

N O R T H W E S T E R N  
JOURNAL OF TECHNOLOGY  
AND  
INTELLECTUAL PROPERTY

**A (My)Space of One's Own:  
On Privacy and Online Social Networks**

*Patricia Sanchez Abril*



# A (My)Space of One's Own: On Privacy and Online Social Networks

By Patricia Sanchez Abril\*

## I. INTRODUCTION

¶1 It has been called the greatest generation gap since the early days of rock and roll.<sup>1</sup> And, like that famous gap, it is fueling a moral panic that threatens to obscure the value of a new form of community and self-expression.

¶2 Participants in online social networking sites (OSNs) such as MySpace<sup>2</sup> and Facebook<sup>3</sup> (among hundreds of others) revel in the freedom and communion facilitated by the burgeoning social Internet. They often express offense or a feeling of intrusion when their online personae are discovered by meddling parents, employers, or other unintended audiences. Meanwhile offline, the uninitiated and sometimes older generation, fueled by the dizzying media chatter regarding sexual predation, pornography, and cyber-bullying on OSNs,<sup>4</sup> scoff at their protectorate's foolhardy disclosure of personal stories, images, and information online, concluding that these will inevitably invite social and professional disgrace. They accuse OSN participants of being ignorant of the technology's risks, not caring about privacy, or having poor judgment. Moreover, some subscribe to the notion that online privacy is non-existent and its protection, whether legal or practical, is therefore futile.

¶3 It is only by sidestepping the predominant fear and mistrust of the technology and objectively understanding the often generation-specific conceptualizations of privacy that we can expose the shortcomings in this area and inform new law, ethics, and technology that can apply to modern harms.

¶4 To that end, Section II provides a brief overview of online social networking phenomena and outlines some of its real and perceived threats. Section III lays out the current privacy debate between two camps: the net-savvy users of the medium who

---

\* Assistant Professor of Business Law, University of Miami School of Business Administration. B.A., Duke University, 1996; J.D., Harvard Law School, 2000.

<sup>1</sup> Emily Nussbaum, *Say Everything*, N.Y. MAGAZINE, Feb. 12, 2007, at 24, available at <http://www.nymag.com/news/features/27341>.

<sup>2</sup> MySpace.com is a registered trademark of MySpace, Inc. For ease of reference, this article refers to MySpace as exemplary of OSNs.

<sup>3</sup> Facebook.com is a registered trademark of Facebook, Inc.

<sup>4</sup> See, e.g., Julia Angwin, *How Safe Are the Top Social-networking Sites for Teens?*, WALL ST. J., Jul. 24, 2006, at R10; Alex Kumi, *Porn and Bullying Common on MySpace and Bebo, says Which?*, GUARDIAN (U.K.), Sept. 14, 2006, available at <http://www.guardian.co.uk/technology/2006/sep/14/news.uknews>; Kevin Poulsen, *MySpace Predator Caught by Code*, WIRED, Oct. 16, 2006, available at <http://www.wired.com/science/discoveries/news/2006/10/71948>; Susanna Schrobsdorff, *Predator's Playground*, NEWSWEEK, Jan. 26, 2006, available at <http://www.newsweek.com/id/47351>; Greg Toppo, *High-tech Bullying May Be on the Rise, USA TODAY*, Apr. 11, 2006, at 8D; *MySpace: Your Kids' Danger?*, CBS News, Feb. 6, 2006, available at <http://www.cbsnews.com/stories/2006/02/06/eveningnews/main1288944.shtml>.

ground their formulation of privacy in anonymity versus the physical-world generation who find privacy in control over their personal information. Unfortunately for both, neither complete anonymity nor control is possible online. To date, as Section IV describes, the law has embraced the notion of privacy as control over information, thus detrimentally focusing the burden of protecting and adjudicating on the technology's users. In order to allow the medium to flourish positively and accommodate the new privacy challenges, we must redefine the need for it. Section V posits five reasons why privacy and personality should be protected on OSNs and other digital media. The article concludes that the burdens of this protection should be borne by all and offers suggestions on how this can be accomplished.

## II. UNDERSTANDING ONLINE SOCIAL NETWORKS

¶5 If MySpace alone were a country and each of its profiles a person, it would be the 12th most populous nation in the world.<sup>5</sup> The overwhelming magnitude and success of OSNs lies in their unprecedented ability to provide a platform for self-identification, communication, and their unique ability to mimic human intimacy. The ease with which profiles can be created and updated facilitates disclosure and self-invention within a perceived community.

¶6 Participants in the most ubiquitous OSNs, primarily teenagers and young adults,<sup>6</sup> need only a valid e-mail account to set up a profile or page. A profile is a multimedia collage that serves as one's digital "face" in cyberspace using images, video, audio, and links to other profiles and websites. A high tech cross between a bumper sticker and a diary, digital profiles commonly broadcast personal philosophies and preferences, as well as everything from artistic creations to the mundane details of everyday life. Profiles can be adjusted to be public or private, depending on its author's intended audience. Public profiles are searchable and visible to anyone in cyberspace, while accessibility to private profiles is by invitation only.

¶7 These managed identities are linked together by real-world relationships and OSN ties to form a network of "friends." Through these networks of associated profiles, OSN participants can post or exchange photographs and video, send messages to friends instantaneously, join interest groups dedicated to virtually any topic, and leave notes on their friends' profiles that are visible by anyone with access to the profile. As such, self-disclosure is the currency and the means that participants use to "hang out" on OSNs. According to a recent study conducted by the Pew Internet Project, the majority of OSN users generally believe that sharing gossip and personal information about themselves on OSNs is acceptable.<sup>7</sup>

---

<sup>5</sup> MySpace boasts over 100 million users worldwide. Patricia Sellers, *MySpace Cowboys*, FORTUNE, Sept. 4, 2006, at 66. Population-wise, it would fall between Mexico (with a population of approximately 106 million) and the Philippines (with a population of approximately 88 million). UNITED NATION DEPARTMENT OF ECONOMIC AND SOCIAL AFFAIRS, WORLD POPULATION PROSPECTS: THE 2006 REVISION, [http://www.un.org/esa/population/publications/wpp2006/wpp2006\\_highlights\\_rev.pdf](http://www.un.org/esa/population/publications/wpp2006/wpp2006_highlights_rev.pdf).

<sup>6</sup> According to marketing firms, only 10 percent of participants in OSNs are over the age of 55 and close to 50 percent are under 35. Press Release, comScore, Inc., Demographic Profile of Visitors to Select Social Networking Sites, *available at* <http://www.comscore.com/press/release.asp?press=1019>.

<sup>7</sup> Amanda Lenhart & Mary Madden, *Teens, Privacy & Online Social Networks: How Teens Manage their Online Identities and Personal Information in the Age of MySpace*, PEW INTERNET & AM. LIFE PROJECT, Apr. 18, 2007, at 20, *available at*

¶8

However, the hallmarks of digital information and the ease of informational exchange facilitated by this medium lead to more noxious privacy and personality harms than ever before. Privacy law has traditionally been criticized for not having “enough dead bodies.”<sup>8</sup> While this corporeal metaphor no longer applies, privacy harms are no longer short-lived and innocuous. The information’s digital permanence, searchability, replicability, transformability, and multitude of often unintended audiences make its effects more damaging than ever. Lacking the relative transience of human memory, the digital record has increased the stakes of privacy today, as Professor Larry Lessig has pointed out.<sup>9</sup> Moreover, technology allows individuals to troll for information to which they would otherwise never have had access and increases the risk that information may be seen and interpreted by multiple invisible audiences.<sup>10</sup> This invites readings divorced from the information’s original context and conclusions that may be erroneous, discriminatory, and often irrefutable. Further, it allows third parties to manipulate and further disseminate information or images without the editorial lens of professional ethics or individual accountability.

¶9

A person’s digital dossier can betray him in the physical world, resulting in harms like the denial or loss of employment,<sup>11</sup> shame and embarrassment, denigration of reputation, or merely exposure in an unwanted light. Harmful postings can be intentionally so, as with ex-lovers who vengefully post nude pictures or embarrassing information to harass their former flames,<sup>12</sup> or the many students who have sought to disgrace their teachers with false MySpace profiles defaming them as pedophiles or sexual deviants.<sup>13</sup> And they can also be unintentionally damaging, as with the many anecdotal cases in which the innocent posting of pictures of social activism,<sup>14</sup> risky behavior,<sup>15</sup> or controversial opinions<sup>16</sup> cause their subjects to lose a job, a new relationship, or a respectable reputation.

---

[http://www.pewinternet.org/pdfs/PIP\\_Teens\\_Privacy\\_SNS\\_Report\\_Final.pdf](http://www.pewinternet.org/pdfs/PIP_Teens_Privacy_SNS_Report_Final.pdf). Interestingly, most agree that while gossip about others is okay to share, personally identifying information about themselves, like their own personal medical information, is almost never okay to share.

<sup>8</sup> Ann Bartow, *A Feeling of Unease about Privacy Law: In Response to Daniel J. Solove, A Taxonomy of Privacy*, (2006), <http://www.pennumbra.com/issues/response.php?rid=3>.

<sup>9</sup> Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56 (1999).

<sup>10</sup> danah boyd, *Social Network Sites: Public, Private, or What?*, KNOWLEDGE TREE 13, May 2007, [http://kt.flexiblelearning.net.au/tkt2007/?page\\_id=28](http://kt.flexiblelearning.net.au/tkt2007/?page_id=28).

<sup>11</sup> See Donald C. Davis, *MySpace Isn’t Your Space* (The Berkeley Electronic Press, Working Paper No. 1943, 2007), <http://law.bepress.com/expresso/eps/1943> (calling for a fortification of employment law in the face of the widespread practice of passing judgment on potential job candidates based on OSN background checks).

<sup>12</sup> *Benz v. Washington Newspaper Publishing Co.*, 2007 WL 1794104 at \*1 (D.D.C. Sept. 29, 2006); see also Nussbaum, *supra* note 1, at 24.

<sup>13</sup> For example, in *J.S. v. Blue Mountain School District*, 2007 U.S. Dist LEXIS 23406, at \*1-2 (D. Pa. 2007), a fourteen-year-old created a false profile for his school principal on MySpace.com. The profile described him as a bisexual pedophile whose interests included “fucking in his office” and “hitting on students and their parents.” *Id.* at \*2.

<sup>14</sup> Diane Coudu, *HBR Case Study and Commentary: We Googled You*, HARV. BUS. REV., Jun. 2007, at 37 (discussing the effects of a hypothetical young woman’s social activism online on her future job prospects).

<sup>15</sup> Associated Press, *Captions, Not Photos, Trouble Miss New Jersey*, MSNBC, Jul. 11, 2007, available at <http://www.msnbc.msn.com/id/19620261/> (detailing a blackmail threat to Miss New Jersey that involved pictures taken from her private Facebook page).

<sup>16</sup> Michelle Kaufman & Sarah Rothschild, *Space Invasion*, MIAMI HERALD, Aug. 30, 2006, at D1 (reporting that reputation-wary college athletic departments have prohibited their athletes from engaging in OSN communications).

## III. THE DIGITAL PRIVACY DEBATE: NATIVES VERSUS IMMIGRANTS

¶10 Privacy expectations on OSNs seem to be overwhelmingly generation specific. As Professor John Palfrey put it, cyberspace can be divided between digital natives, those who grew up with the Internet, and digital immigrants, the older generation who have practically (but not always philosophically) immigrated to it.<sup>17</sup> This distinction frames the debate regarding the very existence of privacy online. Deconstructing each side's assumptions reveals their biases, their varying levels of dependence and reliance on the technology as safeguard, and ultimately, I argue, their fundamental conceptual differences regarding privacy.

¶11 The digital natives take advantage of their online existence and take MySpace's name to heart: for them, it really is about *their* personal *space* that is unmediated and free. Although accused of having a poorly developed sense of the risks inherent in the technology, digital natives, by virtue of being raised in an Internet-immersed culture, are extremely cyber-savvy. Although accused of reckless apathy when it comes to privacy, digital natives are wont to cry out when their privacy is breached.<sup>18</sup>

¶12 To appreciate their ethos, consider this physical space analogy: all automobile drivers know that they are in public when they drive on public streets. As such, in the absence of opaquely tinted windows, they do not have a reasonable expectation of privacy from other's glances or scrutiny while driving. Somewhat inexplicably, however, drivers often tend to do things that they otherwise wouldn't do in public, such as picking their teeth or their noses, belting out show tunes, or talking to themselves. This is because most of the time, while driving, drivers are not expecting to have a wide audience. It is possible that this figment of privacy is created by the automobile technology itself: the shell of metal and glass that encases them. Drivers' false sense of privacy can also be created by their perception of their minute place within the vastness of the hectic public sphere. They find privacy through the anonymity granted by the lack of attention (they imagine) is focused on them. Finally contributing to the drivers' sense of privacy is the inherent assumption that, even if the driver next door is staring at them, chances are very small that it is someone they know. In other words, *no one knows me, no one cares, and no one is focusing on me.*

¶13 Some of the time, however, drivers use their cars to express their personalities or garner attention from certain perceived audiences. They might try to look cool with one

---

<sup>17</sup> John G. Palfrey, Jr., *Commentary: We Googled You*, HARV. BUS. REV., June 2007, at page 5 (distinguishing digital natives from digital immigrants). I concede that this grouping inevitably results in generalizations, as there are certainly cyber-savvy octogenarians and teenagers who have never been online. However, for the purposes of this article, Professor Palfrey's clever distinction serves us well.

<sup>18</sup> The development and refinement of enhanced privacy technologies on OSNs has been driven in large part by consumers protesting privacy breaches. Facebook, for example, has responded to public outcries with changes to their privacy controls, features, and settings. For example, when Facebook introduced a new feature called "News Feed" and "MiniFeed," widespread anger and pervasive protest among its users prompted swift reactions and changes to the website's privacy functions. Originally designed to make it easier for friends to keep up to date with each other, these features had resulted in the bombardment of disclosure of trivially personal information such as the initiation of a new relationship or the posting of a new photo by a friend. Ultimately, the privacy controls were recoded and users were permitted to choose which types of personal stories became available to MiniFeed and News Feeds. *See, e.g.,* John Leyden, *Users Protest Over 'Creepy' Facebook Privacy Update*, THE REGISTER (U.K.), Sept. 7, 2006, available at [http://www.theregister.co.uk/2006/09/07/facebook\\_update\\_controversy](http://www.theregister.co.uk/2006/09/07/facebook_update_controversy).

hand on the wheel and music blaring as they cruise in front of their peers on a Saturday night or drive fast to showcase their automobiles' capabilities. This is behavior in which they wouldn't necessarily engage in the presence of a police officer, their mother, or employer. They might also display religious, academic, national, social, or political affiliations on their bumper stickers (as in "*My child is an Honor Student at XYZ Elementary*") or decorate their cars with words, neon lights, stickers identifying the composition of their families, or even memorials to the deceased. These expressions of individual identity, although publicly visible, may not necessarily be for everyone's eyes. Of course, the parents of the honor student wouldn't want to divulge that information to a pedophile or a stalker, who can easily conclude the child's whereabouts.

¶14 Like automobile drivers, digital natives' complex expectations of privacy on OSNs rest on a combination of technology, the anonymity of the multitude, and assumptions about the presence of their unintended audiences. While young digitals know on some level that their online behavior is ultimately subject to the unforgiving scrutiny of the Internet, they demand the right to exercise their situational personalities and still be shielded from unintended audiences. Theirs is a conception of privacy rooted in their perceived entitlement of selective *anonymity*.

¶15 Digital immigrants, on the other hand, grew up in a world where they had the luxury of control over their information. Their era gave them the opportunity to successfully rewrite their personal histories through legal and social mechanisms: criminal records could be expunged, foolish marriages could be annulled, shameful teenage pregnancies could be covered up by "moving away," and all was forgotten. In their youth, newspapers yellowed and memories failed, leaving only the person's word as evidence (i.e., the laughably exonerating, "*I smoked marijuana but never inhaled*"<sup>19</sup>).

¶16 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.<sup>20</sup>

¶17 Disturbingly for the digital immigrants, the digital medium has eviscerated an individual's control over her personal information. This is true whether the person self-posted on an OSN, made a purchase with a credit card, or was surreptitiously photographed with a camera phone while walking on a public street and exposed on a video sharing site. While the control argument has some merit when applied to those who do not protect their personal information — either by password or by the OSN security features — it fails when applied to the many others who are the reluctant subjects of online discussions and photographs. This argument assumes that the victim of

---

<sup>19</sup> During the 1992 presidential campaign, Bill Clinton was quoted as saying: "But when I was in England I experimented with marijuana a time or two, and I didn't like it. I didn't inhale it, and never tried it again." Gwenn Ifill, *The 1992 Campaign: New York; Clinton Admits Experimenting With Marijuana in 1960's*, N.Y. TIMES, March 30, 1992, available at <http://query.nytimes.com/gst/fullpage.html?res=9E0CE0DF1F38F933A05750C0A964958260>.

<sup>20</sup> Charles Fried, *Privacy*, 77 YALE L. J. 475, 482 (1968) ("[Privacy] is the *control* we have over information about ourselves."); Alan F. Westin, *PRIVACY AND FREEDOM* 7 (1967) ("Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others.").

a personality or privacy breach has full control over what is posted of her and that she was the original discloser of the information. This assumption is simply not valid in world where ubiquitous tiny cameras can easily capture and widely disseminate images without consent or bloggers can unilaterally defame individuals without opportunity for rebuttal or editorial restraint.

¶18 Unfortunately for the digital natives, so too has the digital medium erased the possibility of anonymity and concealment from unintended audiences. While both sides are fundamentally mistaken in their assumptions, it is possible, however, that digital natives are ahead of the curve in recognizing that the Internet is more likely to grant them selective anonymity than control over their information. This notion informs anonymity as the foundation of their conception of privacy. Unfortunately, the privacy law, technology, and ethics have not caught up to the harms they purportedly protect and redress.

#### IV. THE LAW AS DIGITAL IMMIGRANT

¶19 The digital immigrant formulation of privacy as control has pervaded the development (or lack thereof) of the law and technology that protects online socializers from privacy and personality harms. It is rooted in a simplistic notion of privacy as *control* over personal information and the mistaken assumption that such control is possible on- or off-line. This ill-fitting and impossible conception of privacy places the burden of “remaining private” squarely on the individual, who is ultimately without recourse from existing law or technology (as personified by its creators and disseminators, the Internet Service Providers (ISPs)) in the event they are harmed.

##### A. *Tort Law Provides Limited Recourse to the Shamed*

¶20 In tort law and beyond, the notion of “privacy as control” is reflected in a focus on assumption of risk. In other words, those who have exposed themselves to the public eye cannot claim a reasonable expectation of privacy in their exposure. Categorically, everyone would agree that those who carelessly post shameful pictures of themselves or incriminating information on profiles that are accessible to everyone on the Internet cannot reasonably claim privacy in their posting.<sup>21</sup> Regardless of what the moral panic’s fomenters may fear, this is likely a very small percentage of OSN participants.

¶21 For those who did not affirmatively seek publicity or even tried assiduously to avoid it by staying offline, tort law provides limited atonement for cybershame. In fact, causes of action that primarily protect one’s reputation, dignity, or privacy — such as defamation, privacy torts, and intentional infliction of emotional distress — have traditionally been both anemic and anomalous, due in part to the lack of tangible or gaugeable harm of the dignitary injuries they address.<sup>22</sup> The following actions are often

---

<sup>21</sup> A recent Ohio child custody case exemplifies this point. In *Dexter v. Dexter*, the mother seeking custody of her child had detailed her drug usage and incriminating innermost thoughts on her MySpace profile, including statements that she was “on a hiatus from using illicit drugs during the pendency of [the child custody] proceedings, but that she planned on using drugs in the future.” 2007 Ohio 2568, P32-33 (Ohio Ct. App. 2007). The court wisely concluded that she could “hardly claim an expectation of privacy regarding these writings.” *Id.* at n.4.

<sup>22</sup> See *Lynch v. Knight*, 9 H.L.C. 577, 598, 11 Eng. Rep. 854 (1861) (famously noting that “mental pain

stymied after a balancing the aggrieved's evanescent humiliation with the actor's formidable First Amendment rights.<sup>23</sup>

¶22 The torts of defamation — libel and slander — do not apply if the information published was true or opinion, however harrowing.<sup>24</sup> Thus, if the disclosure is true but nonetheless embarrassing or meant for other audiences, these dignitary torts are inapplicable. Moreover, their prosecution is wrought with serious practical hurdles: the actor's anonymity could make it difficult to find a defendant, the aggrieved parties must bring suit against the actual publisher of the information, not the ISP,<sup>25</sup> and bringing suit could bring more negative and unwanted publicity than remuneration. For example, one recently publicized case involved a lawyer, a scorned ex-girlfriend, and a website called dontdatehimgirl.com, which invites women to “dish dirt” on ex-lovers in a social networking context. Prompted by the site's vengeful mission, the ex-girlfriend publicly posted that the attorney had cheated on her and was infected with a venereal disease.<sup>26</sup> The lawyer then sued the elusive woman. While the future of this case remains uncertain,<sup>27</sup> a trial surely will submit the plaintiff to further embarrassment since he will have to prove that he was somehow faithful and healthy. Regardless of legal redress, veracity, or the aggrieved's opportunity to refute, the harm to his reputation is likely to be indelible.

¶23 What if, however, it was true that the dontdatehimgirl.com plaintiff had a sexually transmitted disease? What if an embarrassing moment was surreptitiously captured on video and publicly posted by someone other than its subject on a video-sharing site such as YouTube.com?

¶24 Prosser's four-fold privacy torts — intrusion upon seclusion, public disclosure of private facts, false light privacy, and appropriation<sup>28</sup> — are similarly fragile in the face of such disclosures. The tort of intrusion upon seclusion addresses harmful information-gathering, but not the subsequent disclosure of its fruits.<sup>29</sup> It would only apply if the information was uncovered in a furtive way from a place within which the plaintiff had a reasonable expectation of privacy, such as a home,<sup>30</sup> hotel room,<sup>31</sup> a tanning booth,<sup>32</sup> or a

---

or anxiety the law cannot value”).

<sup>23</sup> Florida Star v. B.J.F., 491 U.S. 524, 550 (1989).

<sup>24</sup> RESTATEMENT (SECOND) OF TORTS § 613 cmt. j (1977).

<sup>25</sup> See *infra* note 51 and discussion of the Communications Decency Act.

<sup>26</sup> *Man Fights Back After Appearing on Dontdatehimgirl.com: Local Man Says Entries Are False*, WPXI.COM, June 8, 2006, <http://www.wpxi.com/news/9343498/detail.html>; Laura Parker, *Court Says Blogs Not Liable for 3rd Parties Calif. Ruling also Covers Site Owners*, USA Today, Nov. 22, 2006; *Lawsuits Aim at Libelous Bloggers*, DAILY RECORD (St. Louis), Oct. 28, 2006.

<sup>27</sup> Hollis v. Joseph, No. GD06-12677 (Pa. C.P. Alleghany, Apr. 5, 2007). The attorney, Todd Hollis, also sued the Florida-based website itself for soliciting the negative comments. This lawsuit was dismissed by the Pennsylvania court on jurisdictional grounds. Joe Mandak, *Judge Tosses Date Dissing Web Suit*, MSNBC, Apr. 11, 2007, available at <http://today.msnbc.msn.com/id/18044225>.

<sup>28</sup> See William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383 (1960).

<sup>29</sup> Intrusion upon seclusion requires the plaintiff to show that the defendant (a) intentionally intruded, physically or otherwise, (b) on the solitude or seclusion of another or on his private affairs or concerns, (c) in a manner highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

<sup>30</sup> Dietmann v. Time, Inc., 284 F. Supp. 925 (C.D. Cal. 1968); Welsh v. Pritchard, 241 P.2d 816 (Mont. 1952).

<sup>31</sup> Newcomb Hotel Co. v. Corbett, 27 Ga. App. 365 (1921).

<sup>32</sup> Sabrina W. v. Willman, 540 N.W.2d 364 (Neb. Ct. App., 1995) (noting that the “tanning room in the hair salon had a door which locked from the inside” in concluding that defendant intruded upon the seclusion of plaintiff when he secretly watched and photographed her in various stages of undress and

shopping bag.<sup>33</sup> The tort also clearly encompasses the activities of high tech Peeping Toms, as it covers “unwarranted sensory intrusions like eavesdropping, wiretapping, and visual or photographic spying.”<sup>34</sup> However, if the reluctantly photographed and “YouTube-ed” was not in seclusion, but rather in front of a classroom full of students<sup>35</sup> or a city street,<sup>36</sup> no court would hold that he had a reasonable expectation of privacy — regardless of his own expectation of “audience.”<sup>37</sup>

¶25 The tort of public disclosure of private facts similarly rejects the notion of a “reasonable expectation of audience.” The tort provides redress for the unwarranted publication of truthful but non-newsworthy, private, and offensive facts.<sup>38</sup> However, courts often take the stringent stance that once information has been disclosed or exposed by its subject, it is no longer legally protectable as private. Some courts have disqualified the privacy of information that had been disclosed to one other person or to individuals within the aggrieved’s intimate circle<sup>39</sup> and courts have uniformly held that there is no reasonable expectation of privacy in public places.<sup>40</sup> In today’s legal and technological world, telling one can literally mean telling the world.

¶26 The tort of false light privacy, a first cousin of defamation that focuses on protecting the plaintiff’s peace of mind rather than reputation, requires the injurious publication to have been published with knowledge of its falsity in addition to being false or misleading and highly offensive in nature.<sup>41</sup> As with the other privacy torts, an action for false light privacy must involve matters that are inherently private. As such, any matter that has been divulged to others or is visible from a public place is not actionable, no matter how offensive its repercussions.<sup>42</sup>

¶27 Appropriation, the last of the four traditional privacy torts, is uniquely property-focused and does not involve a false statement or a shameful disclosure. Instead, the tort focuses on the unpermitted commercial use of a person’s identity and its ensuing

---

nude).

<sup>33</sup> Sutherland v. Kroger Co., 110 S.E.2d 716 (1959).

<sup>34</sup> RESTATEMENT (SECOND) OF TORTS, § 652B com. b, illust. 1-5 (1977).

<sup>35</sup> Requa v. Kent School District, 2007 U.S. Dist. LEXIS 40920 (D. Wash. 2007).

<sup>36</sup> Arrington v. New York Times Co., 55 N.Y.2d 433; 434 N.E.2d 1319; 449 N.Y.S.2d 941; 1982 N.Y. LEXIS 3203; 8 Media L. Rep. 1351 (N.Y. Court of Appeals 1982) (holding no reasonable expectation of privacy when a man was photographed on a city street and featured on the cover of the New York Times Magazine).

<sup>37</sup> *But c.f.*, M.G. v. Time Warner, Inc, 107 Cal. Rptr. 2d 504, 511-12 (2001) (finding that Little League players and coaches had a privacy claim against Time Warner after HBO showed the team’s group photo in a story about the team manager’s molestation of several pictured team members).

<sup>38</sup> According to the Restatement, the disclosure tort requires the plaintiff to show that the defendant (a) gave publicity, (b) to a private fact, (c) that is not of legitimate concern to the public, where such disclosure (d) is highly offensive to a reasonable person. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

<sup>39</sup> Sipple v. Chronicle Publ’g Co., 201 Cal. Rptr. 665 (1984) (holding that the fact that the plaintiff had confided to a group of people that he was homosexual vitiated the matter’s privacy).

<sup>40</sup> According to the Restatement, “the plaintiff cannot normally complain when his or her photograph is taken while he or she is walking down the public street and is published in the defendant’s newspaper. Nor is the plaintiff’s privacy invaded when the defendant gives publicity to a business or activity in which the plaintiff is engaged in dealing with the public.” RESTATEMENT (SECOND) OF TORTS § 652D cmt. b (1977).

<sup>41</sup> W. Page Keeton et al., PROSSER AND KEETON ON THE LAW OF TORTS § 117, at 863-868 (5th ed. 1984).

<sup>42</sup> See Cefalu v. Globe Newspaper Co., 391 N.E.2d 935 (Mass. App. Ct. 1979) (denying the false light claim of a person who was photographed in line outside of an unemployment office, resulting in the implication that he was unemployed, regardless of the fact that he was only there as a translator). See also Floyd v. Park Cities People, Inc. 685 S.W.2d 96 (Tex. App. 1985) (holding that plaintiff did not have a reasonable expectation of privacy while standing on his front porch).

dignitary harms.<sup>43</sup> Hence it would only apply if the plaintiff's information or image were used without his consent for the defendant's commercial purposes. For example, Facebook has recently launched a platform called Social Ads that allows advertisers to use pictures of Facebook members in advertisements without their prior consent.<sup>44</sup> While the tort of appropriation has not been tested in the OSN context, it seems likely that it would be applicable in this recent case.

¶28 Finally, intentional infliction of emotional distress is ineffectual. According to the Restatement, "one who by extreme and outrageous conduct intentionally or recklessly causes severe emotional distress" will be liable for its emotional or physical manifestations.<sup>45</sup> This has traditionally been a parasitic tort with more academic hullabaloo than real-world success. Most courts have held that actionable conduct must exceed all reasonable and socially-tolerable bounds of decency. This has set a high bar for the tort. Actionable conduct should "arouse resentment against the actor"<sup>46</sup> on the part of a civilized and decent community member and further "lead him to exclaim, 'Outrageous!'"<sup>47</sup> In an online environment where individuals voluntarily release sex tapes to promote their careers<sup>48</sup> or "fart their way into the spotlight"<sup>49</sup> for a chance at fleeting cyber-stardom, one may be hard pressed to find "outrageous!" conduct, much less define "community member." Moreover, many courts have held that physical manifestations of the emotional distress are necessary, thus further diluting the disgrace-focused tort.<sup>50</sup>

¶29 Interestingly, intellectual property law might be the only effective legal mechanism to stop further dissemination of embarrassing images online. In the event that the individual who posted an incriminating or shameful photograph or video is not its owner, the owner can send a takedown notice to the ISP pursuant to the Digital Millennium Copyright Act.<sup>51</sup>

#### B. *The ISPs and the Technology Provide Limited Recourse to the Shamed*

¶30 In the absence of robust law protecting against reputational injury, there is a void in preventative measures and dispute resolution mechanisms for these matters. The OSNs themselves shun the role of judge and jury in relational disputes. In fact, they too have adopted the premise of privacy as *control*, thereby focusing responsibility for these privacy and personality harms on the OSN participants. For example, one of Facebook's core privacy principles states, "you should have control over your personal

---

<sup>43</sup> J. THOMAS MCCARTHY, *THE RIGHTS OF PUBLICITY AND PRIVACY* § 5:61 (2d ed. 2007).

<sup>44</sup> Kenneth Corbin, *Facebook Ads: An Illegal Revolution?*, INTERNET NEWS, Nov. 12, 2007, available at <http://www.internetnews.com/bus-news/article.php/3710341>.

<sup>45</sup> RESTATEMENT (SECOND) OF TORTS § 46(1) (1965).

<sup>46</sup> *Id.* cmt. d.

<sup>47</sup> *Id.*

<sup>48</sup> Lola Ogunnaike, *Sex, Lawsuits, and Celebrities Caught on Tape*, N.Y. TIMES, Mar. 19, 2006, available at <http://www.nytimes.com/2006/03/19/fashion/sundaystyles/19tapes.html> (noting that "gone are the days when a sex tape - which might seem the most embarrassing of disclosures - automatically destroys a celebrity's career.").

<sup>49</sup> Nussbaum, *supra* note 1.

<sup>50</sup> KEETON ET AL., *supra* note 39, §12, at 64.

<sup>51</sup> 17 U.S.C. § 512(c)(3) (1999).

information.”<sup>52</sup> As mentioned above, this conceptualization of privacy is based on a sense of control that is not consistent with the transferability and malleability of the digital form.

¶31 The ISP’s lack of involvement stems from strong public policy favoring ISP immunity for third party postings. In the interest of maintaining the free flow of discourse without fear of liability, section 230 of the Communications Decency Act of 1996 insulates ISPs such as OSNs<sup>53</sup> from liability for any tortious postings by a third-party user or any harm flowing from the dissemination of that content.<sup>54</sup> Regardless of this legislative grant of immunity, OSN’s terms and conditions generally contain clauses prohibiting the submission of material that is, among other things, defamatory or libelous or contravening an individual’s privacy and publicity rights.<sup>55</sup> On the other hand, the same terms and conditions include seemingly contradictory releases from liability for “inaccurate, offensive, indecent, or objectionable” postings.<sup>56</sup>

¶32 While some OSNs might accede to take down material that is clearly offensive (however that may be defined), in the interest of the First Amendment and maintaining their own impartial role, OSNs will generally not take down material that is merely embarrassing, purportedly defamatory, or shameful to its subject. Resultantly, retribution for online personality harms has almost solely taken the form of “tit-for-tat” disparagement. In one case, a young woman’s ex-boyfriend maliciously posted a clip of the two having sex that included all of her contact information. In a modern-day twist on Nathaniel Hawthorne’s *Scarlet Letter*, she resorted to creating a MySpace group advocating “chemically castrating” her ex-boyfriend and posted a picture of him with the word “loser” stamped across his forehead in bold red letters.<sup>57</sup> This wild-west style vigilantism can escalate quickly and be overly harassing or defamatory. In essence, anyone can post “their side” of a story without a bona fide verification process. This digital “he said-she said” inevitably fails to exonerate but nevertheless remains as part of its participants’ digital identities.

---

<sup>52</sup> Facebook Principles, <http://www.facebook.com/policy.php> (last visited Aug. 20, 2007) (The Principles go on to state: “We understand you may not want everyone in the world to have the information you share on Facebook; that is why we give you control of your information.”).

<sup>53</sup> Courts have affirmed the applicability of the law to OSNs like MySpace. *See, e.g., Doe v. MySpace, Inc.*, 474 F.Supp. 2d 843 (W.D. Tex. 2007) (dismissing an action against MySpace for harms arising from a minor’s sexual assault by a fellow MySpace member).

<sup>54</sup> 47 U.S.C. §§ 230(c)(1), (e)(3) (2006) (The Communications Decency Act states that “[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider,” and expressly preempts any state law to the contrary.); *Almeida v. Amazon.com, Inc.*, 456 F.3d 1316, 1321 (11th Cir. 2006) (“The majority of federal circuits have interpreted the CDA to establish broad ‘federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service.’” (quoting *Zeran v. America Online, Inc.*, 129 F.3d 327, 330 (4th Cir. 1997))); *see also Carafano v. Metrosplash.com, Inc.*, 339 F.3d 1119, 1122 (9th Cir. 2003) (citing *Batzel v. Smith*, 333 F.3d 1018, 1026-27 (9th Cir. 2003)).

<sup>55</sup> *See, e.g., MySpace Terms & Conditions*, § 6(2), 8, 9, <http://www.myspace.com/index.cfm?fuseaction=misc.terms> (last visited on Nov. 14, 2007); *YouTube Terms and Conditions* § 5.C, <http://www.youtube.com/t/terms> (last visited Aug. 12, 2007).

<sup>56</sup> *MySpace Terms & Conditions*, § 5.G, <http://www.myspace.com/index.cfm?fuseaction=misc.terms> (last visited on Nov. 14, 2007).

<sup>57</sup> Nussbaum, *supra* note 1.

## V. ARGUMENT: WHY WE SHOULD PROTECT PRIVACY AND PERSONALITY ON OSNs

¶33 I have defined the digital natives' conception of privacy as anchored in anonymity, while the digital immigrants' is based in control. In truth, the digital form allows for neither complete anonymity nor control. Regardless, the law, propounded and applied by digital immigrants, is firmly rooted in privacy as control, a notion that is no longer applicable and affords inadequate protection and adjudication to modern harms. As such, we must reformulate and refocus the privacy debate, cutting through the thicket of moral panic and finger-pointing, to justify the protection of privacy on OSNs.

¶34 To that end, the following are four compelling arguments militating for the protection of privacy and personality on OSNs and beyond. Each carefully balances social welfare, public policy, and the realities of contemporary social networking technology.

### A. Identity

¶35 Many digital immigrants perceive the OSN phenomenon as pathologically narcissistic and voyeuristic — yet another piece of evidence pointing to the obsessive self-importance of the Millennials, also known as Generation Me,<sup>58</sup> the Net Generation,<sup>59</sup> and the MySpace Generation,<sup>60</sup> who foolishly trade away their privacy to “broadcast themselves” for the chance at unmerited celebrity.

¶36 However, social networking profiles serve an important identity-building function: they are personal billboards representing one's managed, researched, and well-crafted identity. One reason for their success lies in their ability to allow the participant to easily mold identity and manage the way their world perceives them. Profiles allow OSN participants to try on masks and test them among the focus group of their peers, a practice critical to socialization in teenagers and young adults.

¶37 By divorcing the social world from physical space, they allow for communication without judgment based on appearance. The OSN participant uploads a picture that represents his face in cyberspace — this may be anything from a flattering picture of himself to a picture of Superman — and thereby communicates with others. This levels the playing field as identity is not judged in physical space terms of physical appearance, race, class, or body size — but in terms of interests, dialogue, and design.

¶38 As noted OSN commentator danah boyd has remarked, with the dearth of unmediated physical spaces available to today's youth (like the drive-in or the mall), OSNs provide a unique and valuable forum for identity creation and exploration. Affording privacy to these activities protects their crucial developmental purpose.<sup>61</sup>

---

<sup>58</sup> JEAN M. TWENGE, *GENERATION ME: WHY TODAY'S YOUNG AMERICANS ARE MORE CONFIDENT, ASSERTIVE, ENTITLED — AND MORE MISERABLE THAN EVER BEFORE* (2006).

<sup>59</sup> DON TAPSCOTT, *GROWING UP DIGITAL: THE RISE OF THE NET GENERATION* (1998) (predicting the future influence of the Net Generation, or N-Gen, in their unique position as the first generation to be immersed in the digital revolution from birth).

<sup>60</sup> Jessi Hempel with Paula Lehman, *The MySpace Generation*, *BUSINESSWEEK*, Dec. 12, 2005, available at [http://www.businessweek.com/magazine/content/05\\_50/b3963001.htm](http://www.businessweek.com/magazine/content/05_50/b3963001.htm).

<sup>61</sup> 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>.

### B. Dignity

¶39 While, generally-speaking, the adult personality is not in such constant flux, it nevertheless warrants similar privacy protection. Individuals assume different personae in social life that are often fundamentally incompatible with one another and often defined by time and space.<sup>62</sup> In other words, people do not dress, behave, engage in the same conversations using the same words or language, or generally present themselves as the same “person” with everyone they know. In a now-famous episode of the television show, *Seinfeld*, Jerry’s perpetual sidekick George Costanza posited the “Worlds Collide” theory, prompted by concern that his new girlfriend was infiltrating his group of friends. He ominously warned:

I have ‘Relationship George’ but there is also ‘Independent George’ . . . that is the George you know, the George you grew up with — that’s movie George, coffee shop George, liar George, bawdy George... if ‘Relationship George’ walks through this door, he will kill ‘Independent George’! A George divided against himself cannot stand!<sup>63</sup>

¶40 Behavioral science has long recognized that individuals need privacy to shield their multiple personalities from one another and “to explore different identities and develop a sense of autonomy.”<sup>64</sup> As one noted behavioral anthropologist has commented,

The fact that so few businessmen have offices in their homes cannot be solely explained on the basis of convention and top management’s uneasiness when executives are not visibly present. I have observed that many men have two or more distinct personalities, one for business and one for the home. The separation of office and home in these instances helps to keep the two often incompatible personalities from conflicting and may even serve to stabilize an idealized version of each which conforms to the projected image of both architecture and setting.<sup>65</sup>

¶41 As one U.S. court put it, privacy law should protect “an integral part of our humanity; one has a public persona, exposed and active, and a private persona, guarded and preserved. The heart of our liberty is choosing which parts of our lives shall become public and which parts we shall hold close.”<sup>66</sup> Consistent with this court’s dicta, scholars have noted that American society and jurisprudence places great importance on privacy as liberty while European societies tend to value privacy more in the context of personal inter-social interaction.<sup>67</sup> Therefore, European societies recognize the “right to a private

---

<sup>62</sup> WALTER MISCHEL, *PERSONALITY AND ASSESSMENT* (1968) (concluding that a person’s behavior can more certainly be predicted from knowledge of the situation she is in rather than from her personality traits).

<sup>63</sup> *Seinfeld: The Pool Guy* (NBC television broadcast Nov. 16, 1995).

<sup>64</sup> Dan Gibbard, *Social Sites Can Aid Parents; Kids May Vventlssues Online*, CHI. TRIB., Mar. 14, 2007, at Metro 1 (quoting Justine Cassell, director of the center for Technology & Social Behavior at Northwestern University).

<sup>65</sup> EDWARD T. HALL, *THE HIDDEN DIMENSION* 104-105 (Anchor Books 1990) (1966).

<sup>66</sup> *Lake v. Wal-Mart Stores, Inc.*, 582 N.W.2d 231, 235 (Minn. 1998).

<sup>67</sup> See, e.g., Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161-1162 (2004);

life” as a fundamental matter of human dignity<sup>68</sup> and are perhaps more apt to recognize situational personalities as healthy facets of human interaction that deserve privacy protection. In the U.S., however, the sustainability of situational personalities is threatened by the loss of privacy on OSNs and the void in adjudication and recourses to the unwitting victims of cybershame. Law and technology should recognize the importance of privacy in situational personalities on OSNs.

### C. Intimacy and Socialization

¶42 As the digital immigrants would say, there is no doubt that the most effective way of controlling information about oneself is to keep it to oneself. If you don’t want to run the risk of being wiretapped, don’t use the telephone. Don’t want to run the significant risk of bodily injury? Don’t travel by automobile. Don’t want your face PhotoShop’d onto a pornographic image? Don’t allow your picture to be taken. While these arguments are certainly logical and prudent, when the technology becomes ubiquitous and central to the way society functions, these admonitions cease to be reasonable. At their extreme, they are also both socially and psychologically undesirable.

¶43 As many behavioral scientists and some legal theorists have noted, the voluntary disclosure of personal information and gossip about others are sources of intimacy and lead to healthy interpersonal relations.<sup>69</sup> Intimacy enhances social welfare and promotes psychological and relational benefits like solace, kinship, and counsel. Eminent privacy theorists have argued that without legal privacy protection, intimacy would not flourish or exist.<sup>70</sup> For example, Professor Charles Fried theorizes that the act of sharing intimate information functions as a relationship-building commodity:

To be friends or lovers persons must be intimate to some degree with each other. Intimacy is the sharing of information about one’s actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love.<sup>71</sup>

By fomenting strong interpersonal ties, privacy enhances intimacy and strengthens community.

---

Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU, and Canada: The Allure of the Middle Ground*, 2 U. OTTAWA L. & TECH. J. 357 (2005).

<sup>68</sup> Avner Levin, *Two Notions of Online Privacy: Facebook and Personal Information Protection* (working paper, on file with author).

<sup>69</sup> CHARLES FRIED, AN ANATOMY OF VALUES: PROBLEMS OF PERSONAL AND SOCIAL CHOICE 142 (1970); Thomas E. Runge & Richard L. Archer, *Reactions to the Disclosure of Public and Private Self-Information*, 44 SOC. PSYCHOL. Q. 357, 361 (1981) (discussing experimental findings in which subjects claim to like their stranger-partner more if the stranger-partner shares information that she claims she has not previously revealed).

<sup>70</sup> Robert S. Gerstein, *Intimacy and Privacy*, PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 265, 265 (Ferdinand David Schoeman ed., 1984). See also CARL D. SCHNEIDER, SHAME, EXPOSURE, AND PRIVACY 42 (1977) (“In the area of personal relationships, such as family, friends, and lovers where quality is important, privacy is an operative principle. These relationships can’t be sustained with everyone. To function, they depend on an excluding condition. Privacy creates the moral capital that is spent in friendship and intimate relations.”).

<sup>71</sup> FRIED, *supra* note 69.

¶44 Such disclosure is the lifeblood of OSNs. The immense success of OSNs has stemmed from their ability to simulate real-life social interaction, allow old friends to keep in touch, and thereby recreate intimacy and community online. This success and laudable goal would be undermined if some degree of privacy were not protected on OSNs.

#### D. Discourse

¶45 The more people hear stories of others getting “busted” on OSNs, the less likely they will be to share their stories and opinions, and thus continue to develop OSNs as a platform for communication and meaningful social interaction. OSNs are the latest wave of Internet technologies to successfully bring people of similar interests together with few or no transaction costs. This has led to the swelling of political and social activism on OSNs among an age demographic that has traditionally been criticized for its apathy.<sup>72</sup> Even presidential candidates have swarmed to OSNs to rally support among the wired generation.<sup>73</sup> Many political and social groups’ successes at bringing people together could only have been made possible with the networking power of OSNs. To some, this begs a troubling question: what happens to political and social discourse and activism when it is engraved in the indelible memory of the digital form? What happens to our freedom of association?

¶46 Recording something in electronic form facilitates monitoring without the transience of human memory.<sup>74</sup> Present or future voyeurs can easily attain a detailed, often first-hand account of personal facts that occurred years before. Digital dossiers may serve to ensure that people are perpetually tagged and identified by activities in which they engaged years ago. We can no longer erase or ignore our pasts.

¶47 Such surveillance changes behavior. Awareness of monitoring can make a person feel extremely uncomfortable and ultimately lead to self-censorship, inhibition, and a chilling of discourse. As Justice Douglas observed, “monitoring, if prevalent, certainly kills free discourse and spontaneous utterances.”<sup>75</sup> Although the rapidly rising number of profiles and seeming ubiquity of OSNs does not appear to indicate that this chilling effect has taken place, several recent cases — both in the courts and in folklore — have tested the boundaries of speech on OSNs and have served as a warning that such speech can have physical space consequences.<sup>76</sup> University administrators reportedly troll OSNs when investigating illegal activities on campuses. Employers are notoriously looking at OSNs for quick and easy background checks on prospective employees that may constitute a basis for discriminating against them due to their past activities or political views.<sup>77</sup> Some are using OSN postings to publicly shame others’ political views and

---

<sup>72</sup> A MySpace group called “dollarsfordarfur,” recently founded by two high school students, raised both awareness and significant funds for the humanitarian crisis in Darfur. *See* dollarsfordarfur, <http://www.myspace.com/dollarsfordarfur> (last visited Oct. 26, 2007).

<sup>73</sup> *See* Alex Williams, *The Future President, On Your Friends List*, N.Y. TIMES, Mar. 18, 2007, available at <http://nytimes.com/2007/03/18/fashion/18myspace.html>.

<sup>74</sup> *See* Lessig, *supra* note 9.

<sup>75</sup> *U.S. v. White*, 401 U.S. 745, 762 (1971) (Douglas, J., dissenting).

<sup>76</sup> *See, e.g., J.S. v. Blue Mountain School District*, 2007 U.S. Dist. LEXIS 23406 (M.D. Pa. Mar. 29, 2007); *Requa v. Kent School District No. 415*, 492 F. Supp 2d 1272 (W.D. Wash. 2007).

<sup>77</sup> *Davis, supra* note 11; *Coutu, supra* note 14.

opinions or to judge them based on their OSN associations, networks, and friends.<sup>78</sup> Reports abound of organizations acting swiftly to hush criticism of them on OSNs.<sup>79</sup> In order to allow for free association and exchange of ideas, OSN members must maintain the ability to disclose or opine without fear of mass disclosure or retaliation.

## VI. CONCLUSION

¶48 While reputational harms are more tangible and indelible than ever before, there is a dearth of support for the aggrieved. Our current law is ill-equipped to protect these injuries, ISPs are unwilling to mediate them, codes of ethics are scant, and technology is still too fragile to protect them. For digital immigrants, this lack of protection and redress is justified, after all, online, “you have zero privacy — get over it.”<sup>80</sup> While a prudent personal admonition, it is too simplistic and cynical to inform the law, public policy, ethics, or the future of technology.

¶49 In order to analyze the shortcomings in this area, it is necessary to sidestep the cyber-immigration debate and understand the personal, relational, and social benefits of protecting privacy and personality on OSNs and beyond. Individuals need privacy to develop and sustain personality, strengthen interpersonal relationships, voice and test opinions, become producers of culture, and, ultimately, be free.

¶50 The burden of protecting privacy on OSNs should not be solely borne by the OSN participants, rather it should be shared by the individuals, law, ethics, ISPs, and technology. Individuals should be cognizant of the reality of digital information and prudent in their selections of ISPs, privacy controls, and self-disclosure without assuming entitlement to selective anonymity. The law must also be updated to address modern harms, perhaps by incorporating a reasonable expectation of audience standard or a uniform code of privacy for adoption by state legislatures. Codes of ethics addressing dignitary harms on OSNs should be promulgated, perhaps encouraging employers to disclose the sources of an employee’s background check and allow opportunity to refute any questionable online information.

¶51 Finally, ISPs, who are perhaps the best situated actors to carry some of these burdens, should proactively educate their users as to the risks inherent in online disclosure, incorporate a code of online ethics to which participants can subscribe, and perhaps offer an active adjudication system for member privacy disputes. ISPs can also tailor the technology to protect situational personalities, perhaps allowing the online socializer to zone his personality as he can in real space. Protecting privacy and personality on OSNs from various angles and by several actors would ensure that the

---

<sup>78</sup> See Wikipedia Facebook entry, <http://en.wikipedia.org/wiki/Facebook> (last visited Oct. 26, 2007) (listing reported incidents).

<sup>79</sup> See, e.g., Chris Williams, *University Moves to Hush Facebook Criticism*, THE REGISTER (U.K.), May 22, 2007, available at [http://www.theregister.co.uk/2007/05/22/keele\\_facebook](http://www.theregister.co.uk/2007/05/22/keele_facebook) (documenting the policies of English universities that have threatened students who criticize them online).

<sup>80</sup> Scott McNealy, CEO of Sun Microsystems, famously retorted this statement to a group of reporters and analysts at an event to launch his company’s Jini technology in January of 1999. See Polly Sprenger, *Sun on Privacy: ‘Get over it’*, WIRED, Jan. 26, 1999, available at <http://www.wired.com/politics/law/news/1999/01/17538>. He has since claimed that the “zinger” was misconstrued and oversimplified as a sound bite. Don Tennant, *Q&A: McNealy defends Sun reliability, personal privacy views*, COMPUTERWORLD, Nov. 27, 2001, available at <http://www.computerworld.com/hardwaretopics/hardware/story/0,10801,66102,00.html>.

technology evolves in ways that encourage identity-building, intimacy, and social discourse, yet simultaneously protect and respect its participants.