2) the importance of protecting human dignity and fostering human relationships.[44] Note, however, that "that the concept of privacy is embarrassingly difficult to define."[45] To segment privacy regimes into exclusive theoretical groups – or even attempt to define privacy in a comparative context – requires generalization that will not always yield wholly accurate results.[46] That being said, such a conceptual exercise provides a helpful foundation for privacy analysis. This Article will attempt to follow some accepted generalities about the approaches of various jurisdictions and present conclusions based on those broad conceptions.

[8] The European emphasis on protecting the private life has its roots in the laws of France and Germany.[47] These regimes initially sanctified personal dignity and honor to protect the elite.[48] Today, the European Charter embodies this guarantee,[49] defended by the ECHR. The European Charter states that "[h]uman dignity is inviolable. It must be respected

---

[43] *See* Levin & Abril, *supra* note 5, at 1007-08 (noting that privacy has been conceptualized as the right to be "let alone," the right to exercise "control over personal matters or information," or the value of "personhood, intimacy, social relationships, and secrecy").

[44] *Id*. at 1008.

[45] Whitman, *supra* note 7, at 1153.

[46] *See* Levin & Abril, *supra* note 5, at 1007-08 (discussing an absence of unanimity in privacy regimes, one conception preferred over another based on a particular society's "distinct historical and sociological influences, norms, and values").

[47] *See id*. at 1014; *see also* Warren & Brandeis, *supra* note 3, at 214 ("The right to privacy . . . has already found expression in the law of France.").

[48] *See* Levin & Abril, *supra* note 5, at 1013-14.

[49] *See* European Charter, *supra* note 35, at art. 1.

and protected."[50] It also provides individuals with the "right to respect for his or her private and family life, home and communications."[51] Similarly, the ECHR establishes that "[e]veryone has the right to respect for his private and family life, his home and his correspondence," the exercise of which no public authority shall interfere with except when such "is in accordance with the law and is necessary" to protect democratic interests of public well-being.[52] This conception protects an individual from situations where unwarranted publicity would violate personal dignity.[53] As described in a recent English decision, the law protects an individual's reasonable expectation of privacy, "even in circumstances where there is no pre-existing relationship giving rise of itself to an enforceable duty of confidence. . . . because the law is concerned to prevent the violation of a citizen's autonomy, dignity, and self-esteem."[54] As such, European jurisdictions typically grant high levels of personal privacy protection in various areas "from consumer rights… to discovery in civil litigation."[55]

[9] This theory of privacy protects the "inviolate personality" conceived by Warren and Brandeis[56] and, like those authors, views the "prime enemy of our privacy . . . [as] the media, which always threatens to broadcast unsavory information about us in ways that endanger our public dignity."[57] Although perhaps more dominant in some jurisdictions, many

[50] *Id.*

[51] *Id.* at art. 7.

[52] ECHR, *supra* note 39.

[53] *See* Levin & Abril, *supra* note 5, at 1013 (describing respect for individual dignity as the value shared by all privacy interests).

[54] Mosley v. News Grp. Newspapers, Ltd., [2008] EWHC (QB) 1777, [7] (Eng.); *see also* Whitman, *supra* note 7, at 1161.

[55] Levin & Abril, *supra* note 5, at 1015 (footnote omitted); s*ee also* Whitman, *supra* note 7, at 1156.

[56] Warren & Brandeis, *supra* note 2, at 205; *see also* Levin & Abril, *supra* note 5, at 1012.

[57] Whitman, *supra* note 7, at 1161.

western states also place great importance on the autonomous ability to control personal information.[58] The right to control personal information plays a role in European law, notably manifesting itself in the right of an individual to control his or her public image.[59]

[10] American privacy law, on the other hand, is based primarily on the political value of liberty from government intrusion[60] and sovereignty within the home, rather than public image or social dignity.[61] However, American law also upholds the right to control access to and the dissemination of personal information.[62] This focus on individual liberty to control personal information allows the individual to determine which information to keep private and which information to release into the public domain.[63] Ideas of assumption of risk and privacy waiver have found strong footholds in this control-based jurisprudence.[64] Along with such autonomy, this conception also "places the burden of 'remaining private' squarely on the individual, who is ultimately without recourse from existing law or technology . . . ."[65] Despite the importance of Warren and Brandeis' *The Right to Privacy* in American privacy law, the United States has not yet heeded their call to protect the "inviolate personality."[66]

---

[58] *See* Levin & Abril, *supra* note 5, at 1009.

[59] *See, e.g.*, Whitman, *supra* note 7, at 1161 ("[The German] right to informational self-determination [is defined as] the right to control the sorts of information disclosed about oneself.").

[60] *See* Levin & Nicholson, *supra* note 29; Whitman, *supra* note 7, at 1161.

[61] *See* Whitman, *supra* note 7, at 1161-62.

[62] *See* Levin & Abril, *supra* note 5, at 1008.

[63] *See id*. at 1008-09.

[64] *See generally* Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 78-80 (2007).

[65] *Id.* at 78.

[66] Warren & Brandeis, *supra* note 2, at 205; *see* Levin & Nicholson, *supra* note 29, at 383.

[11] Again, note that the distinction between liberty and dignity is not as much black and white as it is shades of grey.[67] Much crossover exists.[68] Additionally, notions about predicating the reasonableness of an expectation of privacy on the amount of control exercised over personal information in question is not without some mutual recognition.[69] In the context of OSN privacy, however, commentators have described the idea that individual control of information is a sufficient test of the reasonableness of the individual's subjective expectation of privacy as "simplistic," "ill-fitting and impossible."[70] These commentators reason that the test is based on "the mistaken assumption that such control is possible on- or off-line."[71] To properly support a more ideal contemporary conception of what constitutes a reasonable expectation of privacy online, a healthy respect for control and liberty must be balanced with more substantive recognition of the reputational benefits of protecting human dignity.

[67] Whitman, *supra* note 7, at 1162-63 ("[T]his contrast is not absolute. These are complex societies, which are home to a variety of sensibilities, concerns, traditions, and mutual influences. There are certainly some Americans who find the European idea of dignity appealing. This is notably true of Justice Kennedy, whose opinion for the Court in Lawrence v. Texas [123 S. Ct. 2472, 2483 (2003)] expresses admiration for European approaches, and who tries energetically to found his opinion on ideals of both liberty and dignity. For that matter, there are no doubt Europeans who find the characteristic American approach appealing. Moreover, it is certainly the case that both forms of the protection of privacy are in force to some extent on both sides of the Atlantic: There are some protections against the media and the like in the United States, and there are certainly some American tort cases protecting people's public image. As for Europe: There are certainly some quite far-reaching protections against the state there, and there is certainly law protecting people within the bounds of the home." (footnotes omitted)).

[68] *See id.*

[69] *See* Levin & Abril, *supra* note 5, at 1009; Abril, *supra* note 64, at 76 (claiming that those who view their online existence as their own personal space, the "digital natives," are more likely to feel violated by Internet privacy breaches than their less "cyber-savvy" counterparts, the "digital immigrants").

[70] Abril, *supra* note 64, at 78.

[71] *Id*.

III. CHANGING EXPECTATIONS IN THE WORLD OF ONLINE SOCIAL NETWORKS

[12] Commentators have noticed the dichotomy between traditional privacy law – at least in those jurisdictions that base privacy on the ideals of liberty and the right to control information – and recent trends emerging in online communities.[72] Commentators call the dichotomy a "privacy contradiction" because "users of social networking websites tend to disclose much personal information online, yet they seem to retain an expectation of privacy."[73] Under traditional views of privacy and the Internet – held by those whom Professor Palfrey calls "digital immigrants"[74] – there is no reasonable expectation of privacy in anything posted anywhere on the Internet.[75] Indeed, recent judicial decisions have echoed these views,[76] and have also made quite a stir in online chatter.[77] Some call the distinction between "digital immigrants" and "digital natives"[78] "the greatest generation gap since the early days of rock and roll."[79]

---

[72] *See, e.g.*, Levin & Abril, *supra* note 5, at 1002; John G. Palfrey, Jr., Commentary, *Should Fred Hire Mimi Despite Her Online History?*, HARV. BUS. REV., June 2007, at 42 (describing the recent trend of revealing "compromising photos [and] embarrassing conversations" online, despite the fact many people would likely deem such information highly private).

[73] Levin & Abril, *supra* note 5, at 1004.

[74] Palfrey, *supra* note 72, at 42.

[75] *See* Abril, *supra* note 64, at 77 ("To the digital immigrant, [online social network] privacy is an absurd oxymoron.").

[76] *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862-63 (Cal. Ct. App. 2009); Leduc v. Roman, 2009 CarswellOnt 843, paras. 18-19, 32, 36 (Can. Ont. Sup. Ct. J.) (WL); Murphy v. Perger, 2007 CarswellOnt 9439, paras. 1, 4, 17, 19, 20 (Can. Ont. Sup. Ct. J.) (WL).

[77] *See, e.g.*, *Digital Immigrant*, URBANDICTIONARY, http://www.urbandictionary.com/define.php?term=digital+immigrant (last visited Apr. 9, 2011) (discussing how by the time this was written, the phrase "digital immigrant" has received more than 3,500 votes and comments on the popular website).

[78] Palfrey, *supra* note 72.

[79] Abril, *supra* note 64, at 73.

[13] Commentators have noted, "online social networking poses a fundamental challenge to the theory of privacy as control."[80] The stakes have been raised because digital technologies lack "the relative transience of human memory,"[81] and can be trolled or data mined for information in ways previously unthinkable.[82] Digital dossiers contain growing amounts of information from all over the Internet that can result in real world harm.[83] Admittedly, many new technologies may provide a greater ability to control how, where, and when we publish our private information, if we do so at all.[84] However, the nature of the growing participatory Internet poses a greater risk that online socializers will post "unflattering, defamatory, or personal information about each other, and that this information would in turn be available to a large, if not unrestricted, online audience."[85] The Internet and OSNs allow third parties the luxury of broadcasting other people's personal information to large audiences much more easily than through older, more established, modes of communication that existed throughout much of privacy law's development.[86] Some have expressed the view that this change will have profound effects on the concept of reputation in the years to come.[87]

[80] Levin & Abril, *supra* note 5, at 1002.

[81] Abril, *supra* note 64, at 75.

[82] *See* Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 57 (1999).

[83] *See id.* ("A person's digital dossier can betray him in the physical world, resulting in harms like the denial or loss of employment, shame and embarrassment, denigration of reputation, or merely exposure in an unwanted light." (footnote omitted)); *see also* SOLOVE, *supra* note 1, at 2-3.

[84] *Cf.* SOLOVE, *supra* note 1, at 223 (describing how digital dossiers will affect individual freedom and power).

[85] Levin & Abril, *supra* note 5, at 1002.

[86] *See id*. at 1006-07.

[87] *See id*. *See generally* DANIEL SOLOVE, THE FUTURE OF REPUTATION 2-4 (2007).

[14] The other side of the coin concerns the release of one's own personal information onto the Internet. This information is often not released to the public at large but, in many instances, to large numbers of "friends" on a user's MySpace or Facebook profile.[88] Some courts have begun to take the view that this release of information to a large number of friends is essentially the same as releasing it to the public at large, despite the user's subjective expectation to the contrary.[89] Strictly tying the reasonableness of an individual's expectation of privacy to ideas of control and waiver, relevant in the traditional offline context, neglects to consider whether the subjective expectations of the Internet community, a substantial and growing percentage of our society, ought to be afforded greater weight – perhaps even considered reasonable in certain circumstances.[90] Granted, completely disregarding the connection between control, waiver through releasing information, and the reasonableness of an expectation of privacy in that information would prove foolhardy.[91] However, courts may more satisfactorily address this paradox by reading an element of human dignity – such as that found in the jurisprudence of the European Court of Human Rights – into the theoretical basis for protecting privacy in information posted to OSNs.[92]

[15] Professors Levin and Abril recently published the results of an empirical study in which they examined the OSN activity and privacy expectations of 2,500 students in the United States and Canada.[93] After reviewing the results of the study, the professors outlined a "theory of

[88] *See Statistics*, *supra* note 16 ("[the] [a]verage user has 130 friends.").

[89] *See, e.g.*, Leduc v. Roman, 2009 CarswellOnt 843, para. 32 (Can. Ont. Sup. Ct. J.) (WL) (equating a private or limited access Facebook profile with a public profile); Murphy v. Perger, 2007 CarswellOnt 9439, para. 20 (Can. Ont. Sup. Ct. J.) (WL)) (discussing how 366 friends negated any expectation of privacy).

[90] *See* Levin & Abril, *supra* note 5, at 1046.

[91] *See id*. at 1046-47.

[92] *See id*. at 1014-15, 1047.

[93] *See id*. at 1004-05.

network privacy"[94] which supported their conclusion that these "online socializers have developed a new and arguably legitimate notion of privacy online . . . ."[95] Their conclusion draws a clear parallel with the aims of this Article; specifically, that this notion of network privacy, if respected, would "offer online socializers both control and protection of their dignity and reputation."[96] Their work recognizes the link between the degree of control over personal information and the amount of privacy protection afforded such information.[97] Indeed, many of the leading OSNs have themselves propagated this "notion of privacy as user control."[98] An older version of Facebook's privacy policy (as of Nov. 10, 2009) stated as its two core principles: "(1) You should have control over your personal information, and (2) You should have access to the information others want to share."[99] This ability of others to share information is precisely the thorn in the side of the control theory.[100]

[16] According to the results of Levin's and Abril's study, a majority of OSN users reported that their profiles included "their real full name, home town, high school, relationship status, interests, hobbies, favorite music, books, movies, and a picture of themselves."[101] More than three fourths

[94] *Id.* at 1045.

[95] Levin & Abril, *supra* note 5, at 1002.

[96] *Id.*

[97] *See id*. at 1005.

[98] *Id*. at 1005-06.

[99] *Id*. (quoting *Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last visited Apr. 9, 2009) (internal quotations marks omitted) (quoted material since removed from site); *see also Privacy Policy*, FACEBOOK, http://www.facebook.com/policy.php (last modified Dec. 22, 2010) (describing the control settings for personal information); *Privacy Policy*, MYSPACE, http://www.myspace.com/index.cfm?fuseaction=misc.privacy (last modified Feb. 28, 2008) (suggesting that user control over personal information is part of its core).

[100] *See* Levin & Abril, *supra* note 5, at 1006-07.

[101] *Id*. at 1024.

reported posting real photographs of themselves, and only a small minority reported posting fake names or photos.[102] Nearly half the respondents reported serious concerns about strangers accessing their profiles.[103] The respondents demonstrated selectivity in the type of material they posted and, reportedly, were "able to distinguish between personal information that allows them to socialize safely with other users . . . and information that could be potentially dangerous . . . ."[104]

[17] According to the study, seventy-two percent of respondents manually restricted their privacy settings and more than half blocked specific people from viewing their profiles.[105] More than sixty percent believed they take effective measures to protect their privacy, but many felt helpless protecting their character or controlling what information others post about them.[106] Levin and Abril concluded that these results "illustrate[] the difficulty of combining control-oriented privacy protection tools and policies with dignity-based concerns in a coherent manner. The domination of control-oriented tools leads to the dismissal of dignity concerns, while the emergence of such concerns reinforces uncertainty about the efficacy of such tools."[107] The study also found that similar percentages of respondents harbored concerns about controlling their information (thirty-seven percent), and many held concerns specifically directed toward the dignitary ends of protecting reputation and relationships (thirty-two percent).[108] Most respondents felt strongly in favor of the ability to segregate the professional and personal segments of their lives through OSN privacy settings, such as by not allowing profile

[102] *See Id*.

[103] *Id*. at 1026.

[104] *Id*. at 1025.

[105] Levin & Abril, *supra* note 5, at 1033.

[106] *Id*. at 1036.

[107] *Id*.

[108] *Id*. at 1038-39.

access to employers[109] or parents.[110] In sum, many online socializers do maintain subjective expectations of privacy – "grounded in the need to maintain discreet social identities, or situational personalities"[111] – in information uploaded to OSN profiles despite their "penchant for disclosure."[112] Levin and Abril's notion of "network privacy," is therefore "a notion of privacy based on the expected accessibility of personal information to social constituencies."[113] These online socializers are more concerned with who views their information and how it is disseminated, rather than whether this information is disseminated in the first place.[114]

[18] Granted, determining whether an individual maintains a subjective expectation of privacy in his or her OSN profile information cannot always be "scientifically gauged."[115] In fact, "the inherent nature" of the activity of utilizing an OSN itself often "works against any notion of an expectation of privacy."[116] By signing up, logging in, and posting information, the user has shown clear intention "to publicize [the] information to others."[117] These actions show clearer intention to disseminate personal information than in the case of an e-mail or telephone call because of the typical number of recipients.[118] Therefore, OSN profile information appears similar to a "yearbook, directory, or bulletin board," where "users are communicating information for more

[109] *See id*. at 1026, 1043.

[110] *See* Levin & Abril, *supra* note 5, at 1025-26.

[111] *Id*. at 1045.

[112] *Id*.

[113] *Id*.

[114] *See id*. at 1045-46.

[115] Smith v. Maryland, 442 U.S. 735, 743 (1979).

[116] Hodge, *supra* note 19, at 106.

[117] *Id.*

[118] *See* Statistics, *supra* note 16.

than one person by posting that information on a naturally public platform."[119] However, the fact that a person has acted to prevent public access to such information – by selecting privacy settings that limit access to those recognized as "friends"[120] – suggests that such analogies go too far. A "mass e-mail," available only to the intended recipients who must login to their respective inboxes to access the information, may provide a more proper analogy.[121] Obvious in the context of recent decisions, the individual still must fight an uphill battle to show that he or she retained some subjective expectation of privacy in information made available to hundreds – or perhaps thousands – of people.[122] However, the existence of this subjective expectation of privacy actually exists in large numbers of OSN users.[123] It resides at a generational divide of serious depth and consequence.[124]

[19] Those who have grown up with the Internet, particularly the recent interactive rise of web 2.0,[125] view online privacy in a very different way than those of previous generations who have – or have not – immigrated to it.[126] Younger "natives" *expect* technological barriers – whether real or

[119] Hodge, *supra* note 19, at 107.

[120] *See id.* at 110; *see also Privacy Policy*, Facebook, http://www.facebook.com/policy.php (last revised Dec. 22, 2010).

[121] *See* U.S. v. Maxwell, 45 M.J. 406, 412 (C.A.A.F. 1996) ("Messages sent to the public at large in the 'chat room' or e-mail that is 'forwarded' from correspondent to correspondent lose any semblance of privacy."); Hodge, *supra* note 19, at 110 n.110 ("Courts have, however, hinted that an e-mail forwarded to more than one person would not be private. A mass e-mail is not, though, forwarded from correspondent to correspondent, but instead is delivered once to many correspondents." (citation omitted)).

[122] *See* Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 656 (N.Y. App. Div. 2010) (holding that plaintiff did not have a reasonable expectation of privacy in information published on social network web sites).

[123] *See* Levin & Abril, *supra* note 5, at 1045-46.

[124] *See id.* at 1017-18.

[125] *See* Matthew J. Wilson, *E-Elections: Time for Japan to Embrace Online Campaigning*, 2011 STAN. TECH. L. REV. 4, at *1.

[126] *See* Abril, *supra* note 64, at 76.

merely imagined – to protect their information from unintended audiences,[127] while others view their actions as reckless and foolish.[128] One commentator has described this predicament as follows:

> To the digital immigrant, OSN privacy is an absurd oxymoron. After all, *it's the Internet!* When faced with the privacy-related risks of the medium, digital immigrants fervently argue, "if you can't stand the heat, get off of MySpace." This argument is consistent with their history of control over their personal information and the control-centered definitions of privacy of their generation's noted legal scholars.[129]

However, to simply place all things Internet into a basket reserved for only completely public information would seriously undermine the actual subjective – and arguably reasonable – expectations of a large and growing segment of society, ignore the technological protection measures actually available, and lead to an increasing number of unsalvageable real world harms stemming from the technology's use.[130] In short, that approach would refuse to adapt legal protection to a changing world.[131] In this new world, OSNs remain increasingly at the center of the online development of personal identity; they replace and supplement their physical real-world counterparts from days past, such as malls or drive-ins.[132] Affording privacy to the development of personality, identity, and the flowering of relationships would protect "[the] crucial

[127] *See id.*; Levin & Abril, *supra* note 5, at 1033-34.

[128] *See* Abril, *supra* note 64, at 76; Levin & Abril, *supra* note 5, at 1004.

[129] Abril, *supra* note 64, at 77 (citing Fried, *supra* note 34, at 482; ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967)).

[130] *See generally id*. at 86-87.

[131] *See id*. at 78 ("[P]rivacy law, technology, and ethics have not caught up to the harms they purportedly protect and redress.").

[132] *See id*. at 83.

developmental purpose"[133] of OSNs and relates to some of the explicitly defined purposes of ECHR-type private life protections based on a respect for human dignity.[134]

IV. REASONABLE EXPECTATIONS OF PRIVACY UNDER US TORT LAWS

[20] Tort law in many U.S. states recognizes various rights to privacy.[135] These state laws often utilize tests to determine the reasonableness of an individual's expectation of privacy.[136] Many states provide remedies for invasions of privacy that resemble the four main privacy torts Prosser identified in 1960.[137] Prosser concluded that these torts consisted of: "(1) intrusion upon the plaintiff's seclusion . . . (2) public disclosure of embarrassing private facts . . . (3) publicity which places the plaintiff in a false light . . . and (4) appropriation, for the defendant's advantage, of the plaintiff's name or likeness."[138] These torts came to life in response to the very thing of which Warren and Brandeis had warned: privacy violations of the traditional print media.[139] The four torts Prosser defined, however, do not necessarily adapt well to privacy crises in cyberspace.[140]

---

[133] *See id*. (citing Danah Boyd, Address at the American Association for the Advancement of Science: Identity Production in a Networked Culture: Why Youth Heart MySpace (Feb. 19, 2006), *available at* http://www.danah.org/papers/AAAS2006.html).

[134] *See* discussion *infra* Part VII (pertaining to ECHR Article 8's private life jurisprudence).

[135] *See* SOLOVE, *supra* note 1, at 58.

[136] *See id*. at 59-60 (showing that a commonly used test of an individual's expectation of privacy is whether the intrusion is "highly offensive to a reasonable person").

[137] *See* Prosser, *supra* note 2; SOLOVE, *supra* note 1, at 58.

[138] Prosser, *supra* note 2.

[139] SOLOVE, *supra* note 1, at 58.

[140] *Id*. at 58-59; Abril, *supra* note 64, at 78-81.

[21] The tort of intrusion upon seclusion protects "'private affairs or concerns'" from intrusion that "'would be highly offensive to a reasonable person.'"[141] It does not protect private matters kept in anything but non-public places, and, as the Internet is seen primarily as a public medium, this tort does not currently provide adequate protection for information on the Internet.[142] Prosser's second tort, publication of private facts, typically provides a remedy to an individual when a private matter – not of legitimate public concern – is broadcast to a wide audience in a way that is "highly offensive to a reasonable person."[143] The tort does not provide effective remedies for violations of privacy not subject to wide dissemination or not highly offensive.[144] Additionally, the last two torts, false light and appropriation, are closely linked with defamation and intellectual property laws, respectively,[145] and have limited applicability to invasions of privacy in the context of the information technology issues this Article confronts. A state-by-state analysis of privacy related tort law is well outside the scope of this Article. However, one recent California case is relevant to the current discussion and, quite fittingly, portrays a foreboding portrait of the privacy problems inherent at the intersection of the print media and the new medium of the Internet.[146]

[22] In *Moreno v. Hanford Sentinel*, the plaintiff, a U.C. Berkeley student, wrote a scathing ode to her central California hometown of Coalinga and published it to her MySpace page.[147] The post began by stating, "the older I get, the more I realize how much I despise Coalinga"

---

[141] SOLOVE, *supra* note 1, at 59 (quoting RESTATEMENT (SECOND) OF TORTS § 652B (1976).

[142] *See id*.

[143] *Id*.

[144] *See id* at 59-60.

[145] *See id*. at 60.

[146] *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 860 (Cal. Ct. App. 2009).

[147] *See id*. at 861.

and went on to comment negatively about the town and its inhabitants.[148] The post was only available on Moreno's MySpace page for six days before she took it down.[149] However, within that time, the local high school principal located it and forwarded it to the editor of the town newspaper who – without notifying or seeking permission from Moreno – subsequently published it in the paper's "Letters to the Editor" section, attributing it as a submission from Moreno.[150] As a result, Moreno's family in Coalinga received death threats and a gunshot was fired at the family's home.[151] Because of the community's violent reaction, the family moved away from Coalinga and closed their twenty-year-old family business.[152] Moreno and her family sued the paper for invasion of privacy and intentional infliction of emotional distress, but the court dismissed the privacy claim on demurrer, prior to any trial on the merits.[153]

[23] California privacy law – part of the state's constitutional law – largely mirrors Prosser's four privacy torts.[154] It allows remedies for four distinct types of harm: "(1) intrusion into private matters; (2) public disclosure of private facts; (3) publicity placing a person in a false light; and (4) misappropriation of a person's name or likeness."[155] To succeed on an invasion of privacy claim, the party must demonstrate: "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy under the circumstances; and (3) a serious invasion of the privacy interest."[156] In

[148] *Id*. (internal quotation marks omitted).

[149] *Id*.

[150] *Id.*

[151] *Id.*

[152] *Moreno*, 91 Cal. Rptr. 3d at 861.

[153] *Id.* at 860-61.

[154] Hill v. Nat'l Collegiate Atheltic Ass'n, 865 P.2d 633, 647 (Cal. 1994).

[155] *Moreno*, 91 Cal. Rptr. 3d at 862.

[156] *Id.* (citations omitted).

Moreno, the court held that postings on publically accessible MySpace pages were not private, and as such, the plaintiff could not hold a reasonable expectation of privacy in information published to her profile.[157] "Under these circumstances," the court stated, "no reasonable person would have had an expectation of privacy regarding the published material."[158] The court made clear that it did not require total secrecy, but that by publishing the ode on a fully public page, Moreno had failed to "*define* [her] circle of intimacy,"[159] despite expecting that only a limited audience would view her page.[160] In concluding Moreno maintained no objective expectation of privacy in her MySpace post, the court stated, "[b]y posting the article on myspace.com, [Moreno] opened the article to the public at large. Her *potential audience* was vast."[161] A number of courts have begun to come to similar conclusions.[162]

[157] *Id.*

[158] *Id.*

[159] *Id.* (quoting M.G. v. Time Warner, Inc., 107 Cal. Rptr. 2d 504, 511 (Cal. Ct. App 2001)).

[160] *Id.* at 863.

[161] *Moreno*, 91 Cal. Rptr. 3d at 863 (emphasis added).

[162] *See, e.g.*, Beye v. Horizon Blue Cross Blue Shield of New Jersey, No. 06-5337 (FSH), 2007 WL 7393489, at *2 (D.N.J. Dec. 14, 2007) (discussing online journals and diary entries of minors, the court stated, "[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information"); Romano v. Steelcase, Inc., 907 N.Y.S.2d 650, 657 (N.Y. Sup. Ct. 2010) ("[W]hen Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist."); Dexter v Dexter, No. 2006-P-0051, 2007 WL 1532084, at *6 n.4 (Ohio Ct. App. May 25, 2007) (stating that there is no reasonable expectation of privacy regarding Myspace writings open to public view).

V. REASONABLE EXPECTATIONS OF PRIVACY IN DIGITAL COMMUNICATIONS UNDER THE US FOURTH AMENDMENT

[24] The United States Constitution, while not explicitly mentioning a right to privacy, does protect some elements of privacy.[163] The Fourth Amendment to the United States Constitution prohibits some forms of governmental intrusion into an individual's private life – specifically, "unreasonable searches and seizures" – unless a valid warrant adequately authorizes such an intrusion.[164] It only protects against searches where a reasonable expectation of privacy exists.[165] It states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[166]

The Fifth Amendment, by comparison, prohibits the government from forcing an individual to incriminate himself.[167] At one point, these constitutional amendments together barred government from "any forcible and compulsory extortion of a man's own testimony or of his private papers to be used as evidence to convict him of crime or to forfeit his

[163] A right to privacy, for example, has been found within the penumbra of rights granted by the Bill of Rights, and has been articulated in cases involving contraception, abortion, and information – including an individual interest in avoiding disclosure of private matters. *See* SOLOVE, *supra* note 1, at 64-65; *see also* Whalen v. Roe, 429 U.S. 589, 605 (1977) (finding a right of privacy in personal information collected by government agencies); Roe v. Wade, 410 U.S. 113, 154 (1973) (concluding that the right of personal privacy includes abortion decisions); Griswold v. Connecticut, 381 U.S. 479, 485-86 (1965) (finding that use of contraceptives lies within the zone of privacy created by fundamental constitutional gurantees).

[164] *See* U.S. CONST. amend. IV.

[165] SOLOVE, *supra* note 1, at 188-89.

[166] U.S. CONST. amend. IV.

[167] U.S. CONST. amend. V.

goods," because such compulsion is an "invasion of his indefeasible right of personal security, personal liberty and private property."[168] However, the court subsequently backed away from that position in later opinions.[169] Some scholars have argued that the Fourth Amendment focus on privacy is misguided and "has not fared well with the changing times."[170] Others argue that such a focus remains vitally important. In fact, "the Court's failure to conceptualize privacy adequately" has given rise to many of the problems confronting Fourth Amendment jurisprudence in the information age.[171]

[25] In *Olmstead v. United States*, Justice Brandeis wrote a passionate dissent, arguing, much in line with arguments made in his seminal article of 1890,[172] that, by not finding police wire tapping an unreasonable search, the Court's Fourth Amendment jurisprudence failed to properly reflect changing societal conditions.[173] Brandeis wrote, "[c]lauses guaranteeing to the individual protection against specific abuses of power, must have a similar capacity of adaptation to a changing world."[174] Thirty-nine years later, in *Katz v. United States*, the Supreme Court adopted Justice Brandeis's view[175] and, through an influential concurrence by Justice

[168] Boyd v. United States, 116 U.S. 616, 630 (1886); SOLOVE, *supra* note 1, at 63.

[169] *See* SOLOVE, *supra* note 1, at 63-64; *see, e.g.*, Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 309-10 (1967) (overturning the mere evidence rule); Shapiro v. United States, 335 U.S. 1, 16-17 (1948) (explaining the Fifth Amendment does not bar production of an individual's records as incriminating evidence).

[170] SOLOVE, *supra* note 1, at 190 (quoting Scott E. Sundby, *'Everyman's' Fourth Amendment: Privacy or Mutual Trust between Government and Citizen?*, 94 COLUM. L. REV. 1751, 1771 (1994)).

[171] *Id.* at 190-91.

[172] *See generally* Warren & Brandeis, *supra* note 2, at 198.

[173] *See* Olmstead v. United States, 277 U.S. 438, 466, 472-73 (1928) (Brandeis, J., dissenting); Hodge, *supra* note 19, at 100.

[174] *Olmstead*, 277 U.S. at 472 (Brandeis, J., dissenting).

[175] *See* Katz v. United States, 389 U.S. 347, 352-53 (1967).

Harlan, articulated a new two-step approach to determine the reasonableness of government action under the Fourth Amendment.[176] First, a person must "have exhibited an actual (subjective) expectation of privacy."[177] Second, that subjective expectation must "be one that *society* is prepared to recognize as 'reasonable.'"[178] In *Katz*, as well as in *Berger v. New York*, decided earlier that same year, the Supreme Court held that government eavesdropping on an individual's telephone conversation constituted a violation of the Fourth Amendment and, therefore, violated the individual's reasonable expectation of privacy.[179] The caller, stated the *Katz* court, "is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world,"[180] and therefore retains a privacy right in the conversation.[181]

[26] Essentially, to implicate a Fourth Amendment violation, a subjective expectation of privacy must be objectively reasonable.[182] Exceptions do exist, of course, and include police searches in "hot pursuit,"[183] protective sweeps of cars,[184] limited stops and frisks based on reasonable suspicion,[185] searches incident to a lawful arrest[186] and, in

[176] *Id.* at 361 (Harlan, J. concurring); Hodge, *supra* note 19, at 100.

[177] *Katz*, 389 U.S. at 361 (Harlan, J. concurring).

[178] *Id*. (emphasis added).

[179] *See* Berger v. United States, 388 U.S. 41, 62 (1967); *Katz*, 389 U.S. at 359; *see also* Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008).

[180] *Katz*, 389 U.S. at 352.

[181] *Warshak*, 490 F.3d at 470 (citing *Katz*, 389 U.S. at 352).

[182] *See* Hodge, *supra* note 19, at 101.

[183] *See Warden*, 387 U.S. at 310.

[184] *See* United States v. Ross, 456 U.S. 798, 809 (1982).

[185] *See* SOLOVE, *supra* note 1, at 189 (citing Terry v. Ohio, 392 U.S. 1, 1 (1968)).

[186] *See* United States v. Robinson, 414 U.S. 218, 234 (1973).

certain circumstances, searches of electronic communications stored for more than 180 days[187] – although the constitutionality of this statutory provision has been questioned.[188] This subjective determination is "an empirical question which fact finders decide using the evidence from each individual case."[189] The test laid out in *Katz* operates in the context of protecting an individual's expectation of privacy in his telephone communications.[190] Logically, some lower courts have extended it to encompass communication in a digital context,[191] although some lower court judges have not been keen to apply analogies developed in the physical world to an electronic one.[192] However, in 2010, the Supreme Court finally weighed in on the issue, in *City of Ontario v. Quon*.[193]

[27] In *Quon*, the Supreme Court held that a public employer's detailed search of a police officer's pager text messages was ultimately reasonable because it was "motivated by a legitimate work-related purpose," "was not

[187] Stored Communications Act, 18 U.S.C. § 2703(a).

[188] *See generally* Warshak v. United States, 490 F.3d 455, 474-75 (6th Cir. 2007) *vacated*, 532 F.3d 521 (6th Cir. 2008).

[189] Hodge, *supra* note 19, at 101; *see* Note, *Keeping Secrets in Cyberspace: Establishing Fourth Amendment Protection for Internet Communication*, 110 HARV. L. REV. 1591, 1596 n.55 (1997).

[190] *See* Katz v. United States, 389 U.S. 347, 361 (1967).

[191] *See, e.g.*, United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("So long as the risk-analysis approach of *Katz* remains valid, however, this court is compelled to apply traditional legal principles to this new and continually evolving technology."), *aff'd* 225 F.3d 656 (4th Cir. 2000).

[192] *See, e.g.*, United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("The advent of the electronic age and . . . the development of desktop computers . . . go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law." (footnote omitted)); *Hambrick*, 55 F. Supp. 2d at 508 ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional *Fourth Amendment* analysis."); *see also* Hodge, *supra* note 19, at 102.

[193] *See generally* City of Ontario v. Quon, 130 S. Ct. 2619, 2624 (2010).

excessive in scope," and would likely be "'regarded as reasonable and normal in the private-employer context.'"[194] The Ontario Police Department searched transcripts of Quon's pager messages – after Quon surpassed his monthly character allotment – to determine whether the excess resulted from work related messaging (implying the department's character limit was too low) or private communication.[195] When Quon's employer discovered the sexually explicit, non-work related nature of the text messages, his supervisor referred the matter to the department's internal affairs division, which ultimately disciplined Quon for his conduct.[196] Quon sued on Fourth Amendment grounds, claiming the search was unreasonable, but the United States Supreme Court disagreed.[197] Before making its pronouncement, however, the court stated, "[t]he judiciary risks error by elaborating too fully on the *Fourth Amendment* implications of emerging technology before its role in society has become clear."[198] Assuming Quon indeed "had a reasonable expectation of privacy in [his] text messages," the court analogized the search to one involving "a government employer's search of an employee's physical office" space, and found the invasion justified.[199]

[28] In the landmark case of *Smith v. Maryland*, the United States Supreme Court held an individual's reasonable expectation of privacy cannot extend to non-substantive information – such as the numbers dialed – gathered by devices such as pen registers because, unlike the eavesdropping in *Katz* and *Berger*, "pen registers do not acquire the *contents* of communications."[200] The court's holding rested on the

[194] *Id*. at 2632-33.

[195] *See id*. at 2625-26.

[196] *Id*. at 2626.

[197] *See id*. at 2626, 2632.

[198] *Quon*, 130 S. Ct. at 2629.

[199] *Id.* at 2630.

[200] Smith v. Maryland, 442 U.S. 735, 741 (1979); *see* Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008); Hodge, *supra* note 19, at 103.

premise that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company" because their monthly bills reflect these numbers.[201] Although discarding the possibility of any objective reasonableness of the plaintiff's claim, the Court also held that "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as reasonable.'"[202]

[29] The *Smith* decision allowed the government to acquire non-content information derived from the register, namely the numbers the customer dials,[203] but continued to protect the contents of the individual's communication. Justice Stewart, in a dissenting opinion, argued that an expectation of privacy in the communication's contents remains reasonable even though "[t]he telephone conversation itself must be electronically transmitted by telephone company equipment, and may be recorded or overheard by the use of other company equipment."[204] However, *United States v. Miller* put this proposition to the test when Justice Powell – invoking the concept that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties"[205] – wrote that when a party discloses information to another he "takes the risk . . . that the information will be conveyed by that person to the Government."[206] The court has applied this assumption of risk exception in a variety of contexts to defeat Fourth Amendment claims,[207]

[201] *Smith*, 442 U.S. at 742; Hodge, *supra* note 19, at 103.

[202] *Smith*, 442 U.S. at 743 (quoting *Katz*, 389 U.s. at 361) ; *accord* Hodge, *supra* note 19, at 103.

[203] *Accord Warshak*, 490 F.3d at 470; *see Smith*, 442 U.S. at 741-42.

[204] *Smith*, 442 U.S. at 746 (Stewart, J., dissenting).

[205] *Id.* at 743–44.

[206] United States v. Miller, 425 U.S. 435, 443 (1976).

[207] *See, e.g.*, United States v. Jacobsen, 466 U.S. 109, 117 (1984) ("[W]hen 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 governmental use of that information."); United States v. Maxwell, 45 M.J. 406,

and the Supreme Court in *United States v. Jacobsen* reiterated the exception eight years after the *Miller* decision.[208] Therefore, no reasonable expectation of privacy can exist in regard to the actions of other parties to the communication and, potentially, to information channelled through an intermediary.

[30] Obviously, *Smith*, *Miller*, and *Jacobsen* stand strongly for the proposition that society, at least in the late 1970s and mid 1980s, was not prepared to recognize a reasonable expectation of privacy in some types of personal information, especially in non-content information shared with third parties.[209] In contrast, however, Congress and many state courts have taken a different view.[210] Congress enacted legislation that partially superseded both *Smith* and *Miller*,[211] and many state courts have rejected those holdings in favor of broader privacy rights based on state constitutional provisions.[212]

---

419 (C.A.A.F. 1996) (holding that the sender of an e-mail runs the risk that its recipient will publish the contents); *see also* United States v. Payner, 447 U.S. 727, 731-32 (1980) (noting the assumption of risk exception through information contained in records entrusted to a bank officer); *Miller*, 425 U.S. 435, 442-43 (noting the assumption of risk exception through customer's bank records); United States v. White, 401 U.S. 745, 750 (1971) (noting the assumption of risk exception through confidences exchanged in private conversation); United States v. D'Andrea, 497 F. Supp. 2d 117, 120 (D. Mass. Ct. 2007) ("[T]here can be no reasonable expectation of privacy in matters voluntarily disclosed or entrusted to third parties, even those disclosed to a person with whom one has a confidential business relationship.").

[208] *See Jacobsen*, 466 U.S. at 117.

[209] *See* Hodge, *supra* note 19, at 103; *see also Smith*, 442 U.S. at 743; *Miller*, 425 U.S. at 442-43. *See generally Jacobsen*, 466 U.S. at 117 (holding that a party assumes the risk that information will be disclosed to the government when it is voluntarily provided to a third party).

[210] *See* Hodge, *supra* note 19, at 103-04.

[211] *See* 12 U.S.C. § 3405 (2006) ("A Government authority may obtain financial records . . . only if [the records] . . . are relevant to a legitimate law enforcement inquiry . . . [and if] a copy of the summons has been served on the customer . . . ."); *see also* 18 U.S.C. § 3121 (2006) (stating that most pen registers may only be used with a court order).

[212] Hodge, *supra* note 19, at 104 (citing Frances A. Gilligan & Edward J. Imwinkelried, *Cyberspace: The Newest Challenge for Traditional Legal Doctrine*, 24 RUTGERS

[31] An additional exception has also been applied in circumstances where a private party infringes upon the privacy of the individual prior to any government action.[213] In this situation, the police can piggyback onto the private party's breach without causing additional harm to an already frustrated expectation of privacy, thus avoiding a Fourth Amendment violation.[214] The police can also conduct a more thorough or intensive search without violating the individual's Fourth Amendment privacy interest "so long as they do not 'significantly expand' upon or 'change the nature' of the underlying private search."[215] Courts have applied this

COMPUTER & TECH. L.J. 305, 330–31 (1998) ("There is a parallel between Miller and Smith: Both cases have been rejected by state courts . . ."); *see, e.g.*, Charnes v. Digiacomo, 612 P.2d 1117, 1120-21 (Colo. 1980) (en banc); People v. Jackson, 452 N.E.2d 85, 87-88 (Ill. App. Ct. 1983); State v. Thompson, 810 P.2d 415, 417-18 (Utah 1991).

[213] *See Jacobsen*, 466 U.S. at 113.

[214] *See id.* at 117; United States v. D'Andrea, 497 F. Supp. 2d 117, 122 (Mass. Dist. Ct. 2007) ("Where the State is simply the passive recipient of evidence gathered by a private party acting without the State's instigation or direction, a defendant incriminated by that evidence has no recourse to the Fourth Amendment."); *see also* Coolidge v. New Hampshire, 403 U.S. 443, 489-90 (1971) (holding that the government did not violate defendant's Fourth Amendment right by seizing guns voluntarily given to them by defendant's wife); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003) (upholding evidence of a vigilante computer hacker who provided authorities with digital images of the defendant engaging in sexual activity with a child); United States v. Mekjian, 505 F.2d 1320, 1326-27 (5th Cir. 1975) (upholding government's use of photocopied materials the defendant's employee secretly made and mailed to the FBI); United States v. Feffer, 831 F.2d 734, 739-40 (7th Cir. 1987) (approving the government's use of incriminating documents supplied by a disgruntled employee that implicated her supervisor in a crime); United States v. Pryba, 502 F.2d 391, 400-01 (D.C. Cir. 1974) (upholding conviction based on pornography discovered by a curious freight agent who opened a package without the defendant's authorization); Ward v. State, 351 A.2d 452, 454-55 (Md. Ct. Spec. App. 1976) (allowing incriminating evidence provided by defendant's daughter who gave it to the police without his permission or knowledge).

[215] *D'Andrea*, 497 F. Supp. 2d at 123 (quoting United States v. Runyan, 275 F.3d 449, 452 (5th Cir. 2001)); *see Jacobsen*, 466 U.S. at 115 ("The additional invasions of [a defendant's] privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search."); *see also* Paul v. State, 57 P.3d 698, 702-03 (Alaska Ct. App. 2002) (holding that police did not intrude on any Fourth Amendment expectation of privacy by reviewing the entirety of an obscene videotape that had been partially viewed by a private citizen).

exception recently in circumstances where an anonymous caller had given authorities password and username information related to another individual's online photo storage and a government agent used the information to search the directory and locate incriminating photographs of criminal behavior.[216]

A. No Expectations of Privacy in Non-Content Data

[32] Federal and State courts have begun to apply this Supreme Court precedent in the context of digital communication and Internet activity.[217] Interestingly, although not unexpectedly, one District Court observed in 2007 that "[t]he *Smith* line of cases has led federal courts to uniformly conclude that internet users have no reasonable expectation of privacy in their subscriber information, the length of their stored files, and other non-content data to which service providers must have access."[218]

B. Expectations of Privacy in the Content of Digital Communication

[33] One district court recently ruled that it was "obvious that a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, without taking any

[216] *See D'Andrea*, 497 F. Supp. at 122.

[217] *See* Hodge, *supra* note 19, at 101.

[218] *D'Andrea*, 497 F. Supp. 2d at 120; *see* Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that a user loses any expectation of privacy in personal subscription information when it is conveyed to a system operator); United States v. Cox, 190 F. Supp. 2d 330, 332 (N.D.N.Y. 2002) ("[C]riminal defendants have no Fourth Amendment privacy interest in subscriber information given to an internet service provider."); *see also* United States v. Kennedy, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("Congress clearly intended for suppression not to be an option for a defendant whose electronic communications have been intercepted in violation of [the Electronic Communications Privacy Act]."), *aff'd*, 106 Fed. Appx. 688 (10th Cir. 2004); United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) *vacated on other grounds by*, 90 Fed. Appx. 3 (1st Cir. 2004)*;* BidZirk, LLC v. Smith, 2007 U.S. Dist. LEXIS 78481, at *14 (D.C.S.C. 2007) (holding plaintiffs cannot complain that an authorized photo on the Internet was linked to by a blogger in a negative blog post); United States v. Hambrick, 55 F. Supp. 2d 504, 509 (W.D. Va. 1999), *aff'd*, 225 F.3d 656 (4th Cir. 2000).

measures to protect the information."[219] Continuing, the court stated, "[a] person who places information on the information superhighway clearly subjects said information to being accessed by every conceivable interested party. Simply expressed, if privacy is sought, then public communication mediums such as the Internet are not adequate forums without protective measures."[220] The court, therefore, declared that society was not prepared to recognize a reasonable expectation of privacy in a photograph on the Internet.[221] The Court further stated,

> [A] person who places a photograph on the Internet precisely intends to forsake and renounce all privacy rights to such imagery, particularly under circumstances such as here, where the Defendant did not employ protective measures or devices that would have controlled access to the Web page or the photograph itself.[222]

This reasoning seems in line with Fourth Amendment law surrounding the plain view doctrine.[223] When obviously incriminating information is visible from a publicly accessible place, therefore, in plain view, police may seize the evidence without requiring a warrant.[224] Placing an item in plain view necessarily waives any reasonable expectation of privacy.[225] However, the court did not stop its reasoning there. Disturbingly, the court also said, "placing information on the information superhighway necessarily makes said matter accessible to the public, *no matter how*

[219] *Gines-Perez*, 214 F. Supp. 2d at 225.

[220] *Id.*

[221] *Id.*

[222] *Id.*

[223] *See, e.g.*, Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J. concurring).

[224] *See id.* (discussing how under the plain view doctrine, "objects, activities, or statements that [one] exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to [oneself] has been exhibited"); *see also* Hodge, *supra* note 19, at 109.

[225] *See Gines-Perez*, 214 F. Supp. 2d at 225.

many protectionist measures may be taken . . . ."[226] This Author, among others, believes that such a statement goes too far.

[34] Professor Warren LaFave, a preeminent authority on Fourth Amendment law, has argued that an individual should rightfully claim a reasonable expectation of privacy in the contents of a webpage if the individual safeguards those contents through password protection.[227] This argument points out a crucial difference between content and non-content data, suggesting that assumption of risk does not defeat this expectation in webpage privacy because,

> [W]hile a service provider has a need to access information regarding the identity of a site holder and the volume and extent of her usage, it has no legitimate reason to inspect the actual contents of the site, anymore than the postal service has a legitimate interest in reading the contents of first class mail, or a telephone company has a legitimate interest in listening to a customer's conversations.[228]

In this vein, Professor LaFave has argued that "'[r]eliance on protections such an[sic] individual computer accounts, password protection, and perhaps encryption of data should be no less reasonable than reliance upon locks, bolts, and burglar alarms, even though each form of protection is

[226] *Id*. (emphasis added).

[227] WAYNE R. LAFAVE, 1 SEARCH AND SEIZURE A TREATISE ON THE FOURTH AMENDMENT 721 (4th ed. 2004); *see* D'Andrea v. United States, 497 F. Supp. 2d 117, 121 (D. Mass. Ct. 2007).

[228] *D'Andrea*, 497 F. Supp. 2d at 121. *But see* Doe v. GTE Corp., 347 F.3d 655, 660 (7th Cir. 2003) (acknowledging the possibility that the "Good Samaritan" provision of the Communication Decency Act of 1996, 47 U.S.C. § 230 (c), might not have preemptive effect on a state law, thereby imposing a duty on ISP providers to filter offensive content on hosted websites); *see also Id.* at 122 (discussing how LaFave's argument, that a service provider has no legitimate reason to monitor the contents of an Internet site, may not be as rock solid as it appears).

penetrable.'"[229] This reasoning would provide a greater expectation of privacy in password protected or limited-access social networking profiles. The greatest problem with social networking profiles that are open to numerous "friends" would then lie in the risk that one of these "friends" would pass the information along to the government.

[35] However, the decision discussed above is not the only one to reject the idea that e-mail and Internet communication can enjoy reasonable expectations of privacy.[230] One district court stated that, "while individuals generally possess a reasonable expectation of privacy, for Fourth Amendment purposes, in their home computers, they do not enjoy such an expectation of privacy in transmissions over the internet or in e-mail which has already arrived at the recipient."[231] However, properly understood, this rule should apply only to the actions of the recipient, not to any unrelated subsequent search or seizure merely by virtue of the communication reaching its recipient.

---

[229] LAFAVE, *supra* note 227 (footnote omitted) (quoting Randolph S. Sergeant, Note, *A Fourth Amendment Model for Computer Networks and Data Privacy*, 81 VA. L. REV. 1189, 1200 (1995); *accord D'Andrea*, 497 F. Supp. 2d at 121.

[230] *See Gines-Perez*, 214 F. Supp. 2d at 225-26 (explaining that defendant had no subjective expectation of privacy in photograph placed on the public medium of the Internet, society was not prepared to recognize as reasonable any expectation of privacy in information placed on Internet, and the picture was obviously placed on website for commercial purposes); *see also* Konop v. Hawaiian Airlines, Inc., 236 F.3d 1035, 1045 (9th Cir. 2001) ("No expectation of privacy attaches to electronic communications made available through facilities readily available to the public . . . ."); United States v. Hambrick, No. 99-4793, 2000 WL 1062039, at *4 (4th Cir. 2000) (holding that there is no legitimate expectation of privacy in non-content customer information provided to an ISP by one of its customers)); In re Pharmatrak, Inc. Privacy Litigation, 220 F. Supp. 2d 4, 13 (Mass. Dist. Ct. 2002) (holding web-monitoring company's conduct in intercepting Internet users' electronic communications with various health-related and medical-related Internet websites and sharing of private information about their web browsing habits and confidential health information with defendant pharmaceutical companies fell under the exception from liability under the Stored Wire and Electronic Communications and Transactional Records Act).

[231] United States v. Rodriguez, 532 F. Supp. 2d 332, 339 (D.P.R. 2007) (citing United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004).

C. Privacy in E-mail and Other Electronic Communication

[36] In deciding cases involving e-mail privacy and whether the use of electronically mediated communication technologies constitutes a waiver of privacy rights, courts have tended to analogize e-mail to more traditional types of communication, such as letters or telephone calls,[232] although, as mentioned above, not all judges have been apt to follow this course.[233] Courts have also relied on the privacy policies and terms of use propagated by the Internet Service Providers in question,[234] as well as the identity of the recipient.[235] Intermediaries, usually an Internet Service Provider ("ISP"), transmit and deliver e-mails like letters or telephone calls, so such analogies appear to be well grounded and highly relevant to the waiver issue.[236] As such, the law ought to apply to e-mail, and other forms of private mediated electronic communication, in much the same way as it has to its offline counterparts. Indeed, a number of courts have held that, by default, individuals have legitimate privacy interests in their e-mail and computer files, despite the use of an intermediary.[237]

[232] *See* United States v. Maxwell, 45 M.J. 406, 417 (C.A.A.F. 1996); *see also* Warshak v. United States, 490 F.3d 455, 470 (6th Cir. 2007), *vacated*, 532 F.3d 521 (6th Cir. 2008).

[233] *See* United States v. Walser, 275 F.3d 981, 986 (10th Cir. 2001) ("The advent of the electronic age and . . . the development of desktop computers . . . go beyond the established categories of constitutional doctrine. Analogies to other physical objects, such as dressers or file cabinets, do not often inform the situations we now face as judges when applying search and seizure law."); United States v. Hambrick, 55 F. Supp. 2d 504, 508 (W.D. Va. 1999) ("Cyberspace is a nonphysical 'place' and its very structure, a computer and telephone network that connects millions of users, defies traditional Fourth Amendment analysis."), *aff'd* 2000 WL 1062039 (4th Cir. 2000). *See generally* Hodge, *supra* note 19, at 102.

[234] *See* Hodge, *supra* note 19, at 104-05 (citing *Maxwell*, 45 M.J. at 417).

[235] United States v. Charbonneau, 979 F. Supp. 1177, 1185 (S.D. Ohio 1997) ("The expectations of privacy in e-mail transmissions depend in large part on both the type of e-mail sent and recipient of the e-mail.").

[236] *Id*.

[237] *See id.* at 1184.

[37] Additionally, this reasonable expectation applies to communication sent from government or work computers.[238] Problems arise, however, when the intermediary has a policy of monitoring communications sent through its service.[239] In these cases, the individual waives his or her expectation of privacy as a condition of using the service in question.[240] Potentially, a large number of recipients might also diminish an otherwise reasonable expectation of privacy.[241] This potential caveat is especially relevant in the context of OSNs, such as Facebook and MySpace, where large numbers of friends may view even limited-access profiles.[242] However, there is a difference between electronic communications intended for public consumption, or at least visible to the public at large, and those limited to access by a specifically delineated group.[243] As such, postings to publically accessible websites,[244] chat rooms,[245] electronic

[238] *See, e.g.*, United States v. Long, 61 M.J. 539, 543-44 (N-M. Ct. Crim. App. 2005).

[239] *See* United States v. Monroe, 52 M.J. 326, 330 (C.A.A.F. 2000) (stating that an individual lacked a reasonable expectation of privacy in the e-mails sent on the Air Force system, where a specific notice was given that persons logging on to the system consented to monitoring); Hodge, *supra* note 17, at 105-06; *see also* United States v. Simons, 206 F.3d 392, 398 (4th Cir. 2000) (holding that an employee lacked a reasonable expectation of privacy in electronic files on his office computer because of employment policies that explicitly authorized the employer to "audit, inspect, and/or monitor" such files).

[240] *See, e.g.*, *Simons*, 206 F.3d at 398.

[241] Hodge, *supra* note 19, at 105 (citing United States v. Maxwell, 45 M.J. 406, 419 (C.A.A.F. 1996)).

[242] *See* Kevin Lewis et al., *The Taste for Privacy: An Analysis of College Student Privacy Settings in an Online Social Network*, 14 J. COMPUTER-MEDIATED COMM. 79, 81 (2008).

[243] *See* Warshak v. United States, 490 F.3d 455, 472 (6th Cir. 2007) ("[T]he public disclosure of material to an untold number of readers distinguishes bulletin board postings from e-mails, which typically have a limited, select number of recipients."), *vacated*, 532 F.3d 521, (6th Cir. 2008).

[244] *See* United States v. Gines-Perez, 214 F. Supp. 2d 205, 225 (D.P.R. 2002) (holding that there is no expectation of privacy when posting a photo on publically available website).

[245] *See* Commonwealth v. Proetto, 771 A.2d 823, 831 (Pa. Super. Ct. 2001).

bulletin boards,[246] and social network profiles,[247] essentially merit no such expectation of privacy.

[38] In *Warshak v. United States*, the Sixth Circuit analogized the Supreme Court precedent in *Katz*, *Smith*, and *Miller* to situations involving e-mail communications.[248] The court recognized that, as *Katz* pointed out, "the mere fact that a communication is shared with another person does not entirely erode all expectations of privacy . . . ."[249] In situations of shared communication, courts should differentiate between those parties with whom the individual shares the communication and those from whom the individual shields the communication.[250] Despite the fact that a person assumes the risk that those with whom he communicates will reveal the information to the government,

> The same does not necessarily apply, however, to an intermediary that merely has the ability to access the information sought by the government. Otherwise phone conversations would never be protected, merely because the telephone company can access them; letters would never be protected, by virtue of the Postal Service's ability to access them; the contents of shared safe deposit boxes or storage lockers would never be protected, by virtue of the bank or storage company's ability to access them.[251]

Courts limit this expectation of privacy in the information stored by the intermediary, however, to the content of the communication, as set out in *Smith*.[252] The *Warshak* court held that,

[246] *See* Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001).

[247] *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 861 (Cal. Ct. App. 2009).

[248] *Warshak,* 490 F.3d at 469-70.

[249] *Id*. at 470.

[250] *Id*.

[251] *Id*.

[252] *See id*. at 471.

> [A]lthough the government can compel disclosure of a shared communication from the party with whom it was shared, it can only compel disclosure of the specific information to which the subject of its compulsion has been granted access. It cannot, on the other hand, bootstrap an intermediary's limited access to one part of the communication (e.g. the phone number) to allow it access to another part (the content of the conversation).[253]

Under this analysis, compelled disclosure of subscriber information and related non-content information from an individual's ISP would not violate the individual's Fourth Amendment interests under the authority of *Smith* and *Miller*.[254] In contrast, "there is a societal expectation that the ISP or the phone company" will not reveal the contents of the communication "as a matter of course."[255] Indeed, the major OSNs and many other ISPs include this in their privacy policies.[256] The government's subpoena of the content of the communication from the *recipient* of the e-mail – or the "friend" in the OSN context – however, would not infringe on the individual's interests because of the individual's assumption of that risk.[257] This risk does not necessarily extend to the intermediate storage of the information, but it arises only after the final recipient has accessed the e-mail.[258] Additionally, the USA-PATRIOT Act[259] enlarged the definition of a pen register to include "addressing

[253] *Warshak,* 490 F.3d at 471.

[254] *See id.*

[255] *Id.*

[256] *See* Hodge, *supra* note 19, at 119.

[257] *See Warshak,* 490 F.3d at 471; SOLOVE, *supra* note 1, at 204-05 (noting the Department of Justice has interpreted provisions of the Stored Communications Act to allow them to issue subpoenas to ISPs for the contents of the e-mail in question).

[258] *See* SOLOVE, *supra* note 1, at 204-05.

[259] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

information on emails and IP addresses."[260] Government authorization to retrieve this information is not difficult to obtain.[261]

[39] A few circuit court decisions involving use of computer networks have addressed this issue. The Fourth Circuit held that an employee lacked a reasonable expectation of privacy in electronic files on his office computer because of employment policies that explicitly authorized the employer to "audit, inspect, and/or monitor" such files.[262] The Ninth Circuit, however, held that a university student did not waive an expectation of privacy in his computer files on his personal computer even though he attached it to the university network, because the university's policies did not allow blanket monitoring or specifically abrogate such an expectation.[263]

> In instances where a user agreement explicitly provides that e-mails and other files will be monitored or audited as in *Simons*, the user's knowledge of this fact may well extinguish his reasonable expectation of privacy. Without such a statement, however, the service provider's control over the files and ability to access them under certain limited circumstances will not be enough to overcome an expectation of privacy . . . .[264]

Although Fourth Amendment law contains doctrines that might potentially protect information in limited-access profiles, its application to OSN profile information has not been tested, and some doubt exists as to whether protection would survive constitutional scrutiny under the

[260] SOLOVE, *supra* note 1, at 205.

[261] *See id.* at 206.

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

[263] *See* United States v. Heckenkamp, 482 F.3d 1142, 1147 (9th Cir. 2007).

[264] Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007) *vacated*, 532 F.3d 521 (6th Cir. 2008).

approach the Supreme Court has taken with respect to the rules described above.[265]

VI. Reasonable Expectations of Privacy Under the Canadian Charter of Rights and Freedoms

[40] As in the United States, "[t]here is no explicit constitutional protection of privacy in Canada . . . ."[266] Canadian privacy protection under its Charter of Rights and Freedoms, however, seeks to protect the "dignity, integrity and autonomy" of its citizens.[267] The Canadian approach may provide a desirable middle ground between the privacy approaches of the United States and Europe.[268] However, recent decisions determining the reasonableness of an individual's expectation of privacy in limited-access OSN profile information have not provided much guidance.[269]

A. The Parameters of Canadian Privacy Protection

[41] Two sections of the Charter of Rights and Freedoms provide relevant privacy protection; Section 8 of the Canadian Charter protects individuals against unreasonable searches and seizures by the government,[270] in much the same way as the Fourth Amendment in the United States,[271] and Section 7 protects the "security of the person."[272]

[265] *See* Hodge, *supra* note 19, at 118-19.

[266] Levin & Nicholson, *supra* note 29, at 378.

[267] R. v. Plant, 1993 CarswellAlta 94, paras. 24, 27 (Can. S.C.C.) (WL).

[268] Levin & Nicholson, *supra* note 29, at 357.

[269] *See* Leduc v. Roman, 2009 CarswellOnt 843, paras. 1, 32-33 (Can. Ont. Sup. Ct. J.) (WL); Murphy v. Perger, 2007 CarswellOnt 9439, paras. 1, 16, 17, 19, 20 (Can. Ont. Sup. Ct. J.) (WL).

[270] *See* Canadian Charter *supra* note 38, § 8.

[271] Levin & Nicholson, *supra* note 27, at 378.

[272] Canadian Charter, *supra* note 38, § 7.

Both of these sections rely in some measure on an individual's reasonable expectation of privacy.[273] In 1984, the Canadian Supreme Court declared that such an expectation lies at the core of Section 8.[274] Like the American Fourth Amendment, Section 8 only protects against governmental intrusions into expectations that are objectively reasonable.[275] In the criminal context, the court has outlined three conditions that must be met for a search to be reasonable.[276] These requirements compare to those found in their U.S. counterpart, including prior independent judicial authorization, often a warrant, based on probable grounds that evidence of the offence will be found at the searched location.[277] Later courts, however, have determined that these criteria do not establish necessarily hard and fast rules strictly applied in every case, and some measure of reasonable analysis of the context of any given search may warrant some leniency.[278] Rather, the requirements are designed to ensure a proper "balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement." [279]

---

[273] Jason M. Young, *Constitutional Rights in New Technologies in Canada*, *in* CONSTITUTIONAL RIGHTS AND NEW TECHNOLOGIES 57, 65 (Ronald Leenes, Bert-Jaap Koops & Paul De Hert eds., 2008) [hereinafter CONSTITUTIONAL RIGHTS]; *see* R. v. Mills, 1999 CarswellAlta 1055 (Can. S.C.C.) (WL); Hunter v. Southam, Inc., 1984 CarswellAlta 121, para. 25 (Can. S.C.C.) (WL).

[274] CONSTITUTIONAL RIGHTS, *supra* note 273, at 63; *see Southam, Inc.*, 1984 CarswellAlta 121, para. 25.

[275] *See Southam, Inc.*, 1984 CarswellAlta 121, para. 24-25; CONSTITUTIONAL RIGHTS, *supra* note 273, at 63.

[276] CONSTITUTIONAL RIGHTS, *supra* note 273, at 63-64.

[277] *See Southam, Inc.*, 1984 CarswellAlta 121, para. 23; STANLEY A. COHEN, PRIVACY, CRIME AND TERROR LEGAL RIGHTS AND SECURITY IN A TIME OF PERIL 114 (2005); CONSTITUTIONAL RIGHTS, *supra* note 275, at 64.

[278] *See* Thomson Newspapers Ltd. v. Canada, 1990 CarswellOnt 92, para. 96 (Can. S.C.C.) (WL);; COHEN, *supra* note 277; CONSTITUTIONAL RIGHTS, *supra* note 273, at 64; *see also* R. v. Collins, 1987 CarswellBC 94, para. 22 (Can. S.C.C.) (WL).

[279] R. v. Plant, 1993 CarswellAlta 94, para. 26 (Can. S.C.C.) (WL).

[42] Additionally, Section 8 applies to the appropriation of digital data and files,[280] and works alongside Section 7's inherent privacy protection, which protects an individual's privacy as "either incidental to personal security, or an aspect of personal liberty."[281] When determining whether a reasonable expectation of privacy exists in stored or acquired data and other information, the courts have delineated a long list of relevant factors to consider.[282] In application, "the most determinative factor" in the context of digital information has become the nature of the information itself.[283] Business information receives much less protection than more personal data that reflects the "biographical core" of the individual, such as information that reveals personal lifestyle choices.[284] Additional non-personal information, such as public utility records, may not attract a reasonable expectation of privacy.[285] In *R. v. Plant*, the Supreme Court stated that it agreed with the aspect of the U.S. Supreme Court's holding in *United States v Miller* that "[i]n order for constitutional protection to be extended . . . the information seized must be of a personal and confidential nature."[286] The court also held that,

> In fostering the underlying values of dignity, integrity and autonomy . . . [section] 8 . . . seek[s] to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate

[280] *See* R. v. Wong, 1990 CarswellOnt 58, paras. 8, 10, 13 (Can. S.C.C.) (WL), CONSTITUTIONAL RIGHTS, *supra* note 273, at 64-65.

[281] CONSTITUTIONAL RIGHTS, *supra* note 273, at 65 (footnote omitted).

[282] *Id*. at 65-66.

[283] *Id*. at 66.

[284] *Id*. (internal quotation marks omitted).

[285] CONSTITUTIONAL RIGHTS, *supra* note 273, at 68.

[286] R. v. Plant, 1993 CarswellAlta 94, para. 23, 27 (Can. S.C.C.) (WL).

> details of the lifestyle and personal choices of the individual.[287]

B. Communications Privacy in Canada

[43] The Canadian Criminal code provides strong privacy protection to telephone communications.[288] According to the Supreme Court, "the interception of private communications is a serious matter, to be considered only for the investigation of serious offences, in the presence of probable grounds, and with a serious testing of the need for electronic interception in the context of the particular investigation . . . ."[289] Courts require judicial authorization to intercept telephone conversations,[290] and only generally allow interception when "practically speaking, [there is] no other reasonable alternative method of investigation, in the circumstances of the particular criminal inquiry."[291] Despite these established rules regarding wiretapping, however, some questions remain about how this protection applies to e-mail and information in other digital contexts.[292] Some lower courts have found that a reasonable expectation of privacy exists in e-mail correspondence, thus bringing it within the protections of the Charter,[293] however, this expectation of privacy is lower than that granted to "first class (letter) mail, because unencrypted e-mails are vulnerable to being read by intermediaries."[294] After Canadian adoption

[287] *Id*. at para. 27.

[288] *See* CONSTITUTIONAL RIGHTS, *supra* note 273, at 71-72.

[289] R. v. Araujo, 2000 CarswellBC 2440, para. 29 (Can. S.C.C.) (WL) (emphasis omitted).

[290] CONSTITUTIONAL RIGHTS, *supra* note 273, at 71.

[291] *Araujo*, 2000 CarswellBC 2440, para. 29 (emphasis omitted).

[292] *See* CONSTITUTIONAL RIGHTS, *supra* note 273, at 72.

[293] CONSTITUTIONAL RIGHTS, *supra* note 273, at 72; *see, e.g.*, R. v. Weir, 1998 CarswellAlta 151, para. 77 (Can. Alta. Q.B.) (WL).

[294] CONSTITUTIONAL RIGHTS, *supra* note 273, at 72 -73; *see Weir*, 1998 CarswellAlta 151, paras. 72-75, 77 ("The envelope on first class mail shields the contents of the message. The information on the cover carries a lower expectation of privacy than does

of the European Convention on Cybercrime, the Government stated that it would subject orders for the production of "specified computer data" or "subscriber information" and Internet traffic data containing mostly non-content data to this lower expectation of privacy as well.[295] In a Department of Justice consultation paper published in 2002, the government stated that "the standard for Internet traffic data should be more in line with that required for telephone records and dial number recorders in light of the lower expectation of privacy in a telephone number or Internet address, as opposed to the content of a communication."[296] The constitutionality of this lower standard in such data remains in question because Section 8 of the Charter "protects people, not places"[297] or things, and the degree of intrusiveness of an action should depend on "to what extent disclosure of [the] information would impact the reasonable expectation of the individual's privacy."[298]

---

the message inside. In the e-mail environment, the headers (hidden and exposed) can be likened to the information on the envelope. The message is directed by its headers. Much repair work to e-mail can be done through headers. Like the outside of the envelope, the headers have a lower expectation of privacy. The difference between the two types of cover is that in first class mail the cover is respected. In e-mail, the cover is (or was in June of 1996) routinely violated in order to repair the technology. There are two or three levels of violation depending on the type of repair done and excluding a repair done by deleting the message or by enlarging the e-mail box. The size of the attachments may be viewed. The list of attachment names may be viewed. The message itself may be opened which can include looking at the message and the attachments or either. These facts about the technology help [this court] to conclude the e-mail message is unlike first class mail in the level of privacy that it can attract. Another difference between e-mail and first class mail is that in order to make an e-mail message truly private, one can encrypt it.").

[295] CONSTITUTIONAL RIGHTS, *supra* note 273, at 73-74 (internal quotation marks omitted).

[296] DEP'T OF JUSTICE CAN., LAWFUL ACCESS – CONSULTATION DOCUMENT 11-12 (2002), *available at* http://www.justice.gc.ca/eng/cons/la-al/la-al.pdf.

[297] R. v. Edwards, 1996 CarswellOnt 1916, para. 45 (Can. S.C.C.) (WL).

[298] CONSTITUTIONAL RIGHTS, *supra* note 273, at 75 (citing *Edwards*, 1996 CarswellOnt 1916).

C. Recent Decisions Involving OSN Profile Information

[44] Recent cases involving requests for discovery of profile information have tested Canada's respect for privacy in information contained in OSN profiles. In fact, it is "beyond controversy" in Canada that "a person's Facebook profile may contain documents relevant to the issues in an action."[299] The courts have had little difficulty allowing such requests for publically available information, and courts have admitted such information as evidence in a number of proceedings.[300] However, in *Murphy v. Perger* and *Leduc v. Roman* – both personal injury suits arising out of automobile accidents – the court considered the appropriateness of requests for limited-access Facebook profile information.[301] In *Murphy*, the plaintiff posted photos on her publicly accessible profile that showed her "engaged in various social activities."[302] The defendant wanted access to any photographs on the limited-access portion of the plaintiff's profile.[303] In granting the defendant's motion, the court stated that

> It seems reasonable to conclude that there are likely to be relevant photographs on the site for two reasons. First, www.facebook.com is a social networking site where [the court] understand[s] a very large number of photographs

[299] Leduc v. Roman, 2009 CarswellOnt 843, para. 23 (Can. Ont. Sup. Ct. J.) (WL).

[300] *See id.* ("Photographs of parties posted to their Facebook profiles have been admitted as evidence relevant to demonstrating a party's ability to engage in sports and other recreational activities where the plaintiff has put his enjoyment of life or ability to work in issue: Cikojevic v. Timm, 2008 BCSC 74 (B.C. Master), para. 47; R. (C.M.) v. R (O.D.), 2008 NBQB 253 (N.B. Q.B.), paras. 54 and 61; Kourtesis v. Joris, [2007] O.J. No. 2677 (Ont. S.C.J.), paras. 72 to 75; Goodridge (Litigation Guardian of) v. King, 161 A.C.W.S. (3d) 984 (Ont. Sup. Ct.) [2007 CarswellOnt 7637 (Ont. S.C.J.)], para. 128. In one case the discovery of photographs of a party posted on a MySpace webpage formed the basis for a request to produce additional photographs not posted on the site: Weber v. Dyck, [2007] O.J. No. 2384 (Ont. Master).").

[301] *See Roman*, 2009 CarswellOnt 843, para. 1; Murphy v. Peger, 2007 CarswellOnt 9439, paras. 1-2 (Can. Ont. Sup. Ct. J.) (WL).

[302] *Perger*, 2007 CarswellOnt 9439, para. 4.

[303] *See id.* at para. 1.

> are deposited by its audience. Second, given that the public site includes photographs, it seems reasonable to conclude the private site would as well.
>
> On the issue of relevancy, in this case, clearly the plaintiff must consider that some photographs are relevant to her claim because she has served photographs of her prior to the accident, notwithstanding that they are only "snapshots in time."[304]

The court ordered the production of the limited-access profile information at issue, concluding that "*any invasion of privacy is minimal* and is outweighed by the defendant's need to have the photographs in order to assess the case."[305] The court considered the number of the plaintiff's friends who could access the sought after contents of the plaintiff's profile as specifically determinative, holding that "[t]he plaintiff could not have a serious expectation of privacy given that 366 people have been granted access to the private site."[306]

[45] More recently, the Superior Court of Ontario rejected the decision of a Master and permitted the defendant to cross-examine the plaintiff on his Supplementary Affidavit of Documents "regarding the kind of content posted on his [private] Facebook profile."[307] In *Leduc*, the defendant sought production of material on the plaintiff's private profile after the plaintiff admitted during his psychiatric examination that he had many friends on Facebook.[308] His Facebook profile was almost exclusively private, and the public page contained only his name and photograph.[309] In his contrary decision, the Master had concluded the defendant engaged

[304] *Id.* at paras. 17-18.

[305] *Id.* at para. 20 (emphasis added).

[306] *Id.*

[307] Leduc v. Roman, 2009 CarswellOnt 843, paras. 36-37 (Can. Ont. Sup. Ct. J.) (WL).

[308] *See id.* at paras. 3, 6.

[309] *Id.* at para. 5.

in "'a fishing expedition,'" had failed to show that relevant materials were likely to be found in the plaintiff's profile, and had also failed to ask the plaintiff during discovery whether any relevant photos existed in any form.[310]

[46] The court found no problem with the idea that information obtained from publicly accessible OSN profiles fell within the proper scope of discovery.[311] The court also agreed with the *Murphy* decision that "it is reasonable to infer from the presence of content on the party's public profile that similar content likely exists on the private profile."[312] However, most importantly, the court concluded that

> Where, as in the present case, a party maintains only a private Facebook profile and his public page posts nothing other than information about the user's identity . . . a court can infer from the social networking purpose of Facebook, and the applications it offers to users such as the posting of photographs, that users intend to take advantage of Facebook's applications to make personal information available to others.[313]

The court further found that

> A party who maintains a private, or limited access, Facebook profile stands in no different position than one who sets up a publicly-available profile . . . . Mr. Leduc exercised control over a social networking and information site to which he allowed designated "friends" access. It is reasonable to infer that his social networking site likely

[310] *See id.* at para. 32.

[311] *See id.* at paras. 27, 29.

[312] *Roman*, 2009 CarswellOnt 843, para. 30.

[313] *Id*. at para. 31.

> contains some content relevant to the issue of how Mr. Leduc has been able to lead his life since the accident.[314]

These two decisions, although concerned primarily with the application of Canadian Civil Procedure rules to OSN profile information, illustrate the limited sanctity afforded an individual's otherwise subjective expectation that his private OSN profile information will stay private.[315] When courts define an order to produce limited-access photographs and other information as a "minimal" invasion of privacy, solely because courts can "infer" from the general nature of social networking websites that a plaintiff has posted relevant information to their profile, courts severely curtail an individual's subjective – and arguably reasonable – expectation of privacy.[316]

VII. PROTECTING PRIVACY ON GROUNDS OF HUMAN DIGNITY: THE EUROPEAN CONVENTION ON HUMAN RIGHTS AND FUNDAMENTAL FREEDOMS

[47] Article 8 of the European Convention on Human Rights ("Convention") delineates a specific right related to individual privacy, namely that signatory nations respect a person's right to "his private and family life, his home and his correspondence."[317] This right provides for both negative and positive obligations upon public authorities bound by

[314] *Id.* at para. 32.

[315] *See generally id.* at paras. 31-32; Murphey v. Perger, 2007 CarswellOnt 9439, para. 17-18 (Can. Ont. Sup. Ct. J.) (WL).

[316] *See Roman*, 2009 CarswellOnt 843, paras. 25, 32.

[317] ECHR, *supra* note 39 ("[1] Everyone has the right to respect for his private and family life, his home and his correspondence. [2] There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.").

the Convention.[318] Public authorities may only interfere with this right to a private life when, "in accordance with the law," such action "is necessary in a democratic society" and related to important national interests such as "national security, public safety or the economic well-being of the country," or "for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[319] This requirement therefore compels a balancing of "the competing interests of the individual and of the whole community."[320] The court has held that the phrase "in accordance with the law" means any interfering action must accord with national law and that the national law itself must reflect the rights protected by the Convention.[321]

[48] Indeed, because "there must be a measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by [Article 8 § 1]"[322] the Court subjects the national laws themselves to its test of adequacy under Article 8.[323] National laws must give individuals adequate warning of those circumstances where national authorities may interfere with the individual's private life.[324] If

[318] *See*, K.U. v. Finland, No. 2872/02, 48 Eur. H.R. Rep. 52, 1248 § 42 (2009) ("[A]lthough the object of Article 8 is essentially to protect the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life.") (citation omitted).

[319] ECHR, *supra* note 39, at art.8 § 1.

[320] *See* Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 41, 68 § 57.

[321] Copland v. United Kingdom, App. No. 62617/00, 45 Eur. H.R. Rep. 37, 867 § 45 (2007).

[322] *Id.*

[323] *Id.* § 46.

[324] *See, e.g.*, *id.*

they do not, action in reliance on the law that interferes with an individual's private life may violate the Convention.[325]

[49] Despite differences among various jurisdictions,[326] this European take on privacy generally centers on protecting an individual's dignity.[327] Protecting dignity, unlike the more American focus on liberty, finds its focus on guarding social status and protecting individuals from humiliation and preventing unwarranted social perception, and is a social concept that reflects social norms.[328] These social values are apparent in European data protection legislation,[329] as well as in case law of the European Court of Human Rights. National courts in dualist jurisdictions, like the United Kingdom or the Republic of Ireland, which require implementing legislation to give full effect to the Convention in domestic law, "are obliged to take 'into account' the case law of the European Court of Human Rights . . . when determining questions which arise 'in connection' with the right to respect for private life" in the implementing legislation.[330] In addition, with adoption of the Lisbon Treaty, the European Union officially acceded to the ECHR[331] and the Convention has become part of the general law of the Union[332] granting the ECHR's decisions greater institutional backing in Europe. The Treaty of Lisbon

[325] *See id.* § 48-49.

[326] *See generally* Levin & Nicholson, *supra* note 29, at 389-90.

[327] *Id.* at 388.

[328] *See id.*

[329] *Id.* at 390.

[330] N. A. Moreham, *The Right to Respect for Private Life in the European Convention on Human Rights: A Re-Examination*, EUR. HUM. RTS. L. REV., 2008, at 44, 44.

[331] Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Communities, art. 1, § 8, para. 2, Dec. 13, 2007, 2007 O.J. (C 306) [hereinafter Treaty of Lisbon], *available at* http://eur-lex.europa.eu/en/treaties/dat/12007L/htm/12007L.html.

[332] *Id.* at para. 3.

also grants the European Charter – and its core respect for human dignity – "the same legal value as the Treaties."[333]

A. The Right to a Private Life Under Article 8

[50] The European Court of Human Rights has broadly interpreted the right of privacy.[334] Among its broad protections, Article 8's guarantee of a private life "is primarily intended to ensure the development, without outside interference, of the personality of each individual in his relations with other human beings."[335] It specifically protects an individual's right to "a sphere within which he or she can freely pursue the development and fulfilment [sic] of his or her personality"[336] and "the right to establish details of their identity as individual human beings."[337] Protection for the development of personality does not apply only to private matters kept within the individual's closest circle,[338] but explicitly encompasses the "right to establish and develop relationships with other human beings and the outside world" as well.[339] Interaction with others – even in a public context or involving matters of a business or professional nature[340] – may

[333] *Id.* at para. 1.

[334] *See infra* notes 335-41 and accompanying text.

[335] Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 41, 66 § 50; *see also* Botta v. Italy, 1998-I Eur. Ct. H.R. 412, 422 § 32; Niemietz v. Germany, 251 Eur. Ct. H.R.(ser. A) at 33 § 29 (1992).

[336] Sidabras v. Lithuania, 2004-VIII Eur. Ct. H.R. 367, 385 § 43.

[337] Goodwin v. United Kingdom, 2002-VI Eur. Ct. H.R. 1, 31 § 90; *see also* Pretty v. United Kingdom, 2002-III Eur. Ct. H.R. 155, 193 § 61.

[338] *Niemietz*, 251 Eur. Ct. H.R. at 33 § 29.

[339] Peck v. United Kingdom, 2003-I Eur. Ct. H.R. 123, 142 § 57.

[340] *Niemietz*, 251 Eur. Ct. H.R. at 33-34 § 29 ("[I]t is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world.").

fall within the scope of Article 8's notion of "private life."[341] When determining whether a person's activities in the public sphere implicate private life considerations, that person's reasonable expectations of privacy can be a significant factor.[342] As such, appropriate and expected analog or technical monitoring – as by closed-circuit video cameras – may not be a problem.[343] However, "the recording of the data and the systematic or permanent nature of the record may give rise to such considerations."[344] In a recent case, sounding much like Warren and Brandeis in 1890, the court stated that "increased vigilance in protecting private life is necessary to contend with new communication technologies which make it possible to store and reproduce personal data."[345]

B. Legitimate and Reasonable Expectations of Privacy

[51] All individuals – both those known broadly to the public and those absent from the public spotlight – "enjoy a 'legitimate expectation' of protection and respect for their private [lives]."[346] In addition, individuals may enjoy a legitimate expectation of privacy in their telephone calls,[347] e-mails, and Internet usage,[348] which extends to information about the length and time of the communication as well as the numbers dialled.[349]

[341] Von Hannover v Germany, 2004-VI Eur. Ct. H.R. 41, 66 § 50; *Peck*, 2003-I Eur. Ct. H.R. at 142 § 57; P.G. v. United Kingdom, 2001-IX Eur. Ct. H.R. 123, 217 § 56.

[342] *See P.G.*, 2001-IX Eur. Ct. H.R. at 217 § 57; *see also Peck*, 2003-I Eur. Ct. H.R. at 142 § 58.

[343] *See Peck*, 2003-I Eur. Ct. H.R. at 142 §§ 58-59; *P.G.*, 2001-IX Eur. Ct. H.R at 217-18 § 57.

[344] *Peck*, 2003-I Eur. Ct. H.R. at 142 § 59; *see P.G.*, 2001-IX Eur. Ct. H.R at 218 § 57.

[345] *Von Hannover*, 2004-VI Eur. Ct. H.R. at 71 § 70.

[346] *Id.* § 69; Halford v. United Kingdom, 1997-III Eur. Ct. H.R. 1004, 1016 §45.

[347] *See, e.g.*, Copland v. United Kingdom, App. No. 62617/00, 45 Eur. H.R. Rep. 37, 866 § 42 (2007); *see Halford*, 1997-III Eur. Ct. H.R. at 1016 § 45.

[348] *Copland*, 45 Eur. H.R. Rep. 37 at 866 § 42.

[349] *See id.* at 867 § 43.

Under ECHR jurisprudence, an expectation of privacy exists in this non-content oriented information such as "the date and length of telephone conversations and in particular the numbers dialled [sic]" because "such information constitutes an 'integral element of the communications made by telephone.'"[350] This recognition contrasts with United States law withholding constitutional privacy protection for "pen register" information because, by initiating the communication, the individual has voluntarily revealed it to the third party communications service provider, thus waiving any legitimate expectation.[351]

[52] The "reasonable expectation of privacy" test found its way into the ECHR's private life jurisprudence in the 1997 case of *Halford v. The United Kingdom*.[352] In that case, a government employee sued the government for intercepting telephone conversations made from her office and home phones and reviewing the resulting transcripts.[353] Because Ms. Halford had no reason to expect anyone might monitor her telephone conversations, the court concluded that she maintained a reasonable expectation of privacy in her calls made from her office telephone.[354] Following *Halford*, the court has begun to utilize the reasonable expectations test as "a nuanced approach to every new case" in line with common sense.[355] In *Von Hannover v. Germany*, Judge Zupančič stated in his concurring opinion that he would suggest the outcome of that case turn

[350] *Id.* (quoting Malone v. United Kingdom, App. No. 8691/79, 1984 Y.B. Eur. Conv. on H.R. 289, 292 (Eur. Ct. H.R.); *see also* Moreham, *supra* note 333, at 63.

[351] *See* Smith v. Maryland, 442 U.S. 735, 744 (1979). On the other hand, Title III of the Electronic Communications Privacy Act (ECPA) provides for some limited protection of pen register type information against action by the government. *See generally* Electronic Communications Privacy Act, 18 U.S.C. §§ 3121-23 (2006). Under Title III, this requires a court order upon a showing that information relevant to a criminal investigation is likely to be obtained. *See id* § 3123(a).

[352] *Halford*, 1997-III Eur. Ct. H.R. at 1016 §§ 44-45.

[353] *See id.* at 1010-11 §§ 16-17.

[354] *Id.* at 1016 § 45.

[355] Von Hannover v. Germany, 2004-VI Eur. Ct. H.R. 41, 78 (Zupančič, J., concurring).

on the "reasonable expectation of privacy" test set out in *Halford*.[356] The court has also found the test useful in a number of other contexts.[357]

C. Protection for Activities in the Public Sphere

[53] Another major difference between the jurisprudence of the ECHR and Fourth Amendment law in the United States is the fact that public activities can be appropriate subject matter of protected private life under Article 8.[358] In a recent, and rather famous example, *Von Hannover v. Germany*, the court held that Princess Caroline of Monaco had a "legitimate expectation" in the protection of her private life that extended to her activities in public.[359] The court found that the German laws that allowed the publication of paparazzi photographs and articles about the applicant's non-official activities violated Article 8.[360] Interestingly, the court found that "scenes from her daily life . . . such as engaging in sport, out walking, leaving a restaurant or on holiday" constituted "activities of a purely private nature."[361] Thus, even in the case of a person used to the public spotlight and, "although the public has a right to be informed," the situation in that case "[did] not come within the sphere of any political or public debate because the published photos and accompanying commentaries relate exclusively to details of the applicant's private life."[362]

---

[356] *Id*.

[357] *See, e.g.*, Peev v. Bulgaria, App. No. 64209/01, HUDOC, § 38 (Eur. Ct. H. R.) (July 26, 2007); Perry v. United Kingdom, 2003-IX Eur. Ct. H.R. 141, 151 § 37, 153 §43 (using the "reasonable expectation of privacy" test, the Court decided that the covert filming of a person on the premises of the police was an interference with his private life); P.G. v. United Kingdom, 2001-IX Eur. Ct. H.R. 195, 217 § 57; *see also* Peck v. United Kingdom, 2003-I Eur. Ct. H.R. 123, 142 § 58.

[358] *See supra* Part V; *infra* pp. 56-57.

[359] *Von Hannover*, 2004-VI Eur. Ct. H.R. at 48 §§ 8-10, 73 § 78 (2004) (Zupančič, J., concurring (internal quotation marks omitted).

[360] *See id.* at 64 § 45 (majority opinion).

[361] *Id*. at 69 § 61.

[362] *Id.* at 70 § 64.

D. Protection for Communication and Correspondence

[54] The Court has not qualified the Article 8 term "correspondence" in the same way as the term "life" by any requirement that it be "private."[363] Telephone calls, e-mail, diaries, letters, and Internet usage, even in places of employment, fall within the scope of Article 8's prohibition on unjustified interference with an individual's correspondence.[364] As previously stated, individuals may have a reasonable expectation of privacy in these forms of communication.[365] Unjustified monitoring, recording, or other interference with an individual's correspondence violates Article 8's prohibition.[366]

[55] In *Niemietz v. Germany*, the ECHR concluded that a search of the applicant's law office and client files, pursuant to a court ordered warrant, violated Article 8.[367] The court found that the term "correspondence" encompassed some information contained in the lawyer's client files [368] and that the warrant was overly broad despite being in accordance with German law.[369] Because the warrant and search were not proportionate to the legitimate aims of the law, the Court concluded the search violated the applicant's rights under Article 8.[370]

[363] Niemietz v. Germany, 251 Eur. Ct. H.R. (ser. A) at, 34 § 41 32 (1992).

[364] *See* Copland v. United Kingdom, App. No. 62617/00, 45 Eur. H.R. Rep. 37, 866 § 41 (2007); *see also* Moreham, *supra* note 330, at 62-64.

[365] *See Copland*, 45 Eur. H.R. Rep. 37 at 866 § 42 (holding true unless, for instance in the workplace, they have advance warning that their use was subject to monitoring); *Von Hannover,* 2004-VI Eur. Ct. H.R. at 66 § 51; Halford v. United Kingdom, 1997-III Eur. Ct. H.R. 1004, 1016 § 45.

[366] *See* Enea v. Italy, App. No. 74912/01, 51 Eur. H.R. Rep. 3, 135 § 135 (2009) (ordering monitoring of a prisoner's correspondence); Huvig v. France, 176 Eur. Ct. H.R. 39, 52 § 25 (1990) (telephone tapping).

[367] *See Niemietz*, 251 Eur. Ct. H.R. at 29 § 11, 41 § 59.

[368] *Id.* at 34 § 32.

[369] See *id.* at35 §§ 34-35, 36 § 37.

[370] *Id.* at36 §§ 37-38.

[56] In *Copland v. The United Kingdom*, the court held that a public college's monitoring of an employee's telephone and e-mail correspondence and Internet usage, "in order to ascertain whether the applicant was making excessive use of College facilities for personal purposes," violated Article 8.[371] The government admitted to conducting "analysis of the college telephone bills showing telephone numbers called, the dates and times of the calls and their length and cost."[372] The government also admitted to analyzing the applicant's Internet usage,[373] and logging her e-mail correspondence.[374] The court held that because the applicant "had been given no warning that her calls would be liable to monitoring," she had a reasonable expectation of privacy in her telephone calls, e-mail, and Internet usage.[375] Consequently, "the collection and storage of personal information relating to the applicant's telephone, as well as to her email and internet usage, without her knowledge, amounted to an interference with her right to respect for her private life and correspondence within the meaning of [Article 8]."[376] Because no United Kingdom law directly applied in force during the relevant time frame, the employer's conduct was not "in accordance with the law" or in furtherance of other legitimate aims.[377] As such, the conduct violated Article 8.[378]

[57] Recently, in the case of *K.U. v. Finland*, the ECHR decided a rather different question related to Article 8 and involving the use of the

[371] Copland v. United Kingdom, App. No. 62617/00, 45 Eur. H.R. Rep. 37, 860 § 10 (2007).

[372] *Id.*

[373] *Id.* at 860 § 11.

[374] *Id.* § 12.

[375] *Id*. at 866 § 42.

[376] *Copland*, 45 Eur. H.R. Rep. 37 at 867 § 44.

[377] *Id.* at 868 § 48 (internal quotation marks omitted).

[378] *Id.* at § 49.

Internet.[379] The court found that communications privacy and freedom of expression must, on occasion, take a back seat to violations of an individual's private life in the context of criminal activity.[380] In the case, an unknown person placed a personal dating advertisement on the Internet, identifying himself as the applicant, a 12-year-old boy, and claiming an interest in a sexual encounter with another boy or man.[381] The applicant received an e-mail from a man, offering to meet him, and "then to see what you want."[382] The boy's father contacted the police and attempted to discover the identity of the person who posted the advertisement, but the ISP refused to turn over the information on confidentiality grounds.[383] The Helsinki District Court also refused a request from the police to require the ISP turn over the information.[384] The ECHR reiterated that respect for private or family life imposed positive obligations on the State,[385] and held that "where fundamental values and essential aspects of private life are at stake, [Article 8] requires efficient criminal-law provisions."[386] Because the State did not provide the applicant or the police with an effective opportunity to fully address the interference by identifying the perpetrator, the State violated Article 8.[387] The court stated that,

> Although freedom of expression and confidentiality of communications are primary considerations and users of

[379] *See generally* K.U. v. Finland, No. 2872/02, 48 Eur. H.R. Rep. 52, 1246 § 35 (2009).

[380] *See id*. at 1248 § 45.

[381] *See id*. at 1239 §§ 7-8.

[382] *Id.* § 8 (internal quotation marks omitted).

[383] *Id.* § 9.

[384] *See Finland*, 48 Eur. H.R. Rep. 52 at 1239 §§ 10-11.

[385] *Id.* at 1248 § 42.

[386] *Id.* § 43.

[387] *See id.* at 1250 § 49.

> telecommunications and internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or *the protection of the rights and freedoms of others*.[388]

[58] As these decisions make clear, the privacy protection granted by Article 8 of the Convention goes well beyond that granted by the Fourth Amendment in the United States. In addition, these decisions also show the strong tendency of the court to accept a much broader view of what constitutes a reasonable expectation of privacy.[389] Much of this effect likely owes its origins to the Convention's conception of protecting private life out of respect for human dignity, rather than focusing merely on control.[390] Granted, the court's decisions turn on the issue of whether the state has acted in accordance with national laws authorizing the action in question.[391] However, as mentioned earlier, the national laws remain subject to the court's review and the court has actively found violations when state action infringes an individual's reasonable expectation of privacy.[392] By finding these reasonable expectations in public activities, e-mail, Internet usage, communication from work, and non-content communication information – many of which would not withstand current Fourth Amendment scrutiny – the court protected the theoretical groundwork of protecting human dignity and the right to a private life. The court therefore potentially provided greater protection to the quasi-private personal information posted to limited–access OSN profiles intended only for viewing by a defined audience.

---

[388] *Finland*, 48 Eur. H.R. Rep. 52 at 1250 § 49. (emphasis added).

[389] *See, e.g.*, *id*. at 1250 § 49.

[390] *See* Levin & Nicholson, *supra* note 29, at 388-89.

[391] *See, e.g.*, Copland v. United Kingdom, App. No. 62617/00, 45 Eur. H.R. Rep. 37, 867 § 46 (2007).

[392] *See id*.

VIII. CONCLUSION

[59] Many OSN users subjectively expect only those to whom they grant access will view the information they post or upload to their profiles.[393] This conception builds on the privacy tools embedded into technologies employed by the OSNs, which allow users the opportunity to control their own privacy settings.[394] It is a conception built on expectations of selective anonymity[395] and network privacy.[396] However, concerns about preserving reputation and dignity often stimulate control exercised by these users when they restrict their privacy settings. These concerns are legitimate, and these expectations arguably reasonable. Yet few courts respect these expectations as something that society is currently prepared to recognize as reasonable, and many courts have not yet tackled the issue head on.[397] Although, with the numbers of online socializers growing[398] – likely concomitant with the number of those holding these subjective expectations of OSN privacy – and the judiciary becoming more familiar with the technology and with these types of cases, perhaps that recognition is possible in the not so distant future. This recognition can be facilitated in multiple ways, including, as this paper has argued, by adopting more contemporary conceptions of what constitutes reasonable expectations of privacy and by affording more respect for human dignity in tests of reasonableness. Because the private life jurisprudence of the ECHR, rooted in the importance of protecting human dignity and reputation by actively preserving respect for the private life and personal matters of the individual, covers the important elements of relationship building, individual relations with other human beings, and the development of personal identity – and not only in purely private settings

[393] *See* Levin & Abril, *supra* note 5, at 1001-02.

[394] *See id*. at 1035, 1045-46.

[395] *See id*. at 1025.

[396] *See id*. at 1045-46.

[397] *See See* Levin & Abril, *supra* note 5, at 1011.

[398] *See id*. at 1017-19.

– its application in the digital communication context fills a void found in the laws of other jurisdictions.