William Mitchell Law Review

Volume 38 | Issue 1 Article 7

2011

# Are "Private" Spaces on Social Networking Websites Truly Private? The Extension of Intrusion Upon Seclusion

Adam Pabarcus

# ARE "PRIVATE" SPACES ON SOCIAL NETWORKING WEBSITES TRULY PRIVATE? THE EXTENSION OF INTRUSION UPON SECLUSION

Adam Pabarcus†



† Judicial law clerk for the Honorable Jill Flaskamp Halbrooks, Minnesota Court of Appeals; B.A., University of Notre Dame, 2007; J.D., William Mitchell College of Law, 2011. Thanks to Daniel Kleinberger, Christina Kunz, Raleigh Levine, and Michael Steenson for their very helpful comments on earlier drafts.

"He who may intrude upon another at will is the master of the other and, in fact, intrusion is a primary weapon of the tyrant."[1]

## I. INTRODUCTION

### *A. The Case of Brian Pietrylo*

In 2006, Brian Pietrylo was a server at a Houston's restaurant operated by Hillstone Restaurant Group in Hackensack, New Jersey.[2] While working at Houston's, Pietrylo created a MySpace group called the "Spec-Tator."[3] In his initial posting, Pietrylo explained that Spec-Tator's purpose was to "vent about any BS we deal with out [sic] work without any outside eyes spying in on us. This group is entirely private, and can only be joined by invitation." He then proclaimed, "[L]et the s**t talking begin."[4]

Pietrylo invited past and current employees to join the group, including Karen St. Jean, a greeter, and Doreen Marino, a server.[5] Group members posted sexual remarks about Houston's management and customers, jokes about customer service and quality specifications, and references to violence and illegal drug use.[6] TiJean Rodriguez, a Houston's manager, had St. Jean to his home for dinner, and during the evening, St. Jean logged into her MySpace account and showed him the posts on Spec-Tator,[7] which Rodriguez subsequently reported to upper management.[8] St. Jean provided upper management with her username and password,[9]

1. Edward J. Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 974 (1964).
2. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *1 (D.N.J. July 24, 2008).
3. *Id.*
4. *Id.* at *1–2.
5. *Id.*
6. *Id.* at *3–4.
7. *Id.* at *2.
8. *Id.* at *2–3.
9. *Id.* St. Jean claims that even though upper management did not threaten her, she provided them access to her account only because she thought she "would have gotten in some sort of trouble." *Id.* at *3.

and after reading the posts, the regional supervisor fired Pietrylo and Marino because their posts were "offensive" and violated Houston's four core values: professionalism, positive mental attitude, aim-to-please approach, and teamwork.[10] Pietrylo and Marino filed a lawsuit claiming, *inter alia*, invasion of privacy because Hillstone intruded upon their seclusion.[11]

### *B. The Development of Privacy and the Restatement (Second) of Torts Section 652B Intrusion Upon Seclusion*

The common law torts of invasion of privacy and intrusion upon seclusion emerged from the advancement of technology. The advent of instantaneous photography and the invading presence of the newspapers into private affairs led Samuel Warren and Louis Brandeis to write their seminal article *The Right to Privacy* in 1890.[12] The basic right they sought to protect was the right to be let alone.[13] Seventy years later, William Prosser synthesized the common law right to privacy into four distinct torts: (1) intrusion upon seclusion; (2) appropriation; (3) publication of private facts; and (4) false light publicity.[14] The American Law Institute adopted Prosser's classification of the right to privacy in the Restatement (Second) of Torts sections 652A–E (1977),[15] and the vast majority of jurisdictions have specifically recognized section 652B, intrusion upon seclusion.[16]

Section 652B provides, "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person."[17] *Kuhn v. Account Control Technology* breaks the tort into three elements: "(1) an intentional intrusion (physical or otherwise); (2) on the solitude or seclusion of another; (3) that would be highly offensive to a reasonable person."[18] Traditionally,

10. *Id.* at *4.
11. *Id.* at *4–5, *18–19.
12. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890).
13. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 12–13, 162 (2008).
14. William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).
15. RESTATEMENT (SECOND) OF TORTS §§ 652A–E (1977).
16. *Id.* § 652B apps. (listing "court citations to Restatement, Second"). Forty-two states plus the District of Columbia have cited section 652B since 1977. *See id.*
17. *Id.* § 652B.
18. 865 F. Supp. 1443, 1448 (D. Nev. 1994) (quoting PETA v. Bobby Berosini, Ltd., 867 P.2d 1121, 1131 (Nev. 1994)).

intrusion upon seclusion has guarded against an intrusion of one's home or other *physical* area that protects an individual's personal matters, such as a hospital or hotel room.[19] The emergence of online social networking, however, raises the issue of whether a private *virtual* space can be incorporated into the common law's protection against intrusion.

This article begins by presenting the emergence of social networking websites and the appropriate approach to analyze actions on the Internet.[20] Next, this article argues that a private virtual space can satisfy the elements of section 652B.[21] This analysis examines the comments to the Restatement, the case law, and the underlying public policy for the elements of intrusion upon seclusion provided by the *Kuhn* framework by (1) examining what constitutes an intrusion;[22] (2) determining whether a virtual space can be "private" so as to establish an expectation of seclusion;[23] and (3) evaluating the proper standard by which to judge what is highly offensive to a reasonable person within the context of social networking websites.[24]

## II. SOCIAL NETWORKING WEBSITES AND PROBLEMS OF PERSPECTIVE

When approaching legal issues that involve the Internet, practitioners and scholars look for analogies between cyberspace and real space.[25] To make meaningful analogies in the intrusion upon seclusion analysis, the nature of social networking websites must first be understood. This section first explores the emergence of social networking websites to provide background on the privacy interests at stake; second, it provides an analytical structure for how to approach issues involving the Internet—whether the approach should be from the viewpoint of the Internet as a virtual reality or whether it should focus on how the Internet technically functions.

19. *See* SOLOVE, *supra* note 13, at 161–62 (referencing William Blackstone and the law's treatment of the home as one's castle); Prosser, *supra* note 14, at 389–90 (explaining that an intrusion upon one's home, a hospital room where a woman is giving birth, or a person's hotel room all constitute "intrusion").

20. *See infra* Part II.

21. *See infra* Part III.

22. *See infra* Part III.

23. *See infra* Part IV.

24. *See infra* Part V.

25. Orin S. Kerr, *The Problem of Perspective in Internet Law*, 91 GEO. L.J. 357, 361 (2003).

### *A. The Emergence of Social Networking Websites*

Social networking websites have grown exponentially in the last five years, with the two largest sites being Facebook and MySpace.[26] At the time of this writing, Facebook hosts more than 750 million active users worldwide, who collectively spend more than 700 billion minutes on Facebook each month and individually create, on average, 90 pieces of content each month.[27] MySpace, while losing ground to Facebook, is still the second largest social networking website with 63 million users.[28] Currently, to create a Facebook or MySpace account, a person needs a valid e-mail address and must certify that he or she is at least thirteen years old.[29] The person is then prompted to fill out a profile, which contains about forty pieces of personal information.[30] In Facebook, people can network with others by asking them to be their "friend." Once the person confirms the friendship request, they each have access to the other's profile information based on the privacy settings each has in place.[31] In addition, Facebook users can form

26. *See, e.g.*, Clint Boulton, *Facebook Passed Google, Yahoo, Microsoft in User Engagement*, EWEEK.COM (Feb. 9, 2011), http://www.eweek.com/c/a/Web-Services-Web-20-and-SOA/Facebook-Passed-Google-Yahoo-Microsoft-in-User-Engagement-384309/ ("Facebook bested Web giants Google, Yahoo and Microsoft in time spent online in the United States through 2010, with users spending 12.7 percent of their time at the social network Website."); Sampad Swain, *Statistics: Facebook Bypasses MySpace and Twitter Stronger than Ever*, SAMPAD'S BLOG (Feb. 10, 2009), http://sampadswain.com/2009/02/statistics-facebook-bypasses-myspace-and-twitter-stronger-than-ever/. Since 2009, LinkedIn and Twitter have become the third and fourth largest social networking websites, with 26.6 million visitors and 23.6 million visitors, respectively. Boulton, *supra*.

27. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Sept. 6, 2011).

28. Desire Athow, *10 Million Users Leave MySpace Within a Month*, ITPROPORTAL (Mar. 27, 2011), http://www.itproportal.com/2011/03/27/10-million-users-leave-myspace-within-month/. In 2007, MySpace had 185 million registered users with 4.5 million people on the site at any one time. Scott Elkin, *MySpace Statistics*, SCOTTELKIN (May 12, 2007), http://scottelkin.com/programming/aspnet-20/myspace-statistics/. However, Facebook has come to dominate the social networking landscape, as MySpace lost 10 million users between January and February 2011 alone. Athow, *supra*.

29. *Privacy Policy*, MYSPACE, http://www.myspace.com/Help/Privacy (last visited Sept. 13, 2011); *Statement of Rights and Responsibilities*, FACEBOOK, http://www.facebook.com/terms.php (last visited Sept. 13, 2011) [hereinafter *Facebook Terms*].

30. James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1149 (2009).

31. *Privacy Settings*, FACEBOOK, http://www.facebook.com/terms.php#!/settings/?tab=privacy (last visited Sept. 2, 2011) (permitting users to set their desired privacy level for different types of information, including the ability to "customize" certain information, which allows the exclusion of specific

groups with other "friends" where members of the group can share messages, pictures, and videos.[32]

The ubiquitous use of the Internet and the posting of personal information have created a "privacy paradox": users of social networking websites tend to disclose a high degree of personal information online, yet retain an expectation of privacy.[33] The strongest sense of intrusion is when people not understood to be part of a network gain access to the user's information and pictures.[34] To control access, both Facebook and MySpace permit users to set their desired privacy settings. For example, users can control access to their profiles and allow only their approved friends to see their full profiles, while everyone else sees only a shell consisting of the person's name and profile picture.[35] Similar settings can also be applied to groups. In Facebook, a group's privacy setting can be: "secret," where only members can see the group, who is in it, and what is posted; "closed," where anyone can see the group and who is in it, but only members can see the posted material; or "open," where anyone with a Facebook account can view the group, who is in it, and the content posted in the group.[36] The issue of whether intrusion upon seclusion applies to social networking websites arises when a group designated "secret" or "closed" is accessed by a person who is not authorized. This is

information from particular people).

32. To create a group, a user logs in and from the home page clicks on "Create Group."

33. Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1004 (2009) ("[U]sers of social networking websites tend to disclose much personal information online, yet they seem to retain an expectation of privacy.").

34. *Id.* at 1025–26. Results from a survey of 2,500 respondents revealed that sixty-seven percent of respondents were more upset about family versus acquaintances seeing their pictures, and fifty-four percent believe that it is wrong for people to access information that is not intended for them. *Id.*; *see also* Grimmelmann, *supra* note 30, at 1167 ("[For c]lose friends, it is always OK to comment on their profiles. . . . With distant acquaintances, it is almost never OK. It's those in the middle that are tricky . . . ."); Michelle Slatalla, *'Omg My Mom Joined Facebook!!'*, N.Y. TIMES, June 7, 2007, at G1, *available at* http://www.nytimes.com/2007/06/07/fashion/07Cyber.html (recounting the horror of the journalist's teenage daughter when she found out that her mom joined Facebook and began "friending" her friends) (the term "omg" is shorthand for "Oh, my God," used commonly in text messaging or instant messenger).

35. *Sharing and Finding You on Facebook*, FACEBOOK, https://www.facebook.com/about/privacy/your-info-on-fb (last Nov. 26, 2011) [hereinafter *Facebook Privacy Policy*] (select "expand all").

36. *Id.* When logged into Facebook, click on "Groups" in the left margin, then "Create Group," which will prompt the creator to set the desired privacy settings.

the case of Pietrylo, who created the MySpace equivalent of a "secret" or "closed" group.

### *B. Problems of Perspective*

A preliminary issue courts must resolve before reaching the merits of a case involving the Internet is to determine, as Orin Kerr puts it, the "facts" of the case.[37] Should the case be examined through physical reality or virtual reality? Kerr labels the viewpoint of virtual reality as the "internal perspective" and the viewpoint of physical reality as the "external perspective."[38] In the internal perspective, the facts follow the virtual perspective of the user; in the external perspective, the facts follow the behind-the-scenes perspective of how the Internet actually works.[39] Perspective is important because the facts of the case differ drastically depending on the approach and can determine the outcome of a case.[40]

Applying the internal and external perspectives to intrusion upon seclusion and social networking websites produces two different sets of facts. From the internal perspective, a social networking website is an actual place where users can gather to share ideas, pictures, and videos and interact with others. From the external perspective, social networking websites are nothing more than computer codes, wires, and hard drives. For example, if a user of a social networking website sends a message to a friend, the user is instructing her computer to send a message to her Internet Service Provider (ISP), which directs the ISP to forward the message to the friend's ISP.[41] Which set of facts is most appropriate to examine issues of intrusion upon seclusion?

To select the more appropriate perspective, Kerr suggests studying applicable law for clues of an internal or external approach, and if that fails, to adopt the perspective of the party that the law seeks to regulate.[42] The first approach examines statutes, legislative intent, and case law.[43] This approach provides little insight to intrusion upon seclusion. Because the tort is defined by

37. Kerr, *supra* note 25, at 357.
38. *Id.*
39. *Id.* at 363.
40. *Id.* at 364–79 (illustrating the different outcomes as a result of perspective in cases of the Fourth Amendment, Internet governance, computer crime, and copyright).
41. *Id.* at 366 (going through the steps of sending an e-mail message).
42. *Id.* at 389.
43. *Id.* at 391–96.

common law, there are no statutes to examine or legislative intent to consult.[44] Similarly, case law does not reveal an intent to adopt one perspective over the other because intrusion upon seclusion has not been applied in a meaningful way to the Internet or social networking websites.[45] Therefore, the second approach will apply to intrusion upon seclusion involving social networking websites.

The second approach is following the perspective of the person the law seeks to regulate. Although Kerr is cautious about the second approach, he justifies it on the basis that laws are designed to influence the behavior of targeted individuals.[46] When the law regulates offline conduct, the external perspective applies, and when the law regulates online conduct, the internal perspective applies.[47]

Kerr illustrates the online/offline distinction by presenting two cases concerning the Fourth Amendment that are useful to intrusion upon seclusion. The first case is *United States v. Charbonneau*, in which the court adopted the internal perspective.[48] In *Charbonneau*, an undercover FBI agent entered a chat room posing as a pedophile.[49] The defendant was a member of this chat room and sent an e-mail to everyone with an attachment containing child pornography.[50] The court analogized the e-mail to postal mail and held that because the FBI agent was "in" the chat room, the defendant had no expectation of privacy.[51] While the court did not label its approach as the internal perspective, the court treated the chat room as a physical room, adopting the perspective of the police officer—the person the law seeks to regulate.

The second case is *Bohach v. City of Reno*, in which the court adopted the external perspective.[52] *Bohach* involves a case where police officers used the Department's "Alphapage" system to send messages to each other that appeared on visual display pagers.[53] The officers were aware that the system automatically recorded and

44. *See supra* Part I.B (describing the development of intrusion upon seclusion).
45. *See infra* Part III.B (discussing case law interpretations of intrusion).
46. Kerr, *supra* note 25, at 396.
47. *Id.*
48. *Id.* at 398.
49. United States v. Charbonneau, 979 F. Supp. 1177, 1179 (S.D. Ohio 1997).
50. *Id.*
51. *Id.* at 1185; *see also* Kerr, *supra* note 25, at 398 (discussing the reasoning of the court in *Charbonneau*).
52. Kerr, *supra* note 25, at 399–400.
53. Bohach v. City of Reno, 932 F. Supp. 1232, 1234 (D. Nev. 1996).

stored the messages on a central computer "because that's how the system work[ed]."[54] Focusing on the offline conduct, the court held that there was no search under the Fourth Amendment.[55]

The cases Kerr presents under the Fourth Amendment demonstrate the online/offline distinction that can apply to intrusion upon seclusion cases involving social networking websites. When a defendant intrudes upon a plaintiff's online seclusion using the social network's website (e.g., Facebook, MySpace, LinkedIn, or Twitter), then the defendant's conduct is online and the internal perspective applies. When a defendant intrudes upon a plaintiff's online seclusion without logging onto the social network's website or using a computer at all, then the defendant's conduct is offline and the external perspective applies. In the *Pietyrlo* case, upper management accessed the private group by logging onto MySpace, using St. Jean's login and password, and viewing the comments made within the private group.[56] Upper management did not go through the ISP company to retain electronic copies of posted material.[57] The internal perspective would thus apply. For the purposes of this article, only the defendant's online conduct within a social networking website will be examined, so only the internal perspective applies in this intrusion upon seclusion analysis.

## III. INTENTIONAL INTRUSION (PHYSICAL OR OTHERWISE)

The analogies between cyberspace and real space in intrusion upon seclusion focus on virtual rooms and areas and real-world rooms and areas. In making some of these analogies, a few scholars have argued that common law privacy and intrusion upon seclusion are unable to effectively deal with social networking technologies.[58] However, these scholars have not fully examined the extent to which privacy can be created on social networking websites, looking only at information available in the public domain.[59] To fill this

54. *Id.*

55. *Id.* at 1235.

56. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *3 (D.N.J. July 24, 2008).

57. *Id.* at *5.

58. Neil Richards & Daniel Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CALIF. L. REV. 1887, 1918–19 (2010) (arguing that issues involving protection from the media and the extensive collection, use, and dissemination of personal information by businesses has become more problematic with the use of social networking technologies).

59. *Id.* at 1919 (citing Muratore v. M/S Scotia Prince, 656 F. Supp. 471, 482–

gap, this section will analyze what constitutes an intrusion and how the law should include virtual spaces as being capable of being intruded upon by examining the Restatement's definition, case law, and public policy.

### *A. Rule for What Constitutes an Intrusion*

The first element of intrusion upon seclusion is an intentional intrusion, physical or otherwise, perpetrated by the defendant against the plaintiff.[60] There are three general situations that the Restatement identifies as an intrusion. First, it may be a physical intrusion, such as defendants forcing their way into a hotel room or insisting on entering one's home.[61] Second, an intrusion can occur through the "use of the defendant's senses, with or without the help of [technology], to oversee or overhear the plaintiff's private affairs," such as peering through an upstairs window with binoculars or tapping telephone lines.[62] Finally, an intrusion can occur through an investigation or examination of the plaintiff's private concerns, such as "opening his private and personal mail, searching his safe or his wallet, examining his private bank account [information]," or compelling an inspection of his personal documents through a forged court order.[63] An intrusion of a virtual space does not fit under the first category of a physical intrusion, so it must find support from the case law in either the second or third categories.

### *B. Case Law Interpreting the Definition of Intrusion*

Case law recognizes the role technology can play as a vehicle for an intrusion. In 2002, the Ninth Circuit analyzed privacy associated with a personal website from a statutory perspective in *Konop v. Hawaiian Airlines, Inc.*,[64] but noted the difficulty in doing

83 (D. Me. 1987) ("Much of the compilation of data [that businesses collect] occurs from information that is in the *public domain*, and courts have concluded that collecting such data is not an invasion into a person's 'solitude' or 'seclusion.'" (emphasis added))).

60. Kuhn v. Account Control Tech., 865 F. Supp. 1443, 1448–49 (D. Nev. 1994); *see also* RESTATEMENT (SECOND) OF TORTS § 652B (1977).

61. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

62. *Id.*

63. *Id.* Such intrusions would also violate the Fourth Amendment's protection against unreasonable searches and seizures. United States v. Charbonneau, 979 F. Supp. 1177, 1184 (S.D. Ohio 1997) (quoting United States v. Maxwell, 45 M.J. 406, 417 (Armed Forces 1996)).

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

so because the statutes were enacted prior to the everyday use of the Internet.[65] Nevertheless, the similarities to the *Pietrylo* case and the Ninth Circuit's reasoning are instructive on how to treat private groups on social networking websites.

Like Pietrylo, Konop created a personal webpage, controlled access to the content of his page by issuing account names and passwords to coworkers that e-mailed him for access, posted critical comments about his employer, his superiors gained access to it by using the account name and password of an approved member, and Konop was fired as a result of his posts.[66] In its analysis, the Ninth Circuit found "no principled distinction between the employer's eavesdropping . . . and Hawaiian's access of Konop's secure website."[67] The eavesdropping comparison would put the act of accessing a private group on a social networking website in the Restatement's second category of intrusion, when private information in a private space is surreptitiously overseen or overheard.

When technology is used to penetrate a private space or matter, an intrusion has occurred. The Restatement specifically identifies the use of binoculars to look through an upstairs window or a wiretap on a telephone as intrusions upon seclusion.[68] The courts have broadened section 652B's reach to also include the use of television cameras[69] and microphones[70] as means capable of intrusion. The common element is that technology provides access to otherwise private information or spaces. The trajectory of the

plaintiff brought claims under the Electronic Communications Privacy Act, the Stored Communications Act, and the Railway Labor Act. *Id.*

65. *Id.* at 874 ("[T]he difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web.").

66. *Id.* at 872–73.

67. *Id.* at 884.

68. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977); *see also* Ali v. Douglas Cable Commc'ns, 929 F. Supp. 1362 (D. Kan. 1996) (holding that unannounced recordings of personal telephone calls at work constituted an intrusion).

69. *See* Huskey v. Nat'l Broad. Co., 632 F. Supp. 1282 (N.D. Ill. 1986) (holding that an NBC camera man intruded upon a prisoner's seclusion by videotaping him without his consent); Sanders v. Am. Broad. Cos., 978 P.2d 67 (Cal. 1999) (holding that ABC intruded by surreptitiously videotaping conversations with coworkers); Y.G. & L.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488 (Mo. Ct. App. 1990) (holding a news crew violated a couple's privacy by showing footage of them at a hospital event after they actively tried to avoid the cameras).

70. Shulman v. Grp. W Prods., Inc., 955 P.2d 469 (Cal. 1998) (holding that a flight nurse who wore a microphone so that a television producer could record the statements made by a car accident victim while being transported to the hospital constituted an intrusion).

common law is broadening the Restatement to include technologies that make an intrusion possible. The Ninth Circuit's comparison of accessing a private website to eavesdropping and the common law's expansive approach suggests that the element of intentional intrusion of section 652B is satisfied by the infiltration of a private group on a social networking website.

Moreover, unauthorized access into a private virtual space is or should be an intrusion to remain consistent with the virtual space's physical counterparts. The Restatement identifies that opening personal mail or examining private bank account information can result in an intrusion.[71] Likewise, opening other people's e-mail or viewing their banking information online is as intrusive as if the same information were accessed in paper form. Because the act of eavesdropping on a private in-person conversation constitutes an intrusion, the same result should extend to online conversations held in a private virtual space.

Fourth Amendment search and seizure cases also suggest that a private profile or group on a social networking website deserves privacy protection. The test for whether a space is private under the Fourth Amendment is whether there is an actual, subjective expectation of privacy that society is prepared to recognize as reasonable.[72] The Supreme Court ruled that anything exposed to the public does not constitute a search.[73] Examples include a pen register used by the phone company to determine what phone numbers have been dialed from a private home[74] and aerial

71. RESTATEMENT (SECOND) OF TORTS § 652B cmt. b (1977).

72. California v. Ciraolo, 476 U.S. 207, 211 (1986) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)); *see also* Afsheen John Radsan, *The Case for Stewart over Harlan on 24/7 Physical Surveillance*, 88 TEX. L. REV. 1475, 1480–90 (2010) (surveying the Supreme Court's decisions on surveillance and assessing the federal circuit courts of appeals' adherence to Justice Harlan's two-pronged test).

73. *Katz*, 389 U.S. at 351; *id.* at 361 (Harlan, J., concurring).

74. Smith v. Maryland, 442 U.S. 735, 742 (1979). The Court focused on the facts that all telephone users know that they must convey their phone numbers to the phone company, that phone companies make permanent records of the numbers dialed for monthly billing, and pen registers are used to check billing operations, detect fraud, and prevent illegal activity. *Id.* The approach the Court used in this case would be Kerr's external perspective of looking at how technology actually works. Kerr, *supra* note 25, at 357. While the external approach does not apply to the type of actions analyzed in this article, it does illustrate how the external approach will often result in the destruction of privacy because information is conveyed to third parties, such as Facebook administrators, who reserve the right to remove any posts or materials that violate its terms of use. *Facebook Terms*, *supra* note 29.

surveillance of private homes.[75] Applying this reasoning to profiles or groups on social networking websites that are left open by users likewise results in no privacy protection. Facebook explicitly states, "[w]hen you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)."[76] The public exposure of an open profile or group on a social networking website precludes any privacy protection.

When steps are taken to retain privacy, however, the Supreme Court protects the space. Simply by walking inside a telephone booth and pulling the door shut behind him, Katz established a sufficient privacy expectation to be protected by the Fourth Amendment.[77] Fourth Amendment privacy protection also applies when an electronic beeper in a container of chemicals is brought inside a house and reveals information (the location and movement of the chemicals inside the house) that could not have been obtained without a warrant[78] and to infrared radiation emanating from the home that was detected using technology not available to the general public.[79] When social network users create a private profile or group, it is as if they are closing the virtual door behind them. Everyone, including people off of Facebook, can no longer see their profile or groups. Any unauthorized monitoring or viewing of the private virtual space would constitute an intrusion. The case law interpreting statute, common law, and the Fourth Amendment all indicate that a private virtual space created on a social networking website constitutes a space that can be intruded upon.

### *C. Public Policy Reasons for Extending Intrusion to Virtual Spaces*

The harm associated with intrusion is surveillance. Daniel Solove describes "surveillance" as an awareness that one is being watched.[80] As a result, surveillance can lead to anxiety, discomfort,

75. Florida v. Riley, 488 U.S. 445, 451–52 (1989); *Ciraolo*, 476 U.S. at 215.
76. *Facebook Terms*, *supra* note 29.
77. *Katz*, 389 U.S. at 352.
78. United States v. Karo, 468 U.S. 705, 711 (1984).
79. Kyllo v. United States, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant.").
80. SOLOVE, *supra* note 13, at 106–12.

self-censorship, and inhibition.[81] Intrusion protects the individual by creating liability for such unwanted social invasions, which Solove links to what Warren and Brandeis termed "the right to be let alone."[82]

The concept of surveillance appears to be a concern for users of social networking websites. In a survey of 2,500 respondents, almost twenty-four percent were concerned or very concerned with the possibility that their parents could view their profiles, almost thirty-five percent of users were concerned or very concerned that their employer could access their profile, and forty-three percent were worried about strangers.[83] A commonsense response to such concerns is that if people are truly concerned about such information getting out, they simply should not post it on social networking websites, or they should apply the appropriate privacy settings that match their desired protection. However, this is not a satisfying answer. If someone wishes to share information with a certain group and takes measures to create seclusion from others, that space should be recognized as private by the law.

Solove argues that to adequately address the problems of privacy on the Internet, the law should enforce an individual's social expectations of confidentiality.[84] Such expectations should be enforced even if the surveillance is covert and the victim is never aware of the actual intrusion, because the harms have a chilling effect on behavior and speech.[85] The chilling effect applies equally to positive messages and negative messages because surveillance affects all forms of speech on the Internet through intrusion. While people should be held accountable for what they say and do on social networking websites, such monitoring should not come at the expense of otherwise legitimate speech. As a matter of public policy, when a person creates and maintains a private group within a virtual space on a social networking website, the common law and section 652B should recognize unauthorized access as an intrusion to protect against surveillance and its associated harms.

---

81. *Id.* at 108; *see also* Grimmelmann, *supra* note 30, at 1166 (applying Professor Solove's paradigm to surveillance on Facebook).

82. SOLOVE, *supra* note 13, at 162.

83. Levin & Abril, *supra* note 33, at 1025–26.

84. DANIEL J. SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 191 (2007); *see also* Samantha L. Millier, Note, *The Facebook Frontier: Responding to the Changing Face of Privacy on the Internet*, 97 KY. L.J. 541, 549–50 (2009) (discussing Professor Solove's view of privacy on the Internet and his solutions to privacy concerns).

85. SOLOVE, *supra* note 13, at 109.

## IV. SOLITUDE OR SECLUSION

The previous section established that virtual spaces can be intruded upon, and the next issue is whether a plaintiff can demonstrate adequate seclusion while on social networking websites. This section argues that plaintiffs can establish adequate seclusion to support a claim of intrusion upon seclusion. To do so, this section first provides the Restatement's definition of seclusion and applies it to social networking websites; second, it analyzes the nature of seclusion within a group and then on the Internet; and finally, it examines public policy issues related to "Facebook stalking."

### *A. Rule for What Constitutes Seclusion*

The Restatement provides that for defendants to be subject to liability, they must have intruded into "a private place" or "a private seclusion that the plaintiff has thrown about his person or affairs."[86] However, there is no liability for examining things that are already public or part of a public record, and there is no liability for observing or taking someone's photograph while in public.[87] Nevertheless, some matters may still be considered private when in the public sphere, such as the plaintiff's underwear or lack thereof.[88]

Extrapolating from the premises above suggests that profiles and groups on social networking websites without any privacy settings—leaving them "open" to anyone who clicks on them—do not establish seclusion because the users have not attempted to conceal their persons or affairs.[89] Moreover, posting information on the Internet without taking any steps to make it private is analogous to going out in public. The Restatement makes clear that seclusion does not attach to actions and communications performed in public,[90] and therefore a claim for invasion of privacy

86. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).
87. *Id.*
88. *Id.*
89. *See Facebook Terms*, *supra* note 29 (Facebook administrators explicitly state, "When you publish content or information using the Public setting, it means that you are allowing everyone, including people off of Facebook, to access and use that information, and to associate it with you (i.e., your name and profile picture)."); *Facebook Privacy Policy*, *supra* note 35 and accompanying text (explaining that online social network users can select their desired level of privacy).
90. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).

would probably fail for open profiles or groups on social networking websites.

There are two issues that follow for private groups. The first issue is whether the presence of multiple people within a private group precludes an individual within the group from claiming seclusion. The second issue is whether the nature of the Internet refutes any claims of seclusion even if an individual can maintain seclusion while in a group.

### *B. Case Law Interpreting the Definition of Seclusion*

#### *1. Seclusion Within a Group*

Normally when people enter the public sphere, they do not have an expectation of privacy because they have stepped outside their zone of seclusion, but it is not a complete loss of seclusion. In *Huskey v. National Broadcasting Co.*,[91] a television crew was working on a story about the Illinois prison system.[92] A cameraman shot footage of a prisoner exercising in the jailhouse gym with his shirt off, but the inmate was concerned about others outside of the jail seeing his tattoos.[93] Even though the prison guards and anyone else who walked by could see him, the court reasoned that "the mere fact a person can be seen by others does not mean that person cannot legally be 'secluded.'"[94] The courts have extended this principle to protect a couple attending a private event at a hospital that was covered by a television news crew,[95] a car accident victim's conversation while in a helicopter transporting her to the hospital,[96] a couple filmed in the dining room of a private restaurant,[97] and employees' conversations filmed at a private "telepsychic" business by an investigative reporter wearing a hidden

91. Huskey v. Nat'l Broad. Co., 632 F. Supp. 1282 (N.D. Ill. 1986).
92. *Id.* at 1285.
93. *Id.*
94. *Id.* at 1287–88.
95. Y.G. & L.G. v. Jewish Hosp. of St. Louis, 795 S.W.2d 488, 502 (Mo. Ct. App. 1990) (holding that a couple attending an event at the hospital for *in vitro* couples only chose to disclose their participation to other *in vitro* couples and that "they did not waive the right to keep their condition and the process of *in vitro* private, in respect to the general public").
96. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 492–94 (Cal. 1998) (holding that a helicopter nurse who wore a microphone for television producers intruded upon the victim's seclusion because the course of receiving emergency treatment "carries a traditional and legally well-established expectation of privacy").
97. Stessman v. Am. Black Hawk Broad. Co., 416 N.W.2d 685 (Iowa 1987).

camera.[98]

The principle that the presence of others does not necessarily destroy the protection of seclusion also governs the workplace environment. In *United States v. McIntyre*,[99] a city's police chief ordered two officers to bug the assistant chief's office.[100] Although the assistant chief's door was open and a secretary worked fifteen feet away at the time the assistant chief made the recorded statements, the court ruled, "[a] business office need not be sealed to offer its occupant a reasonable degree of privacy."[101] Not only is aural privacy within the workplace protected, but also visual privacy. In *Doe v. B.P.S. Guard Services, Inc.*,[102] the organizers of a fashion show set up a curtained dressing area for the models at the convention center, but did not realize that a security video camera could see into the area.[103] When security guards used the surveillance camera to watch and videotape the models changing clothes, the court found the actions intruded upon the seclusion of the models.[104]

Not all surreptitious video and audio recordings in the workplace, however, intrude upon an employee's seclusion. In *Marrs v. Marriott Corp.*, an employer videotaped an employee while he was picking a locked drawer of a desk in an open office area.[105] *Kemp v. Block* is a case in which an employee recorded a heated argument with his supervisor in an area where coworkers could overhear them.[106] In both cases the courts ruled that the defendants did not intrude upon the plaintiffs' seclusion because the plaintiffs had no privacy vis-à-vis the coworkers who shared that space.[107] The seclusion-within-a-group line of cases provides that seclusion can be established within a defined group of people when

98. Sanders v. Am. Broad. Cos., 978 P.2d 67, 69 (Cal. 1999) ("[E]mployees may enjoy a limited, but legitimate, expectation that their conversations and other interactions will not be secretly videotaped by undercover television reporters, even though those conversations may not have been completely private from the participants' coworkers.").

99. 582 F.2d 1221 (9th Cir. 1978).

100. *Id.* at 1223.

101. *Id.* at 1224.

102. 945 F.2d 1422 (8th Cir. 1991).

103. *Id.* at 1424.

104. *Id.* at 1427.

105. 830 F. Supp. 274 (D. Md. 1992).

106. 607 F. Supp. 1262 (D. Nev. 1985). Even though the court uses the Fourth Amendment analysis of a subjective expectation of privacy that society is prepared to recognize as reasonable, the decision illustrates that there is no privacy expectation in this situation because seclusion cannot be established. *Id.* at 1264.

107. *Marrs*, 830 F. Supp. at 283–84; *Kemp*, 607 F. Supp. at 1264.

steps are taken to keep information within that group and an alleged intruder is outside that group.

Applying this framework to the Spec-Tator group that Pietrylo created on MySpace suggests that Pietrylo created seclusion because privacy was "thrown about his . . . affairs."[108] Pietrylo created a secluded virtual space when he activated the privacy settings on the MySpace group.[109] The only way to gain access to the group was by invitation.[110] Furthermore, MySpace and other social networking websites require an account name and password,[111] which helps assure that a person cannot sign in as another person without authorization. Finally, Pietrylo stated that his intention of creating the group was to provide a forum to talk openly about what occurred at work without management hearing of it.[112] These facts support a finding that Pietrylo created a private, virtual space because the group was only available to a limited number of people and it was not part of a larger common area.

Moreover, the seclusion of the virtual space was not destroyed by the presence of the other group members being able to read the posts. Using the seclusion-within-a-group line of analysis,[113] Pietrylo's expectation of privacy applies only to those outside the group, just as the expectation of privacy in a jailhouse gym or at a hospital social event applies only to a television-viewing audience. Because the Hillstone Restaurant management was explicitly not part of Pietrylo's group,[114] he maintained his seclusion from those individuals.

108. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977); *see supra* notes 2–4 and accompanying text.

109. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *2 (D.N.J. July 24, 2008).

110. *Id.*

111. *See, e.g.*, FACEBOOK, http://www.facebook.com/ (last visited Sept. 14, 2011); LINKEDIN, http://www.linkedin.com/home?trk=hb_home (last visited Sept. 14, 2011); MYSPACE, http://www.myspace.com/ (last visited Sept. 14, 2011) (click the login link at the top to access the site); TWITTER, http://www.twitter.com/ (last visited Sept. 14, 2011).

112. *Pietrylo*, 2008 U.S. Dist. LEXIS 108834, at *1–2.

113. *See supra* notes 91–107 and accompanying text (discussing cases where seclusion was established despite being in a group setting or in the presence of others).

114. *Pietrylo*, 2008 U.S. Dist. LEXIS 108834, at *2.

*a. Meaningful Distinction Between Simultaneous Dissemination and Secondhand Repetition*

It could be argued that the seclusion-within-a-group analysis does not apply because Hillstone was invited into the Spec-Tator group when St. Jean provided upper management with her MySpace account name and password.[115] Even if St. Jean provided upper management with her account information free from coercion, the *Sanders* court would still find an intrusion into Pietrylo and Marino's seclusion. The *Sanders* court reasoned:

> While one who imparts private information risks the betrayal of his confidence by the other party, a substantial distinction has been recognized between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor, whether that auditor be a person or a mechanical device. Such secret monitoring denies the speaker an important aspect of privacy of communication—the right to control the nature and extent of the firsthand dissemination of his statements.[116]

Even though the posts on the Spec-Tator group remained accessible to the group members for an extended period of time, as opposed to a television camera capturing a moment in time, Hillstone entered an on-going private conversation under the pretext of being an actual participant in that conversation, much like the telepsychic investigative reporter posing as a coworker.[117]

But is the *Sanders* court's distinction between simultaneous dissemination and secondhand repetition meaningful? Is there something worth protecting with simultaneous dissemination that is not destroyed by secondhand repetition? If St. Jean had told upper management exactly what was posted on the Spec-Tator group without giving them access to the site itself, there would be no intrusion, the same information would have been disclosed, and Pietrylo and Marino would still have been fired. For the distinction between simultaneous dissemination and secondhand repetition to be meaningful in intrusion upon seclusion claims, the distinction must serve the ultimate goal of protecting the space, regardless of the information that was discovered, because the tort is complete as soon as the intrusion is made. If the essence of Pietrylo's case were

115. *Id.* at *2–3.

116. Sanders v. Am. Broad. Cos., 978 P.2d 67, 72 (Cal. 1999) (quoting Ribas v. Clark, 696 P.2d 637, 640–41 (Cal. 1985)).

117. *Id.* at 70.

the publication of the posts to those outside the Spec-Tator group, then his intrusion upon seclusion claim should not be allowed to go forward because the invasion would not be the harm. While it is not the goal of this article to provide a full and complete answer to this issue, a closer examination of the distinction between simultaneous dissemination and secondhand repetition can provide a more complete picture of what constitutes seclusion and the values intended to be protected.

The Supreme Court's Fourth Amendment analysis on the privacy interests protected during searches rejects the distinction between simultaneous dissemination and secondhand repetition. In *United States v. White*, the defendant and a government informant, Harvey Jackson, engaged in illegal narcotic transactions.[118] A series of four conversations took place at Jackson's home, during which an agent hid in the kitchen closet with Jackson's consent, overhearing the conversations, and a second agent outside Jackson's home listened using a radio receiver from the wire that Jackson wore.[119] The Court ruled that the government did not violate the Fourth Amendment,[120] reasoning that for constitutional purposes,

> no different result is required if the agent instead of immediately reporting and transcribing his conversations with defendant, either (1) simultaneously records them with electronic equipment which he is carrying on his person . . . (2) or carries radio equipment which simultaneously transmits the conversations either to recording equipment located elsewhere or to other agents monitoring the transmitting frequency.[121]

The Supreme Court's analysis found no legitimate privacy interests in the right to control firsthand dissemination as the *Sanders* court did.

The *White* decision appears to put the Fourth Amendment at odds with the distinction the *Sanders* court made between simultaneous dissemination and secondhand repetition in intrusion upon seclusion claims. Moreover, the defendant's liberty interest associated with the Fourth Amendment is greater than a plaintiff's privacy interest in controlling firsthand dissemination, yet the liberty interest loses and the privacy interest prevails. These

118. United States v. White, 401 U.S. 745, 746 (1971).
119. *Id.* at 747.
120. *Id.* at 754.
121. *Id.* at 751.

conflicting outcomes can nevertheless be reconciled upon a closer examination of the values associated with each.

The overriding value in the Supreme Court's decision in *White* appears to be ensuring the proper functionality of the criminal justice system. The Court made a value judgment: there is no privacy interest in interpersonal, face-to-face interactions when committing a crime.[122] The Court reasoned, "[i]nescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police."[123] If the Court were to provide a privacy right under the Fourth Amendment to protect the right to control the nature and extent of the firsthand dissemination of one's statements, then it would be creating an opportunity for criminal behavior to continue. The Court recognized this possibility and explained, "[n]or should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable."[124] The Court identified the benefits of allowing an electronic recording into evidence, which included a more reliable rendition of what occurred, making it less likely an informant will change his mind to testify, less of a chance that threat or injury will suppress unfavorable evidence during trial, and less likely that cross-examination will confound the testimony.[125] All of these values enhance the functionality of the criminal justice system, which appeared to be the Court's primary concern.[126] As a result, the distinction between simultaneous dissemination and secondhand repetition was properly rejected because the balance between a defendant's Fourth Amendment rights and the State's interest in preventing and punishing crime would have been improper.

The distinction between simultaneous dissemination and

122. Other Fourth Amendment rights still apply. If the officer hiding in Jackson's kitchen closet had not first received consent from Jackson, it would have been an illegal entry into Jackson's home without a warrant. Likewise, if the police had placed a listening device in Jackson's kitchen without consent from Jackson or a warrant, that too would be a violation of the Fourth Amendment.

123. *White*, 401 U.S. at 752.

124. *Id.* at 753.

125. *Id.*

126. *Id.* The Court stated:

> Considerations like these [benefits to the criminal justice system] obviously do not favor the defendant, but we are not prepared to hold that a defendant who has no constitutional right to exclude the informer's unaided testimony nevertheless has a Fourth Amendment privilege against a more accurate version of the events in question.

*Id.*

secondhand repetition is properly enforced, however, in a claim for intrusion upon seclusion because the values in this tort shift to protecting the privacy of the space created. What is important in intrusion upon seclusion is maintaining the integrity of an area that people have sought to make private so that actions and communications that are intended to be private remain so. A value protected by maintaining the integrity of seclusion includes what Julie Inness identifies as intimacy.[127] She argues that "privacy cannot be captured if we focus exclusively on either information, access, or intimate decisions because privacy involves all three areas" and suggests that "these apparently disparate areas are linked by the common denominator of intimacy—privacy's content covers *intimate* information, access, and decisions."[128] Inness states that "intimacy" draws its meaning from one's "love, liking, or care. Intimate decisions concern such matter and, thus, involve a choice on the agent's part about how to (or not to) embody her love, liking, or care."[129] In light of her ideas about intimacy, Inness developed a conception of privacy, under which privacy "now amounts to the state of the agent having control over decisions concerning matters that draw their meaning and value from the agent's love, caring, or liking. These decisions cover choices on the agent's part about access to herself, the dissemination of information about herself, and her actions."[130] As such, "the construction of intimacy lies on the agent's shoulders."[131]

Inness's construction of privacy aligns with intrusion upon seclusion. The Restatement (Second) of Torts requires that the plaintiff "throw[]" privacy about his person or affairs.[132] Likewise, the construction of intimacy is on the agent's shoulders, meaning it is the agent—or plaintiff—who has the burden to make a space private. Pietrylo did this by making the Spec-Tator a private group. Pietrylo also shared intimate communications and ideas.[133] While his comments about his place of employment and employer are not intimate in the physical or sexual sense, Pietrylo's comments do

127. JULIE INNESS, PRIVACY, INTIMACY, AND ISOLATION 56 (1992); *see also* SOLOVE, *supra* note 13, at 34–37 (surveying similar theories of intimacy).
128. INNES, *supra* note 127.
129. *Id.* at 75.
130. *Id.* at 91.
131. *Id.*
132. RESTATEMENT (SECOND) OF TORTS § 652B cmt. c (1977).
133. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *3–4 (D.N.J. July 24, 2008).

draw on his caring and liking, or lack thereof, for his workplace.[134] Finally, Pietrylo attempted to control access and dissemination of information about himself by making the group private.[135] All of the elements of Inness's conception of privacy are met by Pietrylo's actions.

The value that is protected through the distinction between simultaneous dissemination and secondhand repetition is intimacy and maintaining space for intimacy to occur. While secondhand repetition is always a concern, such repetition does not threaten the space where intimacy can occur. Rather, it forces people to evaluate with whom they wish to share intimate information. Simultaneous dissemination, however, threatens the space itself. Inness incorporates access to oneself and the dissemination of information about oneself into her conception of privacy,[136] which the *Sanders* court echoes by protecting the right to control the nature and extent of the firsthand dissemination of one's statements.[137] Therefore, because intrusion upon seclusion involves intimacy where criminal behavior does not, the distinction between simultaneous dissemination and secondhand repetition is properly recognized in intrusion upon seclusion to protect the integrity of the space.

### *b. MySpace Page Not Similar to an Open Office Space*

It could instead be argued that the virtual space associated with the MySpace page created an area of common space shared by multiple coworkers, similar to the open office space found in *Marrs*[138] or *Block*.[139] However, this argument fails because the Spec-Tator group (i.e., the virtual space) was only weakly associated with the workplace. There is no evidence that the MySpace group was accessed at the restaurant because Pietrylo and Marino were servers and St. Jean was a greeter.[140] The employees presumably had little to no access to computers with Internet access during their shifts.

134. *Id.*
135. *Id.* at *2.
136. *See supra* notes 127–31 and accompanying text.
137. *See supra* note 117 and accompanying text.
138. Marrs v. Marriott Corp., 830 F. Supp. 274, 283 (D. Md. 1992) (videotaping an employee picking a locked desk in a common area).
139. Kemp v. Block, 607 F. Supp. 1262, 1264 (D. Nev. 1985) (overhearing a heated argument while at work).
140. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *2–3 (D.N.J. July 24, 2008) (discussing how the employees at the restaurant gained access to the website).

Moreover, Pietrylo's stated intention was to air criticism outside the presence of management, which could not be done freely at the restaurant because a supervisor or manager would always be on duty.[141] The fact that Pietrylo dissociated the Spec-Tator group from the restaurant is significant because upper management is removed from the space.

*c. Seclusion Need Not Be Absolute*

Even if the MySpace page were considered to be part of the workplace, the private website would be more akin to *McIntyre* and *B.P.S. Guard Services* than *Marrs* and *Kemp*. *McIntyre* and *B.P.S. Guard Services* established that aural and visual privacy within the workplace does not need to be absolute.[142] The precautions Pietrylo took to make the Spec-Tator group private made it more comparable to a personal office in a police station[143] or an office section protected by curtains,[144] rather than an open office area[145] or a shared common area.[146] Therefore, Pietrylo could probably establish that his private group on MySpace met the seclusion requirement for a claim of intrusion upon seclusion.

*d. Apparent Authority*

Hillstone may argue that there was apparent authority to enter the Spec-Tator group when St. Jean provided her username and password, but the Fourth Amendment's rule on apparent authority can be applied to intrusion upon seclusion to reject such an argument. When a space is owned and controlled by more than one person so that they share common authority, any of those people can give consent to government agents to search the area.[147] The Court has held that common authority rests

> on mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and

141. *Id.* at *1–2.
142. Doe v. B.P.S. Guard Servs., Inc., 945 F.2d 1422, 1427 (8th Cir. 1991); United States v. McIntyre, 582 F.2d 1221, 1224 (9th Cir. 1978); *see supra* text accompanying notes 99–107.
143. *McIntyre*, 582 F.2d at 1224.
144. *B.P.S.*, 945 F.2d at 1424.
145. Marrs v. Marriott Corp., 830 F. Supp. 274, 283 (D. Md. 1992).
146. Kemp v. Block, 607 F. Supp. 1262, 1263 (D. Nev. 1985).
147. United States v. Matlock, 415 U.S. 164, 170 (1974).

> that the others have assumed the risk that one of their number might permit the common area to be searched.[148]

In *Illinois v. Rodriguez*, the Court expanded common authority to those who have apparent authority to give consent to a search based on whether the facts and circumstances would give a person of reasonable caution the belief that the person has authority over the area.[149]

In the case of Pietrylo, assuming St. Jean gave her username and password free from any coercion, Hillstone may be able to claim that it received consent from St. Jean through apparent authority. In *Rodriguez*, the fact that the third party had a key to the apartment was a significant fact in establishing apparent authority.[150] The *Rodriguez* Court also considered the affirmative statements the third party made: she lived there and had furniture and clothing in the apartment.[151] Here, St. Jean's username and password were the virtual equivalent to a key, giving Hillstone access to the Spec-Tator group. However, St. Jean was not the creator of the group[152] and would not have had administrative privileges unless Pietrylo had assigned them to her.[153] Thus, St. Jean did not have the ability to control membership or content of the group, edit the group's description or settings, or remove or ban members.[154] Instead of having common authority over the group, she was the equivalent of a guest in a virtual room, limited to the features enabled by the group's creator.[155] St. Jean's apparent authority would not extend so far as to give a reasonably cautious person the belief that she shared joint control over the

148. *Id.* at 171 n.7.

149. Illinois v. Rodriguez, 497 U.S. 177, 188 (1990).

150. *Id.* at 179–81.

151. *Id.* at 179. The assertions made by the third party were ultimately proven false and it was determined that she did not have common authority over the apartment. *Id.* at 181–82.

152. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *1 (D.N.J. July 24, 2008).

153. *See Facebook Help Center Admin Basics*, FACEBOOK, http://www.facebook.com/help/?page=18829 (last visited Sept. 14, 2011) [hereinafter *Facebook Admin Basics*] (click on the description of "What is a group admin?"). A group member can be given administrative privileges and gain all of these abilities by the creator or another administrator of the group. *Id.* Without administrative privileges, a member can only post comments on the group's wall, post pictures, or do any other activities allowed by the settings of the group. *See Facebook Help Center Group Features*, FACEBOOK, http://www.facebook.com/help/?page=18832 (last visited Sept. 14, 2011) [hereinafter *Facebook Group Features*].

154. *See Facebook Admin Basics*, *supra* note 153.

155. *See Facebook Group Features*, *supra* note 153.

group.

Further analogizing a username and password to a key in the context of social networking websites likewise does not give Hillstone apparent authority to enter the Spec-Tator group. Compare a Facebook profile to a hotel. The manager of the hotel has the master key to all of the rooms. Some of the rooms are vacant, so the manager could enter those rooms without violating anyone's privacy. Other rooms are checked out, and if the manager, or anyone else, were to use the key and enter without the occupants' permission, it would invade their privacy.[156] Here, a Facebook profile is the hotel, the individual's username and password are the master key, and the groups of which the user is a member are the rooms. The groups that are left open are like the vacant rooms—a person can enter them without violating the occupant's privacy. The groups that are private are like the occupied rooms—they cannot be entered without permission. Just as possession of a key by itself does not automatically demonstrate permission to enter a locked area, a username and password do not automatically demonstrate permission to enter a private group on a social networking website. Therefore, having a username and password alone should not be sufficient to give apparent authority to enter a private group on a social networking website.

*2. Seclusion on the Internet*

Given the relatively new phenomenon of social networking websites, no court has explicitly ruled on the threshold question of when a website moves from the public to the private sphere, but other decisions provide valuable insight. In *United States v. Gines-Perez*, the district court in Puerto Rico ruled on the relationship between privacy and the Internet in a criminal case.[157] The police identified the suspect by using a picture that was taken from a business website still under construction and not yet open to the public at large.[158] It ruled that "a claim to privacy is unavailable to someone who places information on an indisputably, public medium, such as the Internet, *without taking any measures to protect the information*."[159]

Using similar reasoning, the Minnesota Court of Appeals in

156. *See* Prosser, *supra* note 14, at 389–90.
157. United States v. Gines-Perez, 214 F. Supp. 2d 205, 225–26 (D.P.R. 2002).
158. *Id.* at 212–13.
159. *Id.* at 225.

*Yath v. Fairview Clinics*[160] ruled that information the defendant posted on an open MySpace page was necessarily made public under a theory of publication of private facts—a related invasion-of-privacy claim provided by section 652D of the Restatement.[161] In a concurring opinion, Judge Johnson suggested that the analysis would be different if it had been a private webpage,[162] but the majority opinion never addressed the issue because it was not part of the fact pattern. Dealing with a restricted website, the Ninth Circuit in *Konop* found that controlling Internet access by assigning account names and passwords was sufficient to create seclusion in a claim based on statutory privacy.[163]

The common element among the different courts and the different contexts in which privacy is applied is whether the plaintiffs took steps to maintain their privacy. The district court in *Gines-Perez* viewed the lack of any positive steps to keep the communications on the Internet private as a fundamental shortcoming for claiming privacy,[164] while the Ninth Circuit in *Konop* found the issuance of account names and passwords to be sufficient.[165] Because all social networking websites require a username and password, that alone may not be adequate, but the *Yath* concurrence suggests that a private webpage would be enough to establish privacy online.[166] Therefore, because Pietrylo took affirmative steps to keep the MySpace group private by personally inviting each member into the group and stating that Spec-Tator was a private group,[167] he probably could satisfy all three standards set forth by the different courts.

### *C. Public Policy Reasons for Extending Seclusion to Virtual Spaces*

Giving private online spaces the protection of "seclusion" would discourage Facebook "stalking" and the like. Using Solove's

160. Yath v. Fairview Clinics, 767 N.W.2d 34, 42–43 (Minn. Ct. App. 2009).

161. *Id.* at 43. Restatement section 652A provides: "(1) One who invades the right of privacy of another is subject to liability for the resulting harm to the interests of the other. (2) The right to privacy is invaded by . . . (c) unreasonable publicity given to the other's private life, as stated in § 652D." RESTATEMENT (SECOND) OF TORTS § 652A (1977).

162. *Yath*, 767 N.W.2d. at 51 (Johnson, J., concurring).

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

164. *Gines-Perez*, 214 F. Supp. 2d at 225.

165. *Konop*, 302 F.3d at 884.

166. *Yath*, 767 N.W.2d at 51 (Johnson, J., concurring).

167. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *2 (D.N.J. July 24, 2008).

framework of surveillance and its associated harms,[168] James Grimmelmann describes "Facebook stalking" as occurring when a person snoops into the profiles of distant acquaintances of those whom are considered to be outside one's general social network.[169] Similar to a Peeping Tom looking through a window at night, the Facebook stalker looks through the virtual window of a person's profile or group.

The privacy paradox in which social network users disclose large amounts of personal information, yet retain a sense of privacy,[170] asserts itself most prominently when plaintiffs assist their stalkers by accepting friendship requests of distant acquaintances.[171] People who accept many distant acquaintances as "friends" and do not set any privacy settings may rightfully react with indignation that their personal information was accessed by someone outside of their normally accepted social network,[172] but they should not be surprised because that is exactly what they gave them permission to do. Even employers are taking advantage of social networking pages that are left open. A survey by the Ponemon Institute reported that "61% of professional services companies, which includes law firms, conduct Google searches on job candidates . . . . [and] more [than] 50% of the companies also search social network websites, such as Facebook and MySpace."[173]

The Restatement and case law seem to indicate that when a social network user leaves an online profile or group open, seclusion cannot be claimed, but when people access a private (protected) profile or group without authorization, they have intruded upon the seclusion of those protected by the privacy settings.[174] The intruding party is not a part of that particular social

168. SOLOVE, *supra* note 13; *see also supra* notes 80–82 and accompanying text.

169. Grimmelmann, *supra* note 30, at 1167. To define the boundaries of a social network—and the status of those members as truly a friend or more of an acquaintance—is difficult because it is a fluid concept. Offline social networks are interconnected and porous, making online social networks even more interconnected and porous because MySpace and Facebook "friends" can change so quickly and they can be accumulated in mass. Levin & Abril, *supra* note 33, at 1046. The average Facebook user has 130 "friends." *Statistics*, *supra* note 27.

170. *See* Levin & Abril, *supra* note 33, at 1045; *see also* Grimmelmann, *supra* note 30, at 1167–68 (quoting a social network user's expectations of privacy).

171. *Cf.* Levin & Abril, *supra* note 33, at 1018–19 ("[T]he making of 'friends' online for the sake of mere accumulation of a large number of 'friends' as a status symbol is a growing online social phenomenon in itself.").

172. *Id.* at 1001–02.

173. Robert B. Fitzpatrick, *Emerging Employment Law Issues*, SP024 ALI-ABA 1995, 2253 (2008).

174. *Supra* notes 86–89 and accompanying text.

network, and the plaintiff has taken steps to retain one's privacy. Although "Facebook stalking" and other unauthorized entries into a profile or group are initially invisible,[175] making detection and a successful claim difficult, it does not mean that the plaintiff's seclusion does not exist. The ubiquitous use of the Internet and social networking websites has challenged the strength of privacy protections in the virtual realm, and the law should respond to provide plaintiffs with a meaningful remedy.

## V. HIGHLY OFFENSIVE TO A REASONABLE PERSON

Users of social networking websites should be able to establish an intrusion into a private area when profiles or groups are made private, but such an intrusion must be highly offensive.[176] The highly offensive standard is a high threshold for plaintiffs to meet and was designed to make bringing a claim difficult.[177] This section discusses whether and under what circumstances an intrusion into a private profile or group on a social networking website would be highly offensive by first examining the Restatement; second, analyzing case law; and third, identifying public policy concerns.

### *A. Rule for What Constitutes Highly Offensive*

As a threshold issue, the common law requires that an intrusion "be highly offensive to a reasonable person."[178] There is no liability unless the interference with the plaintiff's seclusion is substantial and a reasonable person would strongly object to the

175. *See* Grimmelmann, *supra* note 30, at 1168.

176. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

177. *See id.* at cmt. d ("There is . . . no liability unless the interference with the plaintiff's seclusion is a substantial one, of a kind that would be highly offensive to the ordinary reasonable man, as the result of conduct to which the reasonable man would strongly object."); *see also* Prosser, *supra* note 14, at 422–23. Prosser expresses concern over how far intrusion upon seclusion should go, explaining that "the question may well be raised whether there are not some limits, and whether . . . a lady who insists upon sun-bathing in the nude in her own back yard should really have a cause of action for her humiliation when the neighbors examine her with appreciation and binoculars." *Id.* at 422. He concludes, "This is not to say that the developments in the law of privacy are wrong. . . . It is to say rather that it is high time that we realize what we are doing, and give some consideration to the question of where, if anywhere, we are to call a halt." *Id.* at 423. *See also* Richards & Solove, *supra* note 58, at 1890 ("Prosser [the primary author of the Restatement (Second) of Torts] was deeply skeptical of the privacy torts. . . .").

178. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

intrusion.[179] Knocking on the plaintiff's door or calling the plaintiff, even two or three times for payment of a debt, does not constitute a "highly offensive" intrusion because the actions do not amount to a substantial burden to the plaintiff's existence.[180]

### *B. Case Law Interpreting the Definition of Highly Offensive*

The Nevada Supreme Court noted that what constitutes "highly offensive" is "largely a matter of social conventions and expectations,"[181] and identified factors that contribute to determining whether an intrusion was highly offensive: "the degree of intrusion, the context, conduct and circumstances surrounding the intrusion as well as the intruder's motives and objectives, the setting into which he intrudes, and the expectations of those whose privacy is invaded."[182] The California Supreme Court echoed some of the same factors, stating that "all the circumstances of an intrusion, including the motives or justification of the intruder, are pertinent to the offensiveness element."[183] The Nevada and California Supreme Courts identify a broad-range, overlapping, and non-exhaustive list of factors.[184] While this is only a very selective representation of jurisdictions, it does suggest a totality-of-the-circumstances approach to analyzing the factor of "highly offensive." The result is that it gives courts broad authority to decide whether intrusion upon seclusion claims can go forward, and injects a degree of uncertainty into the outcome of jury cases.

In *Pietrylo*, Hillstone management used the username and password of a current group member to secretly and deliberately gain access to the group to monitor and evaluate what it ultimately concluded were "offensive" statements.[185] The facts surrounding

179. *Id.* at cmt. d.

180. *Id.* An example of when an intrusion is "highly offensive" and thereby invades a plaintiff's privacy is when "telephone calls are repeated with such persistence and frequency as to amount to a course of hounding the plaintiff, that becomes a substantial burden to his existence." *Id.*

181. PETA v. Bobby Berosini, Ltd., 895 P.2d 1269, 1281 (Nev. 1995) (quoting J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5.10(A)(2) (1993)).

182. *Id.* at 1282 (quoting Miller v. Nat'l Broad. Co., 232 Cal. Rptr. 668 (Ct. App. 1986)).

183. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 493 (Cal. 1998); *see also* Sanders v. Am. Broad. Cos., 978 P.2d 67, 73–74 (Cal. 1999) ("Privacy for purposes of the intrusion tort must be evaluated with respect to the identity of the alleged intruder and the nature of the intrusion.").

184. *See Shulman*, 955 P.2d at 493; *PETA*, 867 P.2d at 1133.

185. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *3–4 (D.N.J. July 24, 2008).

Hillstone's intrusion using the factors from the Nevada and California courts could be sufficient to classify Hillstone's actions as "highly offensive."

The first factor of degree of intrusion and Hillstone's conduct would favor Pietrylo. Hillstone committed a complete intrusion into the virtual space because upper management used the account name and password of a member to gain full access and read all of the material posted on the Spec-Tator group.[186] Upper management did not accidentally stumble across the website, but made a conscious decision to enter the website and view its contents.[187]

A second factor is the context and circumstances surrounding the intrusion, which may also favor Pietrylo. Hillstone acted with secrecy and deliberateness in accessing the Spec-Tator group,[188] a private virtual space not associated with and operated separately from the restaurant's business. The stealth of Hillstone's actions may contribute to the degree of offensiveness for some juries. The users of online social networking websites are disproportionately represented by younger generations who may be more sensitive to online intrusions,[189] as market research shows that only ten percent of online socializers are older than fifty-five, while almost fifty percent of online socializers are younger than thirty-five.[190]

Finally, Hillstone's motives and objectives are probably canceled out by Pietrylo's privacy expectations. Hillstone's objective was to see what its employees were saying about the restaurant.[191] The fact that Hillstone ultimately fired Pietrylo and

186. *Id.* at *3.

187. *Id.*

188. *See id.* (giving upper management the username and password to read the unedited posts).

189. Levin & Abril, *supra* note 33, at 1001–02 (users of social networking websites react with indignation when their profiles are accessed by those outside their social network).

190. *Id.* at 1017. However, surveys from April 2008 and April 2009 indicate that the highest growth percentage for Facebook users was the 35–49 year-old demographic, followed by the 50–64 year-old demographic. *Product Briefs*, 26 No. 21 LAW. PC 12, 12–13 (2009); *see also* Camille Broussard, *Teaching with Technology: Is the Pedagogical Fulcrum Shifting?*, 53 N.Y.L. SCH. L. REV. 903, 912 (2009) (referring to the generation of young adults who are totally comfortable with emerging technologies as "digital natives," and those who use web-based applications and technologies, but for whom it is not their native soil, as "digital immigrants").

191. *See* Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *3–4 (D.N.J. July 24, 2008) (viewing and printing content from the Spec-Tator).

Marino[192] indicates that its objective in intruding upon the Spec-Tator group was to determine if any employees had committed misconduct. This suggests that Hillstone entered knowing that it was not invited and that the company was searching for employee misconduct. Having intentions where punishment would be a likely consequence seems more offensive than if a member of upper management had discovered the website by accident and surveyed it out of general curiosity.

However, Hillstone's objectionable motives to control what it deemed to be offensive behavior are balanced by Pietrylo's objective expectations of privacy.[193] While Pietrylo maintains that he expected everything to remain private within the Spec-Tator group, he did invite several people to be members of an online group.[194] Information on the Internet can spread rapidly and has a high degree of permanency once posted.[195] Unlike a conversation in a physical room, where the spoken word has no lasting presence, posted material on the Internet can remain indefinitely.[196] The nature of the Internet makes an intrusion less offensive than if Hillstone had clandestinely listened to a spoken conversation. While Hillstone's motives may factor in favor of Pietrylo, they seem to be balanced out by Pietrylo's chosen medium.

### *C. Public Policy Reasons for Extending the Concept of "Highly Offensive" to Virtual Spaces*

The factors to determine what is highly offensive, presented above,[197] are necessarily judgment calls for the finder of fact to decide. While it is a subjective process, the factors appear to advance a concept of personal dignity, and understanding the role of personal dignity through the development of the right to privacy provides guidance for determining what constitutes "highly offensive." In 1890, Warren and Brandeis reasoned:

> The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some

192. *Id.* at *4.
193. *See id.* at *18 ("A right to privacy may be a source of 'a clear mandate of public policy' that could support a claim for wrongful termination; however, these privacy interests will be balanced against the employer's interests in managing the business.").
194. *Id.* at *2.
195. *See* Levin & Abril, *supra* note 33, at 1046.
196. *See id.*
197. *See supra* Part V.B.

> retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions upon his privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury.[198]

Their reflection on society could apply equally well to social networking websites today. Warren and Brandeis went on to argue that developments in technology made solitude and privacy more essential to the individual.[199]

Edward Bloustein contends that Warren and Brandeis's right to privacy protects personal dignity, which should be the fundamental concept courts use to decide cases of intrusion upon seclusion.[200] Bloustein explains, "[O]ur Western culture defines individuality as including the right to be free from certain types of intrusions. This measure of personal isolation and personal control over the conditions of its abandonment is of the very essence of personal freedom and dignity . . . ."[201] The *Shulman* court couched its intrusion analysis in Bloustein's reasoning,[202] finding that an intrusion into private places, conversations, or matters represents the best example of an invasion of privacy.[203] Moreover, sociological research suggests that even when people are in public spaces, they need personal space for "comfort, ease, and relaxation."[204]

In *Pietrylo*, Hillstone's intrusion may meet the element of "highly offensive" when using Bloustein's definition of privacy based on the loss of personal isolation and the loss of personal control of choosing when to abandon that seclusion. Pietrylo created a space to relax and find comfort with other coworkers and by excluding management from the Spec-Tator group, Pietrylo attempted to create a partially isolated place to vent about personal matters, such as his feelings about his workplace.[205] When upper management entered the Spec-Tator group, Hillstone intruded

198. Warren & Brandeis, *supra* note 12, at 196.
199. *Id.* at 195.
200. Bloustein, *supra* note 1, at 971, 973–74.
201. *Id.* at 973.
202. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 489 (Cal. 1998).
203. *Id.*
204. SOLOVE, *supra* note 13, at 164–65.
205. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *1–2 (D.N.J. July 24, 2008).

upon Pietrylo's isolation by invading the area Pietrylo had created for comfort, ease, and relaxation among his coworkers and friends. Moreover, upper management took away Pietrylo's personal control of abandoning his privacy. Personal dignity is lost as soon as an intruder penetrates the private virtual space that was created because it destroys limited personal isolation and usurps the personal control of choosing when and how to abandon one's seclusion.

A second reason personal dignity should play a role in determining offensiveness is because it best conceptualizes the harm associated with invasion of privacy claims involving digital information. Currently, the competing theoretical approach to the dignity paradigm is that online privacy is rooted in control.[206] This theory provides people, groups, and institutions with the autonomy to decide when, how, and to what extent information is shared with other people.[207] So long as people have control over the personal information that is disclosed about them, there is no violation of privacy.[208] When someone intrudes on another's autonomy by gaining access to private information, the latter has lost control and there is an invasion of privacy.[209]

There are three challenges to this theory. First, online social networks are extremely complex, large, and fluid, making any control settings difficult to maintain if used to keep out specific people or particular types of people.[210] Second, when information is in digital form, it can easily be copied, distributed, and manipulated.[211] The control approach may not always offer

206. Levin & Abril, *supra* note 33, at 1001–02.

207. *Id.* at 1008–09 (surveying different theories of privacy as control).

208. *Id.*

209. *See id.*

210. *See id.* at 1046; *see also* Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs*, U. OF VIRGINIA ENGINEERING DEP'T OF COMPUTER SCI., http://www.cs.virginia.edu/felt/privacybyproxy.pdf (last visited Sept. 19, 2011) (proposing that social networks are "complex" and "fluid"). Examples of "types of people" could include coworkers, family members, or classmates within the same "network school." Facebook uses schools and geographical locations to define networks. Some privacy settings allow everyone within a network to see everyone's profile, regardless of whether they are "friends" or not. Other privacy settings allow friends of friends to have access. Therefore, networks and who is part of a network can constantly change.

211. *See, e.g.*, Emi Kolawole, *DefCon Opens Its Doors to Pre-teen and Teen Hackers*, WASH. POST INNOVATIONS (Aug. 9, 2011, 6:00 AM), http://www.washingtonpost.com/blogs/innovations/post/defcon-opens-its-doors-to-pre-teen-and-teen-hackers/2011/08/08/gIQALnOW3I_blog.html (reporting that the hacking conference, DefCon, now invites young people aged eight to sixteen, as a

adequate protection to a plaintiff, because the ease at which information is created and distributed makes the control approach difficult to apply and thus unenforceable.[212] Finally, the Restatement only seeks to protect against "highly offensive" behavior.[213] Loss of control is not inherently offensive. Rather, it is the nature of the space and the manner in which the space is intruded upon that may be offensive.

A personal dignity approach provides a clearer line of when an intrusion highly offends a reasonable person. When a defendant intrudes upon a private place, conversation, or matter[214] that inhibits the comfort, ease, and relaxation[215] of the plaintiff, the plaintiff's personal dignity has been highly offended. Pietrylo created a private MySpace group to vent about occurrences at work with other restaurant employees outside the presence of management.[216] Hillstone intruded upon this private conversation by using St. Jean's account name and password.[217] Hillstone also inhibited Pietrylo's comfort, ease, and relaxation because it effectively shut down the space and then fired him from his job.[218] This would probably be highly offensive to a reasonable person's sense of personal dignity.

## VI. CONCLUSION

This article began with the question of whether a private, virtual space created by a social networking website would be covered by the Restatement (Second) of Torts section 652B (1977). Given the relatively new emergence of social networking websites, this issue is just beginning to be addressed by courts. While courts have been slow to integrate new technologies into privacy law,[219] the tort of intrusion upon seclusion should be extended to cover intrusion into private areas created on social networking websites because the language of the Restatement is sufficiently broad, it

---

new trend emerges of summer camps and programs dedicated to teaching kids how to manipulate digital information).

212. *See id.* (describing a culture of hacking).

213. RESTATEMENT (SECOND) OF TORTS § 652B (1977).

214. Shulman v. Grp. W Prods., Inc., 955 P.2d 469, 489 (Cal. 1998).

215. SOLOVE, *supra* note 13, at 164.

216. Pietrylo v. Hillstone Rest. Grp., No. 06-5754, 2008 U.S. Dist. LEXIS 108834, at *1–2 (D.N.J. July 24, 2008).

217. *Id.* at *2–3.

218. *See id.* at *3–4 (accessing the group to view the comments).

219. Richards & Solove, *supra* note 58, at 1921 ("[C]ourts appear stuck with notions of privacy more appropriate for the first half of the twentieth century.").

would be a natural extension of the case law, and public policy favors such an interpretation.

Under the first factor—intentional intrusion, physical or otherwise—an intrusion of a virtual space should be assessed based on whether the defendant learned of the plaintiff's private affairs or matters through a type of surveillance. The second factor—establishing an expectation of seclusion or solitude on social networking websites—should be evaluated not by the number of people who have access to the profile or group, but rather by the privacy settings the plaintiff has implemented to restrict access to his or her information. Finally, the third factor—determining what is highly offensive—should be analyzed through a lens of personal dignity that takes into account the private space, conversation, or matter intruded upon and the result of whether the plaintiff's comfort, ease, and relaxation were inhibited. Such an extension of the tort of intrusion upon seclusion will provide the proper protection to online social network users who make the effort to keep certain messages and material private on the Internet.