Vanderbilt Journal of Entertainment & Technology Law

Volume 11
Issue 4 *Summer 2009*

Article 9

2009

Two Notions of Privacy Online

Avner Levin

Patricia S. Abril

Two Notions of Privacy Online†

Avner Levin and Patricia Sánchez Abril***

ABSTRACT

Users of social networking websites tend to disclose much personal information online yet seem to retain some form of an expectation of privacy. Is this expectation of privacy always unreasonable? How do users of online social networks define their expectations of privacy online?

These questions were the impetus behind an empirical study, the findings of which are presented in this Article. The project, simultaneously conducted in Canada, at Ryerson University, and in the United States, at the University of Miami, consisted of a survey regarding personal information protection and expectations of privacy on online social networks (OSNs). Approximately 2,500 young adults between the ages of 18 and 24 were surveyed about the personal information they post online, the measures they take to protect such information, and their concerns, if any, regarding their personal information. Respondents also reacted to several hypothetical scenarios in which their privacy was breached on an OSN by measures both within and beyond their control.

The theoretical assumption underlying this research project is that two prevalent and competing notions of privacy online exist: one rooted in control and the other in dignity. Of the two, the idea of privacy as control over one's personal information has, to date, been predominant. Legislation, regulation, corporate policy, and technology are often analyzed and evaluated in terms of the measure of control

---

† The authors are grateful to participants in the 2008 User-Generated Content, Social Networking and Virtual Worlds Roundtable at Vanderbilt University Law School, and in particular to Professors David Post and Daniel Gervais, for their insightful comments. In addition, the authors would like to thank Alissa del Riego for her valuable research assistance.

* Associate Professor and Chair, Law & Business Department, Ted Rogers School of Management, Ryerson University.

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

offered to individuals over their personal information. Leading OSNs, such as Facebook and MySpace, propagate a notion of privacy as user control. However, online social networking poses a fundamental challenge to the theory of privacy as control. A high degree of control cannot preclude the possibility that online socializers would post unflattering, defamatory, or personal information about each other, and that this information would in turn be available to a large, if not unrestricted, online audience. Many online socializers post personal information seemingly without much concern over the loss of control, yet it seems that online socializers react with indignation when their personal information is accessed, used, or disclosed by individuals perceived to be outside their social network.

The findings presented here indicate indeed that online socializers have developed a new and arguably legitimate notion of privacy online, that if accepted by OSNs, will offer online socializers both control and protection of their dignity and reputation. We call this notion network privacy. According to network privacy, information is considered by online socializers to be private as long as it is not disclosed outside of the network to which they initially disclosed it, if it originates with them, or as long as it does not affect their established online personae, if it originates with others. OSNs, as businesses profiting from socializing online, are best positioned to offer online socializers, often the young and vulnerable, effective protection in accordance with their notion of network privacy above and beyond regular measures of personal information control, and they should be required to do so.

TABLE OF CONTENTS

> I see no hope for the future of our people if they are dependent on the frivolous youth of today, for certainly all youth are reckless beyond words.
>
> —Hesiod 800 BC

Hesiod mused three thousand years ago, yet his comments seem as relevant as ever to the conduct of young online socializers today. Teenagers and young adults post salacious photos of themselves and their peers, blog about intimate details, breakup relationships, forge new ones, and vent about bosses and colleagues online, among other activities that are traditionally deemed private. Reckless? No doubt, and yet, there are many popular accounts of the same online socializers reporting feelings of invasion when unintended audiences discover online photos or when an online "friend" betrays trust.[1] Herein is the privacy contradiction: users of social networking websites tend to disclose much personal information online, yet they seem to retain an expectation of privacy. Is this expectation always unreasonable? Can the ancient wisdom that the "youth of today" behave recklessly be reconciled with the reported feeling of vulnerability online? How do users of online social networks define their expectations of privacy online? Is the feeling of invasion grounded in a sense of privacy and self that the law should protect?

These questions were the impetus behind an empirical study, the findings of which are presented in this Article. The project, simultaneously conducted in Canada, at Ryerson University, and in the United States, at the University of Miami, consisted of a survey regarding personal information protection and expectations of privacy in online social networks (OSNs).[2] Approximately 2,500 young adults between the ages of 18 and 24, who were both students at the participating academic institutions and members of OSNs, were surveyed about the personal information they post online, the measures they take to protect such information, and their concerns, if any, regarding the privacy of their personal information. Respondents

---

1. These feelings of invasion into public online spaces have been well-documented in the press. *See, e.g.*, Michelle Slatalla, *omg my mom joined facebook!!*, N.Y. TIMES, June 7, 2007, *available at* http://www.nytimes.com/2007/06/07/fashion/07Cyber.html?_r=1&scp=3&sq=omg&st=cse.

2. The Canadian portion of this project was funded by the Privacy Commissioner of Canada's Contributions Program. The Canadian figures and their implications have been reported to the Privacy Commissioner of Canada in a report that was subsequently made available to the public. For the full report, see A. LEVIN ET AL., THE NEXT DIGITAL DIVIDE: ONLINE SOCIAL NETWORK PRIVACY (2008), *available at* http://www.ryerson.ca/tedrogersschool/privacy/Ryerson_Privacy_Institute_OSN_Report.pdf. This Article presents the aggregate results of the Canadian and American surveys.

also reacted to several hypothetical scenarios in which their privacy was breached on an OSN by measures both within and beyond their control.[3]

One theoretical assumption formulated as a possible response to the questions above, and underlying this research project, is the existence of two prevalent and competing formulations of privacy: one rooted in control and the other in dignity.[4] Of the two, the conception of privacy as control over who has access to one's personal information has, to date, been predominant and widely accepted in legal theory and analyses of information protection.[5] Both on and off-line, the degree of control over information is often the litmus test for privacy protection mechanisms.[6] Simply put, the greater the measure of control over personal information that is granted, the greater the degree of privacy protection. Personal information protection tools such as legislation, regulation, corporate policy, and technology are often evaluated in terms of the measure of control offered to individuals versus the personal information provided to another party, such as another individual or corporation.[7] Leading OSNs, such as Facebook and MySpace, propagate a notion of privacy as user control. Indeed, Facebook's credo on privacy states that "(1) You should have

---

3. The Canadian portion conducted several interviews with public and private sector organizations about their use of online social networks as well.

4. Philosophers and legal theorists have long debated the meaning and value of the concept of privacy. Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002). Throughout the second half of the twentieth century and into the twenty-first, leading thinkers have repeatedly attempted to categorize the multiple aspects, harms, and bases for privacy. Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006). In this Article, we focus on the two most prominent theories, which are dignity and liberty. *See, e.g.*, Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087 (2001); Daniel Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1094 (2002) ("Although the extensive scholarly and judicial writing on privacy has produced a horde of different conceptions of privacy, I believe that they can be discussed under six headings: (1) the right to be let alone; (2) limited access to the self; (3) secrecy; (4) control of personal information; (5) personhood; and (6) intimacy."); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity versus Liberty*, 113 YALE L.J. 1151 (2004).

5. W.A. Parent, *Privacy, Morality, and the Law*, *in* PHILOSOPHICAL ISSUES IN JOURNALISM 95 (Elliot D. Cohen ed., 1992) ("Indeed, definitions of privacy in terms of control dominate the literature.").

6. *See, e.g.*, OFFICE OF PRIVACY COMMISSIONER OF CANADA, YOUR PRIVACY RIGHTS: CANADA'S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT 2 (2004), *available at* http://privcom.gc.ca/information/02_05_d_08_e.pdf ("Your ability to control your personal information is key to your right to privacy.").

7. *See, e.g.*, OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER OF ONTARIO: WHEN ONLINE GETS OUT OF LINE – PRIVACY: MAKE AN INFORMED ONLINE CHOICE (2006), *available at* http://ipc.on.ca/images/Resources/up-facebook_ipc.pdf.

control over your personal information, and (2) You should have access to the information others want to share."[8]

However, online social networking poses a fundamental challenge to the theory of privacy as control. To understand why, consider a rather common case in which an online socializer is prudent about the information he discloses in his OSN profile. He avails himself of all of the heightened OSN privacy settings. Such a high degree of control would not preclude the possibility that another online socializer would post unflattering, defamatory, or personal information about him, and that this information would in turn be available to a large, if not unrestricted, online audience.

Personal information is broadly defined as information that identifies an individual or information about or relating to a person that most individuals in a given society at a given time do not want widely known about themselves.[9] It can be a concrete identifier, such as a social security number, or a subjective account of a wild night on the town. Many online socializers post personal information on OSNs and make it available to a large audience of "friends," seemingly without much concern over the loss of control. However, anecdotal evidence suggests that online socializers react with indignation when their personal information is accessed, used, or disclosed by individuals perceived to be outside their social network.[10]

One goal of this research project was to determine the dominant notion of privacy among online socializers. Is it based on human dignity, i.e., the interest individuals have in protecting their image and persona as it is comprehended by others? Or is it based on control over access to personal information? The results of this study should be particularly thought-provoking to theorists of online privacy. Perhaps their greatest value is in their implications on the future of cyberlaw and the law of reputation. The development of privacy protection in the law has been deeply affected by the many philosophical debates concerning theoretical foundations for privacy protection. It is clear that OSNs, with their rapid and widespread dissemination of personal information, and in particular, information about an individual that originates with a third party, have the potential to transform the law of reputation, and indeed the concept of

---

8. *See* Privacy Policy - Facebook, http://www.facebook.com/policy.php (last visited Apr. 9, 2009).

9. Parent, *supra* note 5.

10. *See, e.g.*, Leslie Ferenc, *Students Baffled*, TORONTO STAR, Feb. 13, 2007, *available at* http://www.thestar.com/News/article/181019.

reputation.[11] The question for legal scholars and courts is whether there can or should be an effective legal recourse for these privacy breaches.

Part I of this Article discusses the two notions of privacy as they are rooted in the values of "control" and "dignity," and as they are reflected in public policy and existing law. Part II introduces online social networking, distinguishing it from its offline counterparts. Part III presents the results of the empirical study. Part IV offers a reformulation of the traditional privacy foundations based on the stated preferences, behaviors, and concerns of online social networkers. By understanding the root of the new privacy formulation, law can address new privacy breaches when appropriate, as the Article suggests in the concluding Part V.

I. TWO WAYS OF THINKING ABOUT PRIVACY

Privacy has always been difficult to define. It seems that everyone wants it, but there is no consensus as to its meaning or value. Some philosophers have defined privacy as a function of accessibility to a person.[12] Prominent philosophers and legal minds have conceptualized privacy as being let alone.[13] Samuel Warren and Louis Brandeis were the most influential adopters of this notion in their 1890 Harvard Law Review article.[14] Others have defined privacy in terms of control over personal matters or information.[15] Still others have defined it in terms of values such as personhood, intimacy, social relationships, and secrecy.[16] While no unanimous or unitary

---

11. *See* DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (Yale Univ. Press 2007).

12. *See, e.g.*, ANITA L. ALLEN, UNEASY ACCESS: PRIVACY FOR WOMEN IN A FREE SOCIETY 15 (Rowman & Littlefield 1988) ("[P]ersonal privacy is a condition of inaccessibility of the person, his or her mental states, or information about the person to the senses or surveillance devices of others."); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 425–40 (1980) (defining privacy as a variable gradient in three dimensions: secrecy, anonymity, and solitude).

13. *See* Whalen v. Roe, 429 U.S. 589, 608 (1977); Time v. Hill, 385 U.S. 374, 412 (1967) (Fortas, J., dissenting); Katz v. United States, 389 U.S. 347, 350 (1967); WILLIAM DOUGLAS, THE RIGHTS OF THE PEOPLE (1958); Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 205-07 (1890).

14. Samuel Warren & Louis Brandeis, 4 HARV. L. REV. 205-07.

15. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (Antheneum 1967) (listing four "basic states of individual privacy": (1) solitude; (2) intimacy; (3) anonymity; and (4) reserve, which is "the creation of a psychological barrier against unwanted intrusion," and discussing the crucial role of individual control and decision making at each level.); *see also* Charles Fried, *Privacy*, 77 YALE L.J. 475, 482 (1968) ("Privacy is . . . the control we have over information about ourselves.").

16. *See, e.g.*, Solove, *supra* note 4.

definition of privacy exists, the concept governs interactions among members of society and between government and its subjects. Societies, informed by distinct historical and sociological influences, norms, and values, often adopt one conception of privacy over others. Their chosen definition of privacy tends to inform public policy and law. The two predominant conceptions of privacy as evidenced in modern Western legislation and legal analysis are privacy as control and privacy as dignity.[17] For example, American jurisprudence places great importance on the notion of privacy as control over personal information and the autonomy to decide with whom to share it. In contrast, European jurisprudence adopts dignity, or a human being's fundamental right to a private life, as a substantive legal value.[18]

A. Privacy as Control over Personal Information

One of the predominant privacy paradigms is based on control and autonomy.[19] Legal philosophers have long put forth autonomy as the core value of privacy. When individuals are allowed to act with autonomy and are treated as ends in and of themselves, their human rights, dignity, and liberty are assured. As legal theorist Stanley Benn philosophized, the individual is both a product and promoter of this choosing being.[20] His choice to keep certain matters private and make others public is critical to developing his identity as an autonomous person who freely chooses his own life projects.[21] Professor Richard Parker described privacy as "control over when and by whom the various parts of us can be sensed by others."[22] Privacy scholar Alan Westin described it as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[23] It is true that people often voluntarily barter away their privacy for many reasons, be they social (making friends), economic (getting a discount), professional (publicizing oneself), or practical (convenience, time-

17. *See* Whitman, *supra* note 4.

18. *See* Avner Levin & Mary Jo Nicholson, *Privacy Law in the United States, the EU and Canada: The Allure of the Middle Ground*, 2 OTTAWA L. & TECH. J. 357, 357-95 (2005).

19. *See, e.g.*, WESTIN, *supra* note 15; Richard Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 280 (1974).

20. Stanley I. Benn, *Privacy, Freedom, and Respect for Persons*, *in* NOMOS XII: PRIVACY 1, 10 (J. Roland Pennock & John W. Chapman eds., 1971).

21. *See id.* at 24.

22. Parker, *supra* note 19, at 281.

23. *See* WESTIN, *supra* note 15, at 7.

saving). The choice of whether and to what extent to engage in these privacy transactions is one that most people cherish and value highly.

Modern Western societies place great value in an individual's freedom to control his or her information, which means freely choosing who has access to it. Giving individuals control over personal information avoids the paternalistic dilemma that is often inherent in privacy regulation. A focus on the individual's control over information allows him to decide for himself what measure of privacy to grant certain topics. It can also relieve the burden of determining responsibility for certain perceived privacy breaches. For example, it is clear that the online socializer who posts embarrassing pictures of himself publicly and without heightened privacy settings is a victim of his own reckless behavior. By publicizing embarrassing information, he voluntary relinquished control—and a legally recognizable privacy right—over it.

Both in the U.S. and abroad, control and autonomy have become the theoretical foundation for many privacy laws and policies. As discussed below, two examples are the Fair Information Practices and U.S. privacy tort jurisprudence.

1. Fair Information Practices

Generally, the "privacy-as-control" approach has manifested in the area of personal information protection as a call for awarding individuals the greatest control possible over their personal information. This is reflected in what are commonly referred to as Fair Information Practices (FIPs).[24] The overall purpose of FIPs is to ensure that an individual will maintain control over his personal information when it is in the hands of an organization.[25] FIPs provide an individual with the necessary information about an organization's information collection practices so that he may make an informed decision whether or not to divulge his personal information.[26]

---

24. FIPs were first defined in the U.S. in *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973). There are five American FIPs: Notice/Awareness; Choice/Consent; Access/Participation; Integrity/Security; and Enforcement/Redress. *See* FEDERAL TRADE COMMISSION, FAIR INFORMATION PRACTICE PRINCIPLES (2007), *available at* http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

25. Accordingly, some would argue that "control" is a notion of how privacy should be managed, rather than a conceptual basis for privacy. William McGeveran, *Comment,* Vanderbilt 2008 Intellectual Property Roundtable. The authors are grateful to William McGeveran for this point.

26. It should be noted that the US FIPs obligate the federal government but are only a recommendation to the private sector. *See supra* note 24. In contrast, in many other

Similarly, FIPs attempt to ensure that an individual has control not only over the initial act of supplying the personal information, but also over later stages of interaction with the website. In this manner, FIPs provide individuals the option to monitor the use, disclosure, and retention of their personal information. An individual can also verify the accuracy of the information collected about him and help monitor the organization's actions.[27]

Personal information protection regimes based on FIPs distinguish implicitly between personal information that is supplied to an organization directly by the individual and personal information about the individual that is collected or supplied by third parties. The idea of control applies mainly to personal information that is supplied directly by the individual, and less to personal information provided about an individual by others.[28]

2. The U.S. Tort of Public Disclosure of Private Facts

The American tort of public disclosure of private facts safeguards the aggrieved whose true, but private, information is widely disseminated in an unsanctioned manner.[29] The tort is designed to give redress to the victim whose reputation or dignity has been injured unjustifiably by the revelation of truthful information. Its elements require the plaintiff to prove that the defendant publicized a private fact that was not of legitimate public concern, where such disclosure was highly offensive to a reasonable person.[30] The success of this cause of action hinges on an assessment of the reasonableness of the victim's expectation of privacy in the space invaded or information disclosed.[31] This determination is highly dependent on the nature of the space or information invaded, the

---

jurisdictions, such as the EU Member States, FIPs obligate private sector organizations as well. *See infra* note 63.

27. The degree of organizational adherence to the FIPs varies, and with it the degree of control offered to individuals. *See e.g.*, OFFICE OF THE PRIVACY COMMISSIONER OF CANADA: CANADIAN BUSINESSES AND PRIVACY-RELATED ISSUES (2007) *available at* http://privcom.gc.ca/information/survey/2007/ekos_2007_01_e.asp.

28. It is perhaps not always desirable that an individual have control over his personal information that was provided by others, and privacy interests should probably be weighed against other interests, such as financial, economic or health-care interests, before a legislative or regulatory decision on the level of control is reached. For example, an individual's objection on privacy grounds to information included on their credit history is not as important as its accuracy. *See e.g.* GRAMM-LEACH-BLILEY FINANCIAL SERVICES MODERNIZATION ACT Pub. L. No. 106-102, Stat. 113 (1999).

29. RESTATEMENT (SECOND) OF TORTS § 652D (1977).

30. *Id.* § 652B, 652D.

31. *See id.* § 652D cmt.c.

circumstances surrounding the breach, and the prevailing social norms.[32]

The definition and judicial interpretation of the public disclosure tort espouse a control-related view of privacy. Many courts have held that once the plaintiff relinquishes or loses control of the presumptively private information, the information is no longer protectable as "private."[33] An individual could lose control of his information either because he voluntarily disclosed it or because the information was already publicly available, viewable, or generally known. Indeed, the law does not protect privacy in public places, even when the information is sensitive in nature.[34]

These control-based limitations are rooted in legitimate public policy considerations. The burden to protect sensitive information is logically placed on the invaded victim before an invasion occurs. Only plaintiffs who have maintained control over their information—by drawing their blinds or not sharing their secrets—can be vindicated. A control-based limitation also ensures that the tort does not unduly restrict the free flow of truthful information. A privacy regime that assumes that control over information is dispositive to its free transfer is more likely to tip the scales in favor of freedom of speech.

From a practical perspective, control-based limitations are a palatable solution to the conundrum faced by a judge assessing the merits of a privacy claim. The assessment as to whether the plaintiff lost or relinquished control over the information is more easily ascertainable than if he was ashamed or disrespected.

---

32. *See* Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J. L. & TECH. 1, 13 (2007).

33. RESTATEMENT (SECOND) OF TORTS § 652D (1977); *see also* Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 668-69 (Cal. Ct. App. 1984) (holding that the fact that the plaintiff had confided to a group of people that he was a homosexual vitiated the matter's privacy); Nader v. General Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) ("Information about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff."); Wilson v. Harvey, 842 N.E.2d 83, 91 (Ohio Ct. App. 2005) (concluding that dissemination of the plaintiff's contact information on a flyer was not an invasion of privacy because the information circulated was on the university's website and accessible to anyone).

34. RESTATEMENT (SECOND) OF TORTS § 652C (1977) ("No one has the right to object merely because his name or his appearance is brought before the public, since neither is in any way a private matter and both are open to public observation."); *see also* Castro v. NYT Television, 851 A.2d 88, 97 (N.J. Super. Ct. App. Div. 2004); Sánchez Abril, *supra* note 32.

In sum, the public disclosure tort prohibits certain disclosures based on the control the claimant exercised over the information in question, not the indignity suffered or the intimacy breached.[35]

For some time, U.S. tort law has wrestled with the elusive line delineating when information ceases to be private.[36] Some commentators have advocated for a contextual analysis of the disclosure to assess whether disclosed information is worthy of privacy protection.[37] The question now facing privacy scholars is whether a disclosure online—where networks are even more dynamic, intimacy is diluted, and technology allows for easier and more widespread dissemination—precludes privacy.

B. Privacy as Dignity

Some defend the need for privacy as a matter of human dignity.[38] It is this aspect of privacy that is at the heart of Warren and Brandeis's landmark privacy article. Threatened by "the intensity and complexity of life" and "recent inventions and business methods," the pair noted, "solitude and privacy have become more essential to the individual."[39] The law, they advocated, must protect privacy on the principle of an "inviolate personality."[40]

Since the time of Warren and Brandeis, much has been written about a right to privacy based on human dignity. Edward Bloustein's theory of privacy is grounded on this notion.[41] While conceding it difficult to elaborate a positive description of privacy, Bloustein contended that all privacy interests share one value: respect for individual dignity, integrity, and independence.[42] One's moral personality, according to Professor Bloustein, defines one's essence as

---

35. RESTATEMENT (SECOND) OF TORTS § 652D (1977) (noting the relation of § 652D to the First Amendment to the Constitution); *see also* Arrington v. New York Times Co., 434 N.E.2d 1319, 1322 (N.Y. 1982); Wilson, 842 N.E.2d at 91.

36. Professor Daniel Solove has observed that U.S. law equates privacy with complete secrecy and that "a privacy violation occurs when concealed data is revealed to others. *See* Solove, *infra* note 103, at 497 If the information is not previously hidden, then no privacy interest is implicated by the collection or dissemination of the information." *Id.* Many commentators have noted that interpreting privacy as dependent upon complete secrecy obliterates the concept. *Id.*

37. *See* Sánchez Abril, *supra* note 32.

38. *See, e.g.*, Warren & Brandeis, *supra* note 14; Whitman, *supra* note 4.

39. Warren & Brandeis, *supra* note 14.

40. *Id.*

41. Edward Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U. L. REV. 962, 971 (1964).

42. *Id.*

a human being.[43] A privacy violation leaves a person open to public view and scrutiny. This unauthorized nakedness in the face of the world renders a person and his sense of self vulnerable in a way that is a fundamental affront to human dignity.[44] Noted scholar Charles Fried conceptualized privacy in terms of social currency. Sharing private information, he argued, forms the basis for intimate relationships of friendship, love, and trust.[45] Without privacy, an individual would not be able to nurture his interpersonal relationship and his own identity.[46]

A dignity-focused view of privacy emphasizes the development of one's personality and inner self.[47] In this view, privacy encompasses the right of an individual to keep certain aspects of his life unknown to others, and thereby construct different "situational personalities."[48] In so doing, the individual maintains several public personas, each accessible by different constituencies and in different contexts. Each demonstrates the attributes the individual considers appropriate and desirable for each constituency. It is no wonder that the etymology of the words "person" and "persona" stems from the Latin *persona*, meaning, among other things, a theatrical role.[49] An individual's inability to freely manage disclosure of his multiple personas has profound social consequences. For example, an individual may wish to keep his level of religious devotion hidden from his employer for fear that these may hinder a promotion.

The conception of privacy as dignity has had a great influence on privacy law and policy. A prominent example is the case of European legal regime.

1. Dignity in the European Legal Regime

Europeans have long considered the privacy of personal information to be a fundamental right.[50] Historically, the right to

---

43. *Id.*

44. *Id.*

45. CHARLES FRIED, AN ANATOMY OF VALUES: PROBLEMS OF PERSONAL AND SOCIAL CHOICE (Harvard Univ. Press 1970).

46. *Id.* at 140.

47. Social scientists have long described this as an intrinsic human need. *See, e.g.*, ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (Doubleday 1959).

48. *Id.*

49. CHARLTON T. LEWIS & CHARLES SHORT, A LATIN DICTIONARY (Revised ed., Oxford Univ. Press 1956) *available at* http://artfl.uchicago.edu/cgi-bin/philologic/getobject.pl?c.7:2266.lewshort.

50. For an excellent comparison on European and American views of privacy, see Whitman, *supra* note 4.

"dignity" and "honor" was initially reserved for the aristocracy, perhaps as a way for the nobility to maintain public appearances despite private indiscretions.[51] Developing primarily in France and Germany, the legally recognized right to a private life protects the creation and maintenance of personal identity, intimacy, and community.[52] Warren and Brandeis observed that "the right to privacy. . . has already found expression in the law of France,"[53] in contrast to its relatively feeble American counterpart.[54]

Today, an individual's privacy in Europe is protected under the European Convention on Human Rights, which requires the government to respect individuals' privacy and private family lives.[55] Under Article 8, the European Convention on Human Rights states that "[t]here shall be no interference by a public authority with the exercise of his right [to private life] except such as is in accordance with the law."[56] The Convention ensures a European citizen the right to respect for "his private and family life, his home and his correspondence."[57] The fundamental right to privacy has been incorporated into the laws of EU member states. As one English court commented in a privacy case,

> [t]he law now affords protection to information in respect of which there is a reasonable expectation of privacy, even in circumstances where there is no pre-existing relationship giving rise to an enforceable duty of confidence. That is because the law is concerned to prevent the violation of a citizen's autonomy, dignity, and self-esteem.[58]

Similarly, the constitutions of several European nations recognize rights to human dignity,[59] to informational self-determination, to free development of one's personality,[60] and to

---

51. *See* Warren & Brandeis, *supra* note 14.

52. Whitman, *supra* note 4.

53. *Id.*

54. *See* discussion *infra* I.B.2 (discussing limitations of the U.S. privacy torts).

55. European Convention on Human Rights. art. 8, Nov. 4, 1950, 213 U.N.T.S. 221.

56. *Id.*

57. *Id.*

58. Max Mosley v. News Group Newspapers Limited, [2008] EWHC 1777 (QB) Case No: HQ08X01303 (July 24, 2008) at [7].

59. *See, e.g.*, GRUNDGESEZ [GG] [Constitution] art. 1 (F.R.G.) (discussing the right to human dignity); *see also* DONALD P. KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 323, 324-25 (2d ed., Duke Univ. Press 1997) (discussing the Census Act Case).

60. GRUNDGESEZ [GG] [Constitution] art. 2.1 (F.R.G.) (providing for the right to free development of one's personality).

respect for private life.[61] The current draft of the European Constitution echoes these dignitary values.[62]

Dignity is thus the theoretical basis for privacy protection in Europe. As a result, European laws are very protective of personal privacy in many areas, from consumer rights, as exemplified by the EU Directive that establishes data protection for Europeans in all their commercial transactions worldwide,[63] to discovery in civil litigation.[64] For example, in the well known "Nikon Case" the Supreme Court of France decided that the French Labor Code prevented an employer from presenting an email message sent by an employee as evidence in support of the employee's termination, on the grounds that the message was private even though the employee was emailing "the competition" using the employer's computer.[65]

The right to a private life in Europe has expanded to include all levels of social class and celebrity.[66] Unlike the U.S., most European jurisdictions recognize that an individual's status as a well-known public figure does not deprive him of privacy rights.[67] A controversial 2008 case from England highlights the prominent role of dignity as a privacy value in Europe. In 2007, a British tabloid, *The News of the World,* published a salacious article about Max Mosley, the president of the world governing body for motor sports. The article was entitled "F1 Boss Has Sick Nazi Orgy with 5 Hookers"[68] and was accompanied by various images and an online video depicting the executive engaged

---

61. *See, e.g.*, CC decision no. 2004-499 DC, July 29, 2004, Rec. 2. In France, the respect for private life is recognized as one of the liberties protected under Article 2 of the Declaration of the Rights of Men and Citizens of 1789, which is considered part of the French Constitution of 1958 by virtue of the reference to the Declaration in the preamble to the Constitution. *Id.*

62. *See* EU Draft Constitution, § I-2: The Union's Values, *available at* http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/c_310/c_31020041216en00110040.pdf (last visited Apr. 9, 2009).

63. European Union Directive 95/46EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data.

64. Whitman, *supra* note 4, at 1156.

65. Arret 4164, Cour de Cassation – Chambre Sociale, 2001, *available at* http://www.courdecassation.fr/agenda/arrets/arrets/99-42942arr.htm.

66. *See, e.g.*, Stuart Goldberg, *The Contest for a New Law of Privacy: A Battle Won, a War Lost? Campbell v. Mirror Group Newspapers Limited*, 9 COMM. L. 122 (2004); M.A. Sanderson, *Is Von Hannover v. Germany a Step Backward for the Substantive Analysis of Speech and Privacy Interests?*, 6 EURO. HUM. RTS. L. REV. 631 (2004); Lorna Skinner, *You're a Celebrity, Madam: So do we Have a Right to Share Your Privacy in a Public Place?*, 9 COMM. L. 118 (2004).

67. Huw Beverley-Smith, et. al., PRIVACY, PROPERTY AND PERSONALITY, 224 (Cambridge University Press, 2005).

68. Max Mosley v. News Group Newspapers Limited, [2008] EWHC 1777 (QB) Case No: HQ08X01303 (July 24, 2008) at [1].

in allegedly Nazi-themed sado-masochistic and sexual activities with various prostitutes.[69] The tabloid had equipped one of the participants with a hidden camera and promised her £25,000 for the video.[70] Mr. Mosley sued the newspaper for invasion of privacy and won £60,000 in compensatory damages, an unprecedented amount in a case of public disclosure. The English High Court found that there was no evidence supporting the published allegations that the sexual encounter had a Nazi motif.[71] Even though Mr. Mosley was a well-known public figure, neither his adultery nor his unconventional sexual activities were legitimately newsworthy in the eyes of the court.[72] In the opinion, Mr. Justice Eady stressed dignity as the core function of the cause of action. He cautioned against moral highhandedness as incompatible with protecting dignity.

> It is not for journalists to undermine human rights, or for judges to refuse to enforce them, merely on grounds of taste or moral disapproval. Everyone is naturally entitled to espouse moral or religious beliefs to the effect that certain types of sexual behavior are wrong or demeaning to those participating. That does not mean that they are entitled to hound those who practice them or to detract from their right to live life as they choose.[73]

The court also highlighted untoward or unconventional behavior should not negate the law's protection of dignity.

> One should be careful not to dismiss matters going to personal dignity because a particular sexual activity or inclination itself may seem undignified. After all, sexual activity is rarely dignified. That is far from saying, however, that intrusions into a person's sexual tastes and privacy cannot infringe the right to dignity protected by Article 8.[74]

In determining monetary damages to compensate Mr. Mosley, the High Court weighed the gravity of the indignity and the fact that "[i]nvasion of privacy can never be repaired and the claimant has to live with it for the rest of his life."[75] The court justified the award of damages with meticulous logic, arguing that "the scale of distress and indignity in this case is difficult to comprehend. It is probably unprecedented."[76] Such a scale necessitated vindicating monetary damages "to mark the fact that . . . [an] individual has taken away or undermined the right of another – in this case taken away a person's

---

69. *Id.*
70. *Id.*at [5], [65].
71. *Id.* at [44]-[65].
72. *Id.* at [233].
73. *Id.* at [127].
74. *Id.* at [215].
75. *Id.* at [124]-[134].
76. *Id.* at [216].

dignity and struck at the core of his personality."[77] By solidly anchoring privacy rights in terms of dignity, European jurisprudence continues to diverge from the U.S. model of control and autonomy.

II. PERSONAL INFORMATION ON ONLINE SOCIAL NETWORKS

An online social network can be defined as any website whose main purpose is to act as a connector among users. Online socializers create personalized profiles within a "community." These profiles represent the individual in cyberspace and interact with the profiles of other users. In some important ways, OSNs are fundamentally different from offline or traditional social networks.Several relevant features of OSNs merit discussion.

OSNs have traditionally been a forum for the younger generation. Marketing research demonstrates that only 10 percent of online socializers are older than 55 years old, and close to 50 percent of online socializers are younger than 35.[78] The young age of many online socializers combined with the permanence and infinite transferability of misguided online revelations worry some parents and educators.[79] Aside from cyber-stalking and cyber-bullying, risks of online disclosure and socialization include reputational risks and identity theft, among others.[80] While these are a common concern to all Internet users, they may be more of a threat to online socializers due to their increased and enhanced online presence. News reports chronicling OSN privacy debacles are nearly as common as public service announcements cautioning prudence online.[81] Parents, educators, and others anguish over the future of civility and privacy in a seemingly transparent world.

There are a variety of possible explanations as to why many online socializers seem to ignore risks related to the disclosure of their

---

77. *Id.* at [216].

78. Press Release, More than Half of MySpace Visitors are Now Age 35 or Older, as the Site's Demographic Composition Continues to Shift (Oct. 5, 2006), *available at* http://www.comscore.com/press/release.asp?press=1019.

79. *See, e.g.*, ENVIRONICS RESEARCH GROUP, YOUNG CANADIANS IN A WIRED WORLD (2001), *available at* http://www.media-awareness.ca/english/resources/special_initiatives/survey_resources/students_survey/yciww_students_view_2001.pdf (last visited Apr. 9, 2009).

80. *See* Wendy Cukier & Avner Levin, *Spam and Internet Fraud, in* CRIMES OF THE INTERNET (Frank Schmalleger & Michael Pittaro eds., 2008).

81. *See, e.g.*, Posting of Marshall Kirkpatrick to Read Write Web, (*Facebook Security Lapse Leaves Private Photos Exposed, Even Paris and Zuck's*) http://www.readwriteweb.com/archives/facebook_security_lapse_private_photos.php (Mar. 24, 2008, 18:45).

personal information online. Like Hesiod, many simply fault the foolishness of youth. Online socializers, many argue, may be oblivious to the reputational risks to which they are exposing themselves. In other words, they do not have the capacity to foresee the shame they could bring upon themselves.[82] The reputational risks may only become relevant when young OSN participants seek employment or enter the workforce. The tendency of 15 to 24 year-olds to engage in high risk behavior in spite of clearly identified risks is well-established in both the crime and medical literature.[83] Another common explanation for young people's apparent disregard for traditional privacy norms is a lack of knowledge regarding the technology.[84] Young online socializers, this argument goes, do not realize that they cannot take information down, or that it can be accessed, used, or altered by a third party. This argument, however, ignores the fact that the majority of online socializers grew up online and are perhaps more net-savvy than previous generations.

A second distinctive quality of OSNs is the nature of the interpersonal relationships they foster. The relationships between members of an offline social network differ from those on networks based solely online. Often, offline social networks are relatively small in size in comparison with their online counterparts. [85] In contrast, online social networks can consist of a vast system of connections, some of which are so weak that they would be nonexistent offline. OSNs have loosened traditional notions of intimacy and friendship and their respective nomenclature.[86] The terminology applied to other socializers with access to all or part of an individual's online persona (both MySpace and Facebook refer to all socializers as "friends") is meaningless. Indeed, the making of "friends" online for the sake of

---

82. *See* J. Kimberly et al., *Linking Youth Internet and Conventional Problems: Findings From a Clinical Perspective*, 2 J. AGGRESSION, MALTREATMENT & TRAUMA 15, 39-58 (2007) (providing possible biological reasons).

83. *See, e.g.*, J. Grunbaum et al., *Youth Risk Behavior Surveillance – United States, 2004*, MORBIDITY & MORTALITY WKLY. REP., May 21, 2004, *available at* http://www.cdc.gov/mmwr/preview/mmwrhtml/ss5302a1.htm.

84. *See* CAVOUKIAN, *supra* note 7.

85. See Strahilevitz, *infra* note 110, for more on the relationships within networks, the terminology used with respect to socializers, and the legal implications.

86. *See* Joel Garreau, *Friends Indeed?*, WASH. POST, Apr. 20, 2008, at M01; *see also* James Randerson, *Warning: You Can't Make Real Friends Online,* GUARDIAN (London), Sept. 11, 2007, Final Edition at 9, *available at* http://www.guardian.co.uk/technology/2007/sep/11/facebook.myspace?gusrc=rss&feed=technology.

mere accumulation of a large number of "friends" as a status symbol is a growing online social phenomenon in itself.[87]

Finally, OSNs are usually for-profit businesses. The computer servers on which the website is hosted, as well as any intellectual property related to the OSN, are usually the property of the OSN.[88] As profit-motivated businesses, OSNs have the fundamental objectives of reducing liability and attracting as many members as possible. Although their members do not pay dues, they have a loose contractual relationship with the OSN provider in the form of the OSN's terms of service. OSN providers act as the hub for all of their members' information and contacts. Their consumers are a relatively captive audience. The costs involved in transferring to a competing OSN are high. This would likely involve forfeiting all posted information, photographs, and possibly contacts. Therefore, OSNs do not have significant incentives to cater to the needs and requests of their members.[89]

OSN providers control the rules of the game on an OSN through technology, privacy policies, and terms of service. Thus, the OSN is the legislator, judge, police, and sometimes defendant in privacy-related complaints. It stands to reason, therefore, that most OSN terms of service and privacy policies are clearly established according to the theory of privacy as control.[90]

The personal information protection framework of online socializers is summarized by an OSN's terms of service (i.e., its contracts with members).[91] Both MySpace and Facebook prohibit their members from engaging in a variety of activities, such as use of their accounts for profit or for posting information that is privacy-invasive or generally harmful to others. Facebook allows users to post photos of their "friends," while MySpace allows users to post information about others with their "consent." The terms "friends,"

---

87. *See* Paul Giordano, *How To Get A Lot of Friends on MySpace*, EZINE ARTICLES, http://ezinearticles.com/?How-To-Get-A-Lot-Of-Friends-On-MySpace&id=270277 (last visited Apr. 9, 2009) (instructing socializers on ways to accumulate "friends" and describing accelerated MySpace "friend adding" software).

88. For a detailed discussion on intellectual property and user-generated content see the other articles in this special issue of the *Vanderbilt Journal of Entertainment and Technology Law*.

89. Despite the incentives to the contrary, Facebook has responded favourably to the most vociferous member complaints.

90. *See* Privacy Policy – MySpace.com, http://www.myspace.com/index.cfm ?fuseaction=misc.privacy (last visited Apr. 9, 2009).

91. *See, e.g.*, Terms and Conditions – MySpace.com, http://www.myspace.com/index .cfm?fuseaction=misc.terms (last visited Apr. 9, 2009); Terms of Use – Facebook.com, http://www.facebook.com/terms.php (last visited Apr. 9, 2009).

"consent," and "privacy-invasive" are not defined in the contracts.[92] OSNs avoid any responsibility, legal or otherwise, for the actions of other users. MySpace explicitly states:

> You are solely responsible for your interactions with other MySpace.com Members. MySpace.com reserves the right, but has no obligation, to monitor disputes between you and other Members.[93]

Facebook is equally forceful:

> You are solely responsible for your interactions with other Facebook users. We reserve the right, but have no obligation, to monitor disputes between you and other users.[94]

These statements are in addition to the usual disclaimers and limitation of liability terms found in such contracts. Both networks encourage their members to report breaches of their terms and conditions, but offer no formalized process for dispute resolution or other recourse to members. The protection of privacy for both networks is, therefore, closely associated with control over personal information rather than the protection of the dignity of online socializers.[95]

Privacy policies are similarly infused with the theme of control. MySpace's privacy policy has sections devoted to information collection, use, and disclosure by MySpace. It also contains several other sections that explain to its members how their staff may control the information provided to MySpace. The policy makes no reference to unauthorized disclosures of personal information at the hands of another online socializer.[96]

Facebook has collaborated with the Information and Privacy Commissioner of Ontario to publish guidelines on privacy in an online social network.[97] The guidelines unequivocally state: "remember that you are ultimately responsible for determining what information you share with others."[98] The guidelines also ask: "Have you made informed choices?"[99] The guidelines provide readers with several examples of how Facebook offers socializers the possibility of making informed choices so that they are able to maintain control over their

---

92. *Id.*

93. *Id.*

94. *Id.*

95. *Cf.* Part B (discussing OSN confidentiality agreements as evidenced by PatientsLikeMe.com).

96. *See infra* I.B.

97. CAVOUKIAN, *supra* note 7.

98. *Id.* at 2.

99. *Id.* at 5. Informed choices are necessary for meaningful consent—one of the more important FIPs.

personal information. Indeed, as mentioned above, Facebook's privacy policy states explicitly that it is based on two principles: "(1) You should have control over your personal information, (2) You should have access to the information others want to share."[100] Like MySpace's policy, Facebook's policy does not address the circumstances in which one user discloses the information of another.

The OSN's focus on privacy-as-control begs the question: do OSN members accept this formulation of privacy rooted in control?

III. THE SURVEY AND FINDINGS

The findings reproduced here are part of a larger research project regarding the basic questions of online conduct and OSN use.[101] Only the findings relevant to the topic of this Article—the two notions of privacy online—are discussed below.[102] The first part of the survey pertained to the usage of OSNs. Questions included the frequency of usage, content on respondents' profiles, general expectations of privacy, knowledge of privacy policies, usage of tools afforded by the network to restrict access and enhance privacy, etc. These questions were close-ended, and respondents chose from a list of various answer choices in multiple choice and Likert scale format. In addition, the 2,500 respondents were asked to complete two open-ended questions to indicate their primary concern regarding OSNs, if any, in relation to their personal and professional lives.

The second part of the survey posed four different scenarios. These four scenarios depicted issues that could arise from use of the network and/or privacy breaches within the network. Respondents were asked whether they had personal experience with the scenario, whether they had heard of the scenario happening to others, their thoughts on the potential harm generated by the scenario, who they thought was responsible for the harm caused by the scenario, as well as other questions specific to each scenario. The following are the scenarios posed to the respondents.

Scenario 1: Relationship Breakup

"You have just broken up with your significant other. You are shocked to see that the day after the breakup, your previous significant other posted compromising and what you thought were very private

100. *See* Privacy Policy - Facebook, *supra* note 8.

101. *See infra* Appendix A (providing survey methodology).

102. *See also* LEVIN, *supra* note 2, at 1.

pictures of you on the social network. In addition, this person posted nasty comments that painted a very negative picture of you as a person. As a result, some people whom you thought were your friends have dropped you, and you are no longer included in social events."

Scenario 2: Party Time

"It was your birthday, and you went out with friends for a night on the town. You had a wonderful time, drank way too much, and really can't remember most of the evening. The next day you see pictures of your escapades posted on one of your friend's pages and tagged to you. Your family members see these pictures, are very upset with you, and say they can no longer trust you."

Scenario 3: False Charges

"Anonymous comments circulate on an online social network about your having been arrested for shoplifting. This is not true, and you are shocked to see that these comments have made the rounds to all your friends. No matter what you say, everyone believes you are a shoplifter."

Scenario 4: Sick Leave

"You called in sick to work, because you really wanted to go to your friend's all day graduation party. The next day you see several pictures of you having a great time at the party. Because the pictures are dated, you start to worry about whether you might be caught in your lie about being sick. You contact the developers of the social network and ask that the pictures be taken down because the tagging goes so far, it would take you too long to find all the pictures. There was no response from the network. You are stunned to be called in by your supervisor a week later to be advised that you were being "written up" for taking advantage of sick leave and put on notice that if it happened again you would be terminated."

The findings have been organized into three groups: (1) General Behavior and Perceptions, (2) Control, and (3) Dignity. Note at the outset that the questions asked did not refer directly to the notions of dignity and control, but rather asked respondents indirectly about their sense of harm and who they held accountable. As such, the findings presented below lend themselves to a wide range of interpretations and conceptual privacy frameworks. Hopefully others

will take the opportunity to advance their understanding of privacy online on the basis of the data below.[103]

A. General Behavior and Perceptions

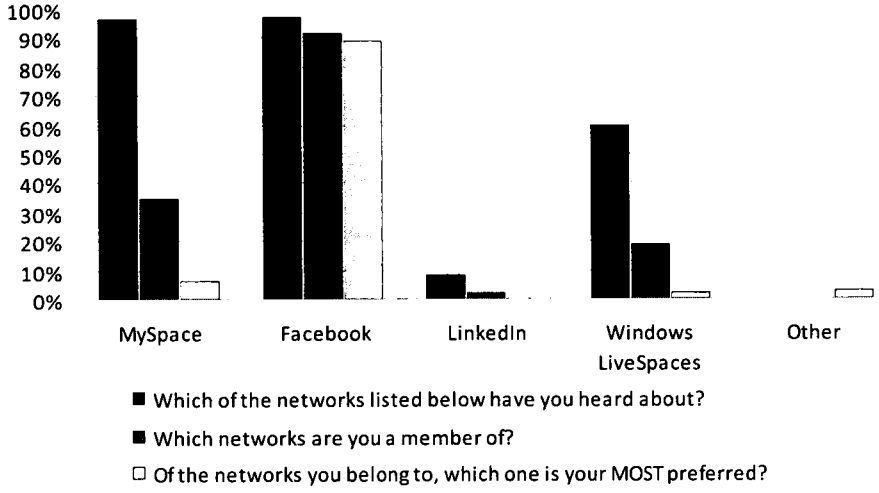
1. The Majority of Respondents Selected Facebook as Their Preferred OSN

Respondents predominantly reported being members of Facebook and MySpace, with 92 percent of the group representing Facebook members and 35 percent representing MySpace members. Of the respondents, 90 percent stated that Facebook was their most preferred OSN, whereas only 6 percent reported that MySpace was their preferred OSN. These findings, collected from students currently enrolled in universities, are consistent with general observations of Facebook demographics. As other commentators have affirmed, Facebook users tend to be college students or those interested in college, while MySpace users include a much wider audience.[104]

103. Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006).

104. Danah Boyd, Viewing American Class Divisions Through Facebook and MySpace, *Apophenia Blog Essay*, June 24, 2007, http://www.danah.org/papers/essays/ClassDivisions.html (observing that Facebook originally launched as a college-only site and has continued to attract college and graduate students, former college and graduate students, and high school students interested in college).

Figure 1: Preferred OSNs[105]



2. Respondents Post a Significant Amount of Truthful Information about Themselves

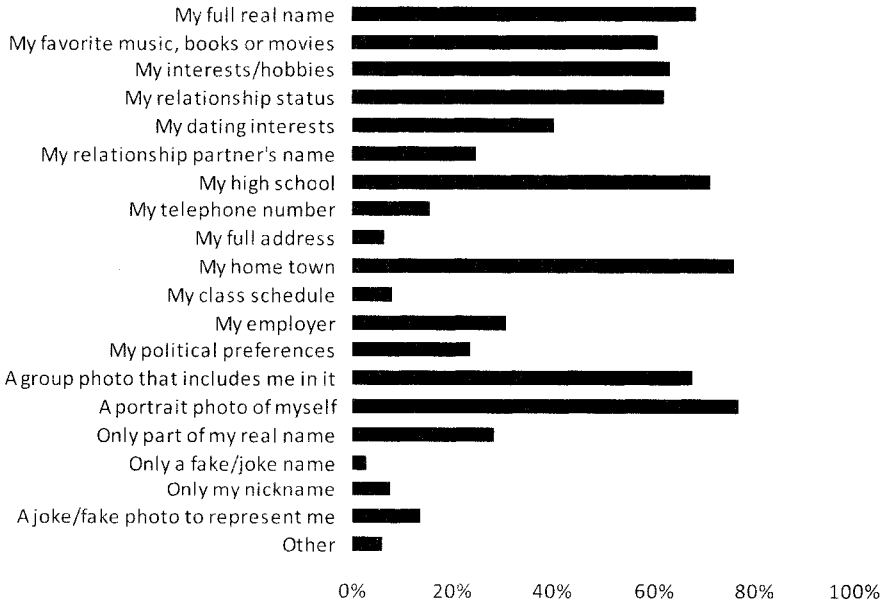
Over 50 percent of OSN users surveyed stated that their profiles contain their real full name, home town, high school, relationship status, interests, hobbies, favorite music, books, movies, and a picture of themselves. The most often-posted piece of information was a portrait photo, with 77 percent of users reporting that they posted a picture of themselves. This was followed by the user's hometown (76%) high school (72%) and real full name (68%). These high frequencies may indicate that the majority of OSN users surveyed are logging on to genuinely socialize with former classmates or past acquaintances.

Only 3 percent of those surveyed claimed to use a fake or joke name as opposed to a real, full, or partial name; 14 percent claimed to have posted a fake or joke photo to represent themselves. Posting fake names or pictures could be a privacy-protective mechanism for the user to participate in the network (and perhaps gain access to others) without being readily identifiable. It could also signal someone who has multiple accounts and operates under different personae in different networks. Aside from these, the three items OSN users reported posting least were: telephone number (16%), class schedule (8%), and full address (6%).

105. Questions listed in the Figures are taken verbatim from surveys.

In addition to posting a considerable amount of information, online socializers are also truthful in the information they post. Despite the fact that respondents share a significant amount of information on their OSN profiles, they are selective in the information they post. The results indicate that respondents are able to distinguish between personal information that allows them to socialize safely with other users of the network (such as hobbies and favorite books and movies) and information that could be potentially dangerous in the hands of a stranger (such as an address or telephone number). Posting truthful information is consistent with an intent to socialize.

Figure 2: Extent of Information Included on Social Network Profile[106]



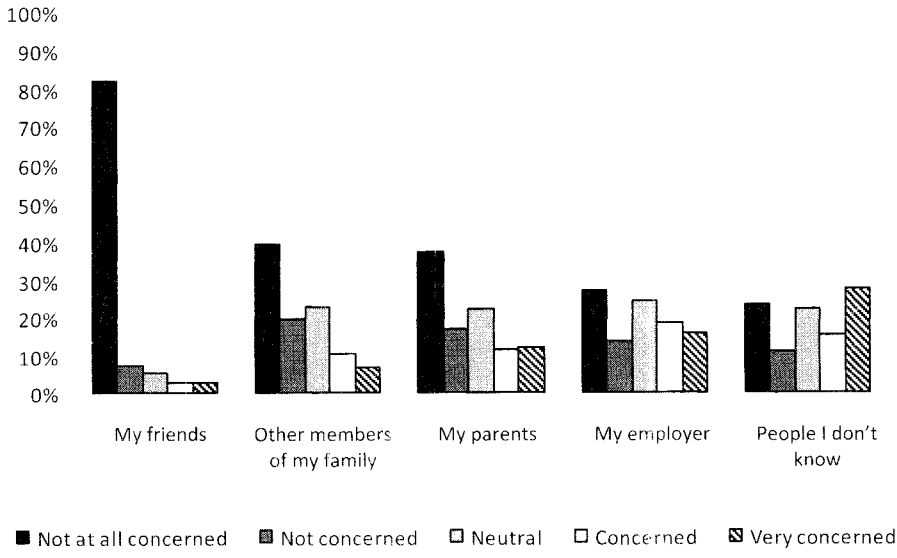
2. Respondents Perceive the Information They Share on OSNs as Intended Only for Members of Their Network

OSN users surveyed experience different levels of concerns depending on the social group that accesses their information. For example, 90 percent of users are not concerned when their friends access their profiles, whereas 24 percent reported being concerned or

106. This Figure is based on the surveys conducted by Acquisti & Gross, *infra* note 112.

very concerned with the possibility of their parents viewing their online profiles. Users also expressed concern about an employer accessing or viewing the information they post online. Nearly 35 percent of users expressed that they would be either concerned or very concerned if their employer accessed their online profiles. Overall, online socializers reported being most concerned about strangers accessing their profiles. Nearly half of all OSN users surveyed (43%) were concerned or very concerned about stranger access. This data suggests that OSN users intend the information they share online primarily for their peers.

Figure 3: Level of Concern About Access to OSN Information: Access by Specific Groups of People



The Party Time scenario involves a situation in which family members of the OSN user access information that was not intended for them to see. As can be seen in the following two figures, the majority of respondents considered this a breach of privacy. Of respondents, 67 percent stated that they were more upset about family versus acquaintances seeing their pictures, and 54 percent believed that it is wrong for people to access information that is not intended for them.

Figure 4: Access by Family versus Acquaintances
"I get more upset about my family seeing compromising pictures of me than if acquiantances see them."

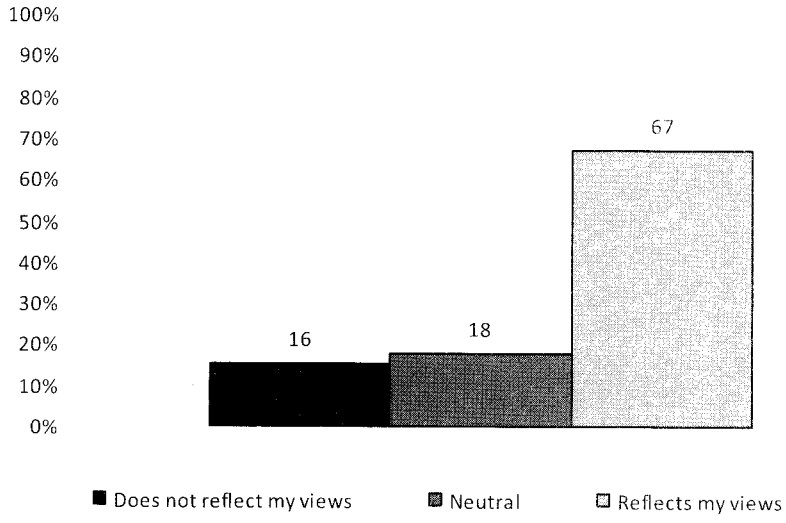
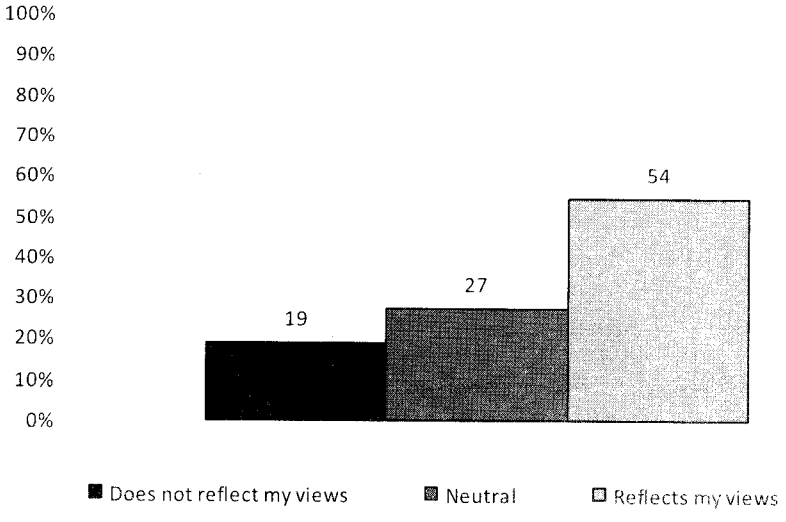


Figure 5: Access by Unintended Audiences
"It is not right when people can have access to information not intended for them."



3. Scenarios Resemble Urban Myths —Very Few Respondents Suffer Actual Harm, Yet Many Appear Aware of Unauthorized Disclosures

Of the four scenarios, the one that respondents personally experienced the most was Party Time, the scenario in which compromising alcohol-related pictures were leaked to family members. Still, only 8 percent said that it had happened to them. However, 65 percent of respondents had heard of Party Time occurring and 18 percent said that it happened to someone they knew personally. This is not surprising, since this example is often discussed in popular culture and in the academic press.[107] Similarly, although only 3 percent of respondents reported being personally involved in a situation like Relationship Breakup, the scenario in which a disgruntled ex-significant other posts compromising and private pictures on the OSN, 59 percent have heard of it happening to someone else. Again, this is unsurprising since media stories abound of such events as well.[108] Four percent of respondents reported being personally involved in a situation like Sick Leave, the scenario in which an employer caught an employee in a lie via an OSN, although slightly less than half (42%) claimed to have heard of it happening. False Charges, the scenario in which an OSN user is defamed as a shoplifter, was the least common. It occurred with least frequency, with only 2 percent of respondents reporting that it had happened to them. These results raise an interesting question, which is beyond the scope of this Article, regarding the role of the media in the creation and perception of harms and risks of online activities and online socializing. The following four pie figures display the perceptions of respondents in graphic form for each scenario.

---

107. Lindsay A. Thompson et al., *The Intersection of Online Social Networking with Medical Professionalism*, 23 J. GEN. INTERNAL MED. (July 7, 2008); *see also Iowa College President Quits After Beer Photo*, MSNBC ONLINE, Aug. 28, 2008, *available at* http://www.msnbc.msn.com/id/26445893; Sánchez Abril, *supra* note 32.

108. *See* Jeffrey Rosen, *Your Blog or Mine?*, N.Y. TIMES, Dec. 19, 2004, *available at* http://www.nytimes.com/2004/12/19/magazine/19PHENOM.html?scp=1&sq=Jessica%20Cutler&st=cse (discussing Jessica Cutler, a Capitol Hill employee who wrote about her love affairs with six different men on her online blog); *see also* Get Revenge on Your Ex, http://www.getrevengeonyourex.com (last visited Apr. 9, 2009).

Figure 6: Relationship Breakup: Has This Happened?

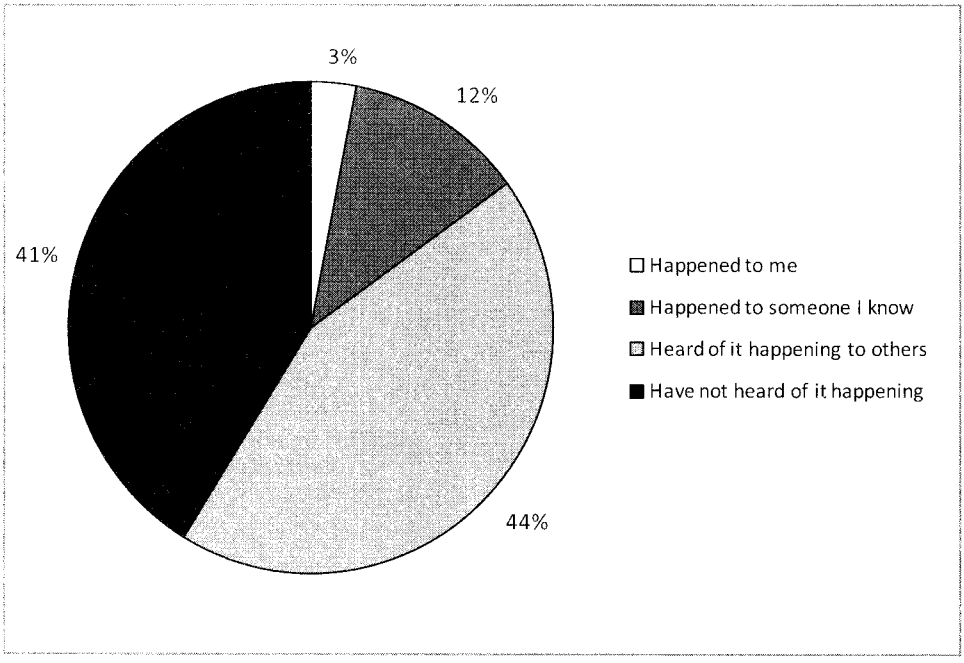


Figure 7: Party Time: Has This Happened?

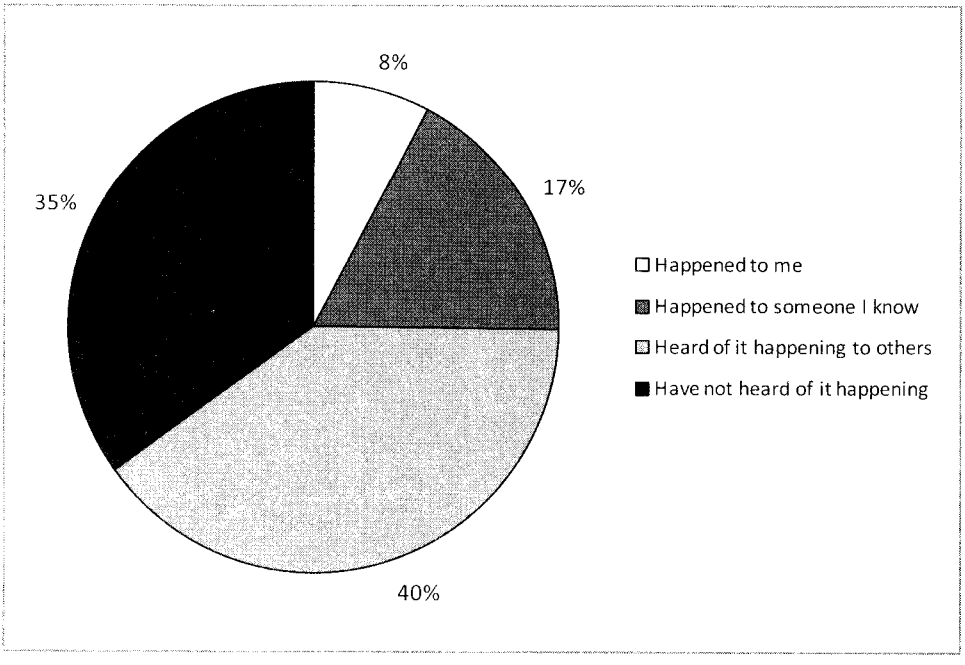


Figure 8: False Charges: Has This Happened?

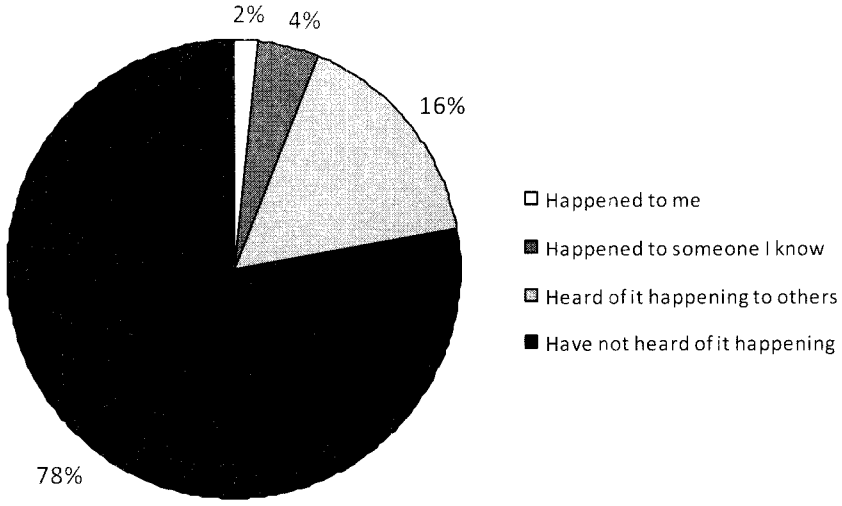
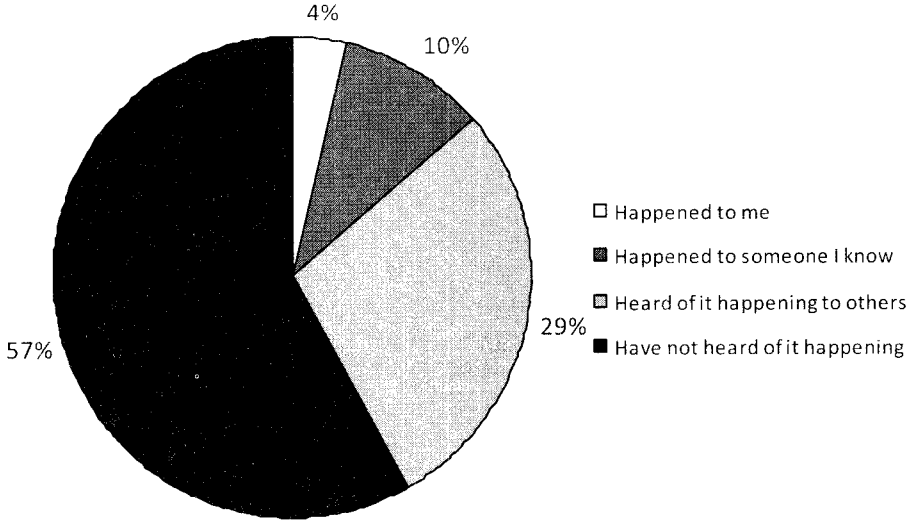


Figure 9: Sick Leave: Has This Happened?



5. Respondents Do Not Hold OSNs Accountable for OSN-Related Privacy Breaches

Although the role of the OSN varied among the four scenarios, an overwhelming 61 to 77 percent (depending on the scenario) of respondents were willing to exonerate the OSN provider completely for any harm caused by the privacy breach. This may indicate that OSNs are effectively propagating the view that they are not liable for anything that occurs on their sites. It may also indicate that OSN users understand the sites to be mere forums for information exchange. Respondents found the OSN developers most responsible for Relationship Breakup in comparison to the other scenarios, but even then, only 18 percent found OSN developers blameworthy.

Furthermore, in Sick Leave, where the OSN provider failed to respond to a request to take down pictures and this inaction led to a reprimand at work, only 12 percent of respondents felt the provider should be legally responsible. Instead, respondent OSN users generally held themselves or the poster primarily responsible, depending on the scenario.

Figure 10: Relationship Breakup: Who is Responsible?

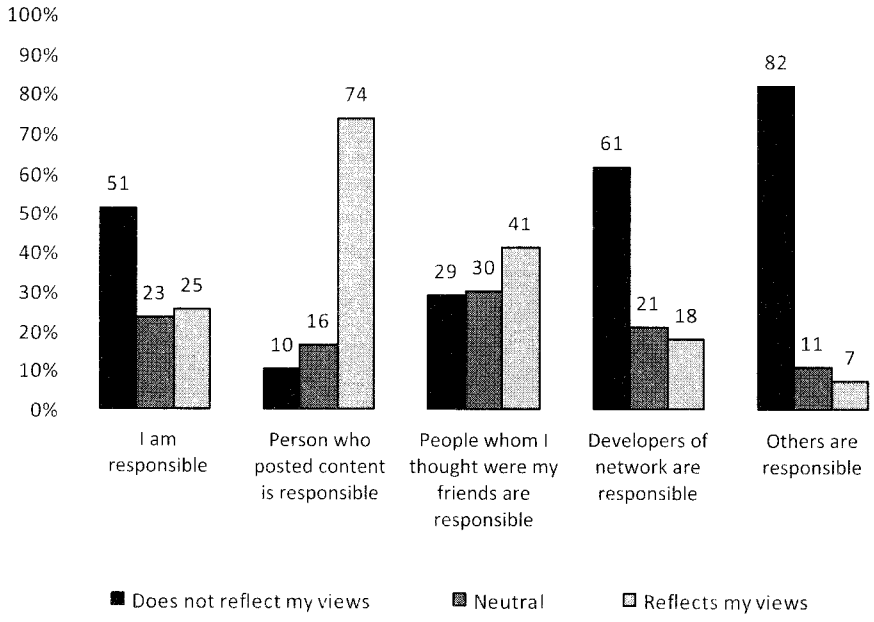


Figure 11: Party Time: Who is Responsible?

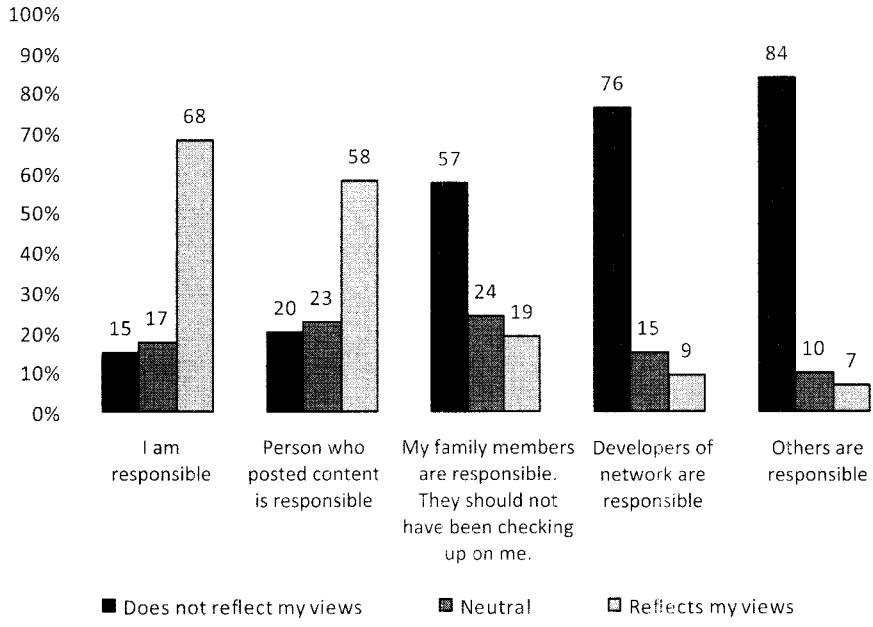


Figure 12: False Charges: Who is Responsible?

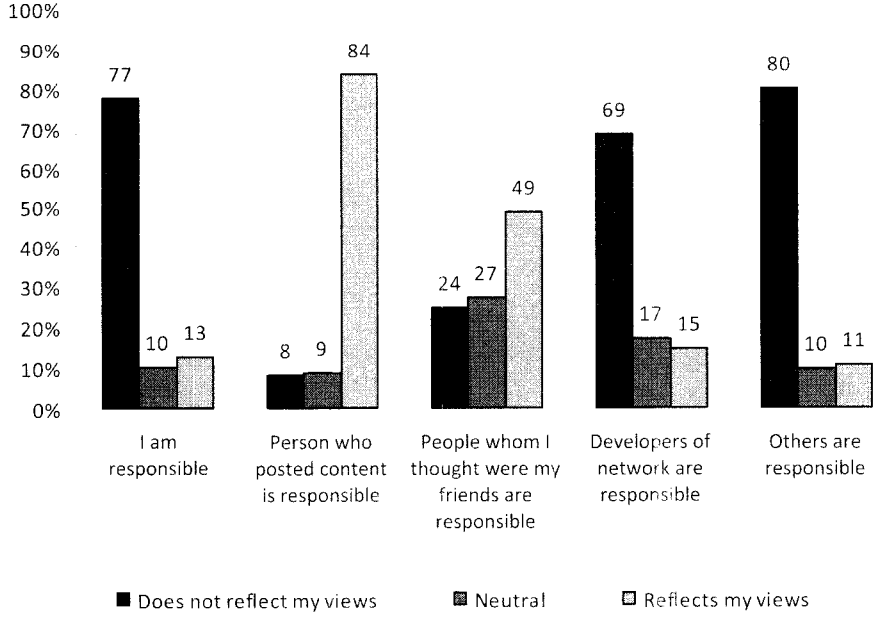
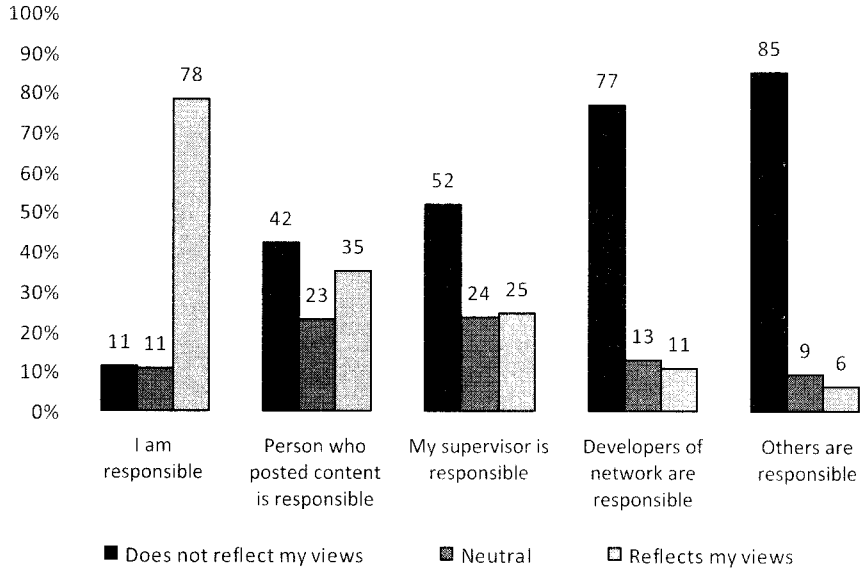


Figure 13: Sick Leave: Who is Responsible?



Does the users' reluctance to hold OSNs accountable for privacy breaches, such as those portrayed in the scenarios, indicate that online socializers accept that the role of OSNs is to only provide them with effective control mechanisms over personal information that they post? And do online socializers avail themselves of such tools? With the next category of findings, this Article seeks to understand how online socializers perceive the notion of privacy as control.

B. Control Over Personal Information on OSNs

1. Respondents Use Personal Information Protection Tools Offered by OSN Providers to Control the Information They Post

The majority of those surveyed are aware of and use the technological privacy-protecting tools offered by OSNs. Of these, 72 percent restricted their privacy settings and 54 percent blocked specific people from accessing their profile. Furthermore, a majority of users (61%) believe they take the appropriate steps to limit access to their profiles. These findings can be explained by understanding young online socializers as being technologically savvy, yet somewhat dismissive of potential risks online (and offline, as discussed above).

It is arguable that the contradictory feelings of invasion that arise when unintended audiences access online postings are the result of an over-reliance on an imperfect technology as a privacy protector. The OSN user who interacts confidently under the impression that the technology will block access to unintended audiences may feel betrayed when it does not work as expected.

Figure 14: Use of Privacy Settings

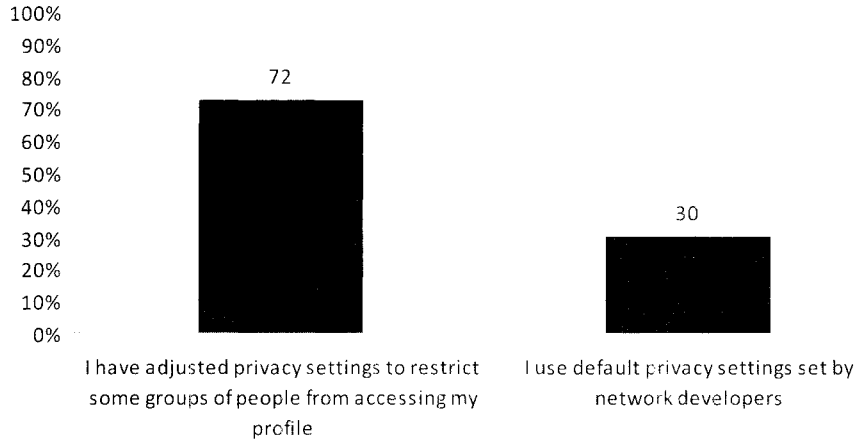
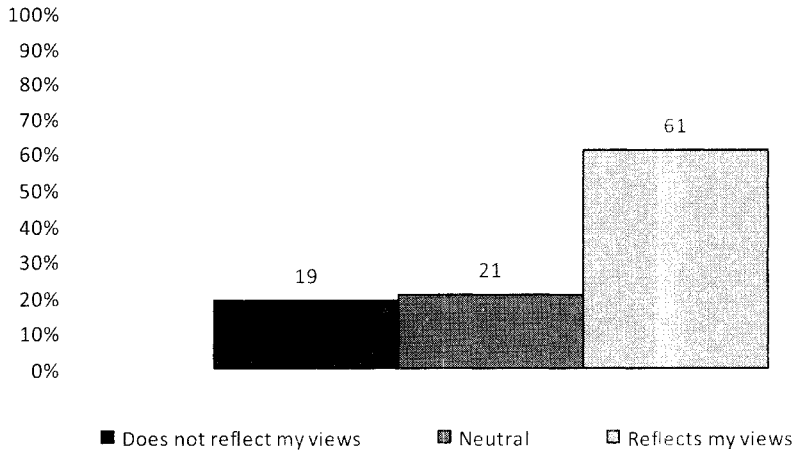


Figure 15: Views on Access to Profile
"I see myself as someone who takes appropriate steps to limit who has access to my profile."

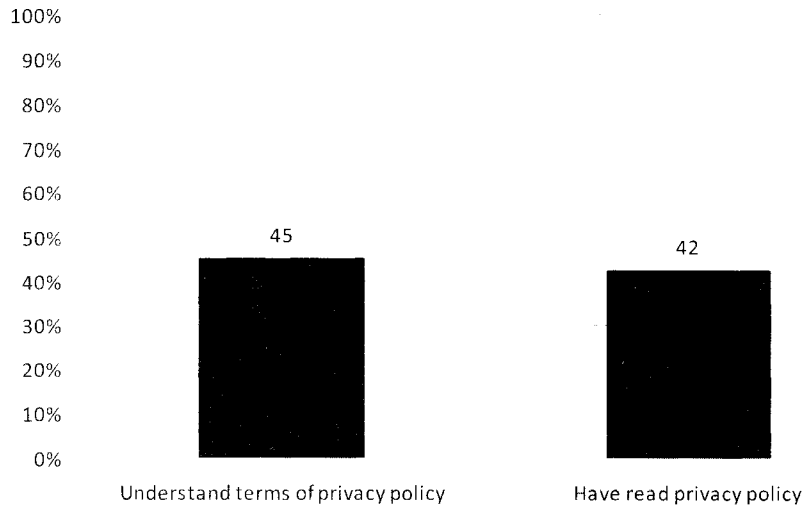


2. OSN Privacy Policies Do Not Inform Respondents' Online Behavior

While 42 percent of respondents reported reading their OSN's privacy policy, more than 45 percent reported understanding it. Hesiod's observation again comes to mind. More conventionally, the 3 percent that purportedly understood the privacy policy without reading it might be explained one of two ways: either the policy was explained to them by another user, the site itself, or another third party (blog, article, class, etc.); or perhaps they assume because they have read other sites' privacy policies, they have a general understanding of their preferred OSN's.

Even though less than half of respondents reported reading and understanding their network's privacy policy, over 70 percent, as noted above, have modified their privacy settings and/or restricted access to their profiles. It appears, therefore, that at least 30 percent of OSN users do not find it necessary to read their network's policy to take advantage of the privacy tools provided. This data reinforces the characterization of online socializers as being technologically savvy since they do not feel that they need to "read the manual" beforehand.

Figure 16: Reading and Understanding Privacy Policies



3. Respondents Understand That They Lack Control Over What Others Post About Them on OSNs

Roughly a third of respondents (34%) were not sure about their ability to control information posted about them on their OSN and whether they should be concerned about information that originates with others (30%). Most respondents were concerned about such information (46%) and a similar number of respondents (45%) stated that they felt helpless when it came to protecting their character on OSNs in the context of a specific scenario. Although more than a third of respondents (38%) felt that they were able to take the appropriate steps to control what was posted about them on their OSN, the remaining respondents (29%) were sure that they were *not* able to control such information. Further, as stated above, 61 percent of respondents believed that they took the right measures to protect their privacy.

These data suggest that although respondents do the best they can with the tools afforded to them by their network, they realize that these tools are insufficient to effectively control everything posted about them on the network. In addition, the high number of online socializers who are unsure about the risks of information posted by others, and unsure about their ability to control it, illustrates the difficulty of combining control-oriented privacy protection tools and policies with dignity-based concerns in a coherent manner. The domination of control-oriented tools leads to the dismissal of dignity concerns, while the emergence of such concerns reinforces uncertainty about the efficacy of such tools.

Figure 17: Control
"I believe I am able to take appropriate steps to control what is posted about me on my OSN."

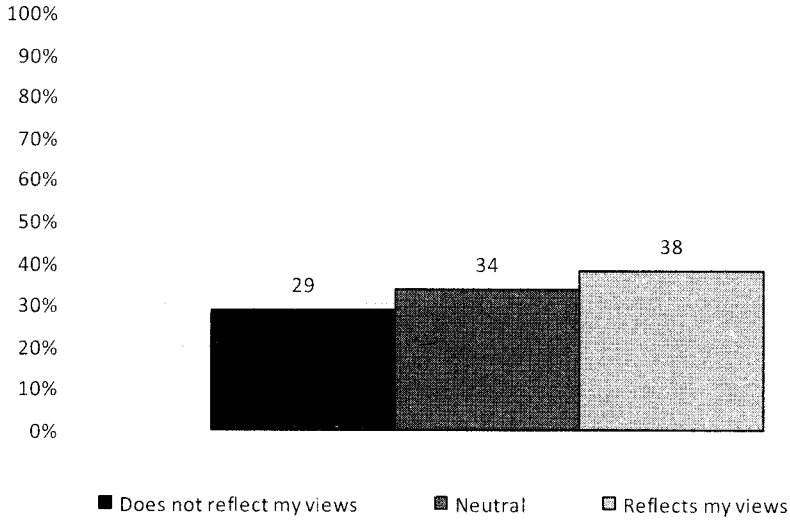


Figure 18: Lack of Control
"It concerns me that material posted about me on the OSN does not always originate with me."

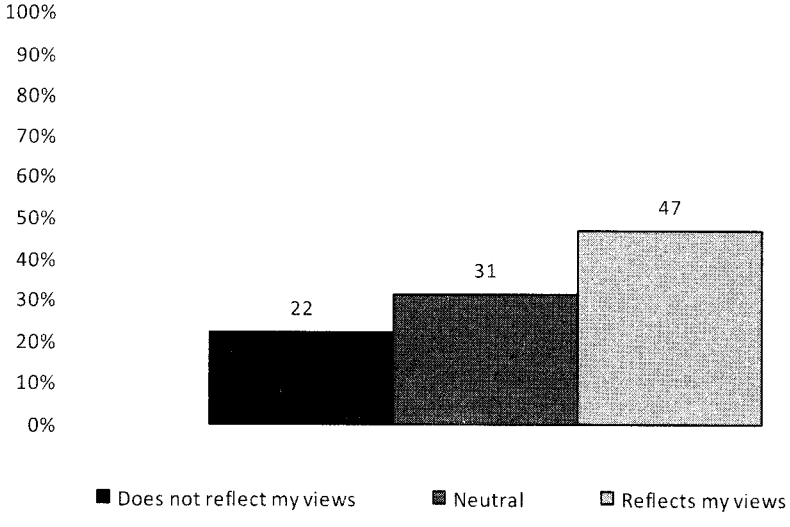
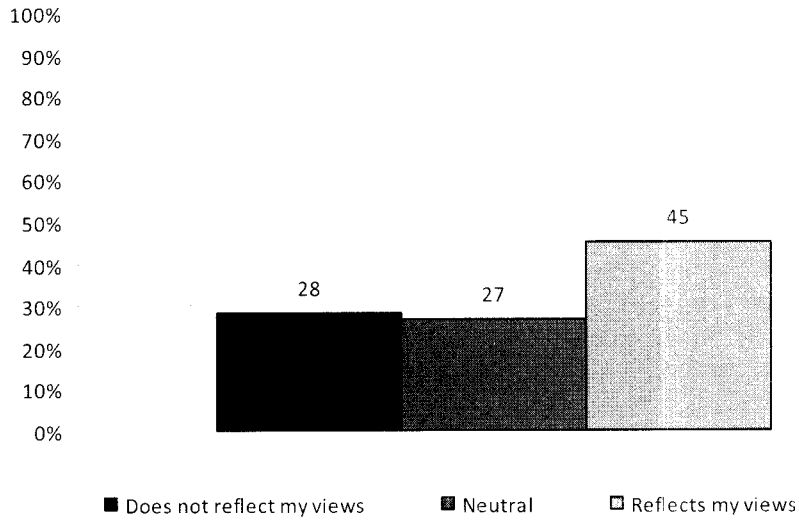


Figure 19: Privacy Protection Online[109]
"I feel hopeless about protecting myself and my character on OSNs."



At the same time, it is possible that the 25 percent of online socializers who indicated a lack of concern over information posted about them by others are not concerned about their dignity. With the next group of findings, this Article explores that possibility in more detail.

C. Dignity and Personal Information on OSNs

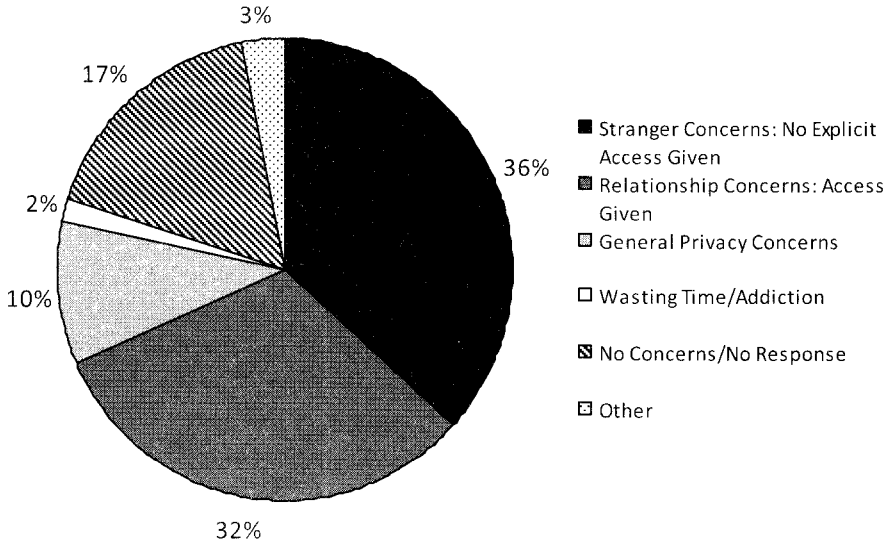
1. Respondents Are Concerned About Harm to Their Reputations

Respondents were asked to answer two open-ended questions regarding any concerns they experienced with respect to their personal lives while networking online. Respondents were free to report concerns of any nature, yet most reported concerns over their personal information, which could be expected given the context of the survey. Many respondents (37%) were concerned about unauthorized access—which is understood as access outside of their control—to their personal information. It appears, therefore, to be a concern based on the notion of control. Significantly, however, the second

109. This question was asked with respect to the False Charges scenario.

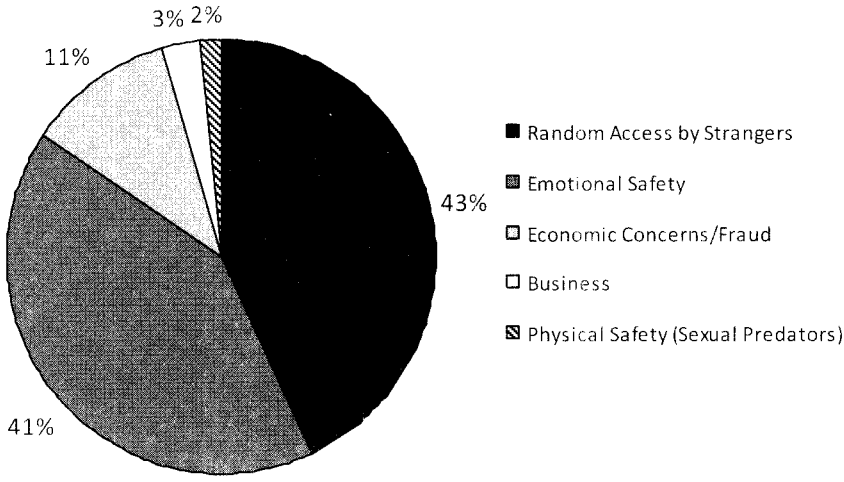
largest concern reported concerned the effects of access to personal information about relationships (32%). Of those, 68 percent specified that their apprehension stemmed out of a fear for their reputation. This seems to be a concern based on the notion of dignity, as are the remaining concerns within this relationship category (listed in the figures below). Therefore, the respondent's responses to the open-ended questions demonstrate that online socializers wish to both control their personal information and protect their dignity.

Figure 20: OSN Concerns Related to Personal Life



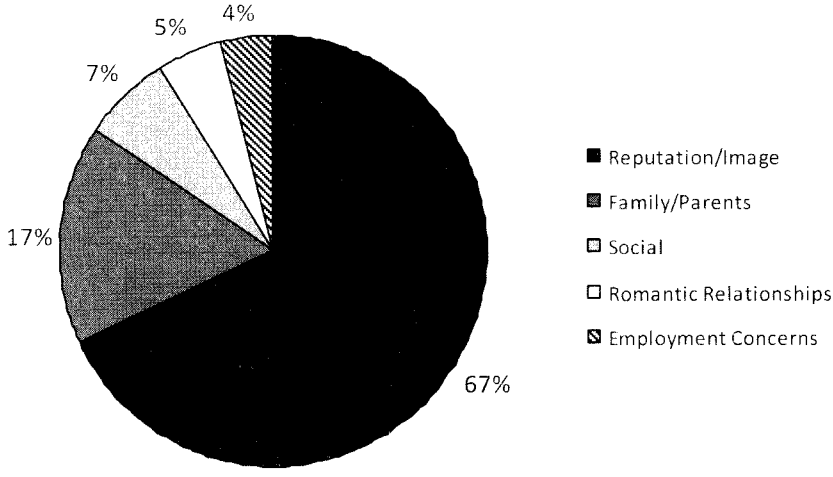
The following two figures break down the main concerns above into sub-categories.

Figure 21: Stranger Concerns: No Explicit Access Given



Note that all of the concerns in this category reflect the notion of dignity to some extent. Significantly, concerns in both figures are triggered when the information is used in unexpected ways or through unanticipated means, although access to it may have been authorized by the indivdual to some extent.

Figure 22: Relationship Concerns: Access Given



2. Respondents Believe That OSN Privacy Breaches Cause Real Harm

Respondents were asked whether any real harm (most likely interpreted as dignitary, economic, or social repercussions offline) could result from each of the four scenarios listed above. Roughly two-thirds of the respondents asserted that real harm could arise from each of these scenarios. The Sick Leave and False Charges Scenarios, both of which were set in an employment context, were considered the most harmful, with 71 percent agreeing that real harm could result from these scenarios. The Party Time Scenario followed closely, with 64 percent of respondents considering it harmful.

Respondents reported that the scenarios caused real harm, although the information was posted about them by another person. This indicates that online socializers perceive their privacy as being dependent on more than their control over the information that they post. It is not the ability to manage the information that they post that mattered to the respondents, it is the effect of information posted by others, information that cannot be controlled by respondents with existing OSN privacy tools. Privacy online can be harmed therefore, even when respondents are able to perfectly control the personal information that they post.

Figure 23: Relationship Breakup: Real Harm
"No real harm can come of this."

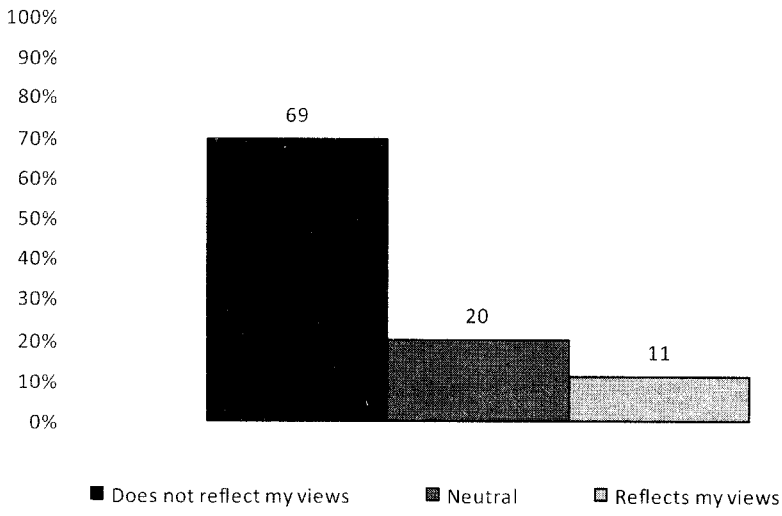


Figure 24: Party Time: Real Harm
"No real harm can come of this."

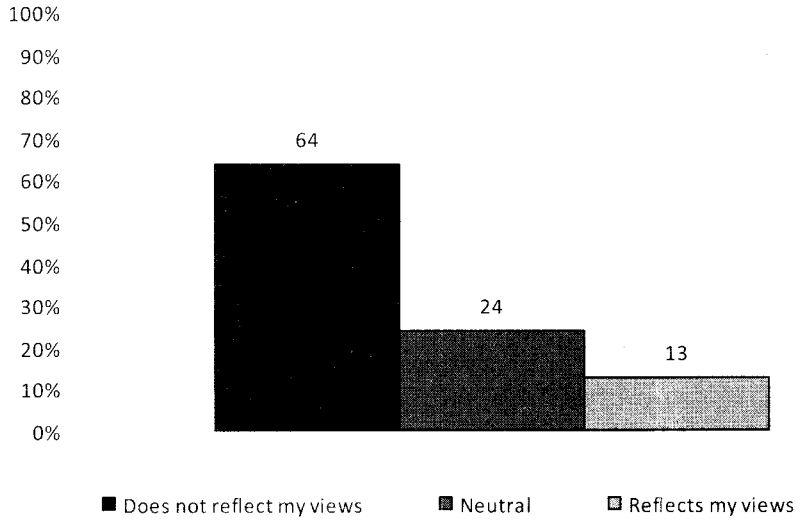


Figure 25: False Charges: Real Harm
"No real harm can come of this."

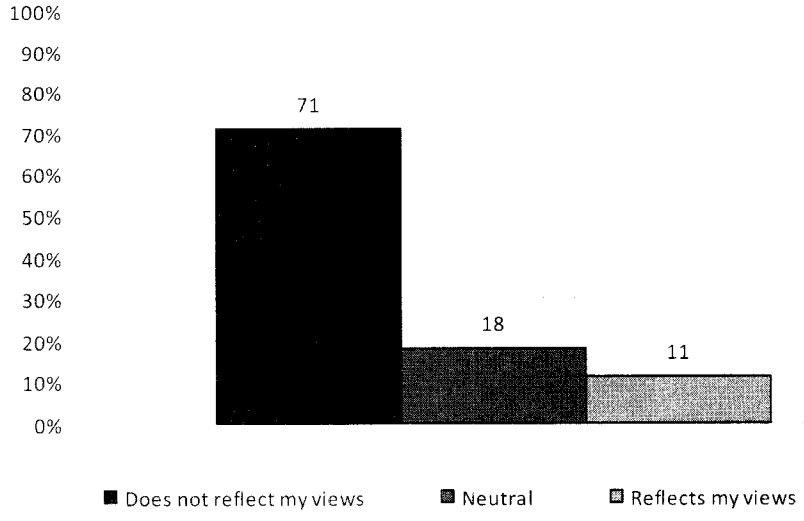
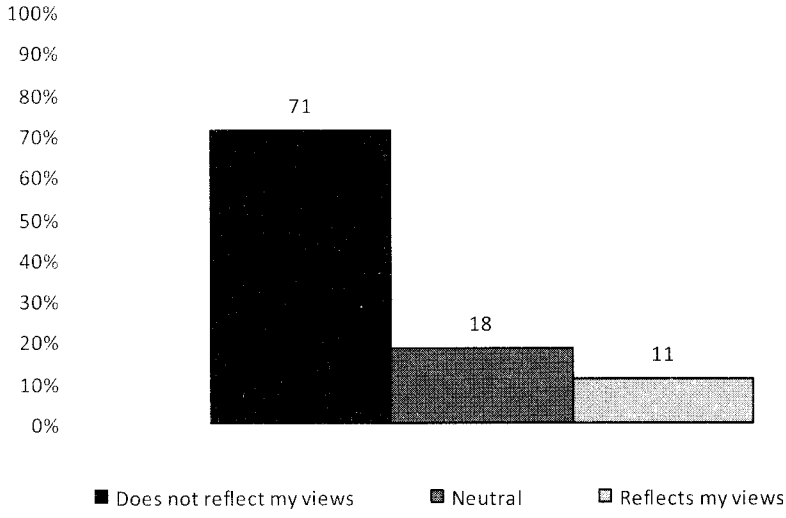


Figure 26: Sick Leave: Real Harm
"No real harm can come of this."



3. The Majority of Respondents Highly Value the Ability to Act Contextually and Expressed Strong Preferences Against Disclosures Across Contexts

Respondents generally expressed the need to compartmentalize distinct areas of their lives, particularly their work and social groups. This human desire has traditionally been associated with human dignity. Over half of respondents (54.3%) agreed with the statement, "Work life is completely separate from personal life, and what you do in one should not affect the other." A mere 6 percent strongly disagreed with this statement. Respondents were also adamant that their employer should not require them to allow the employer to be part of their online "friends" network. This is an increasingly common practice that almost two thirds of respondents (66%) considered very inappropriate.

Figure 27: Managers
"How appropriate is it for managers to require employees to add them as a 'friend' to their social network?"

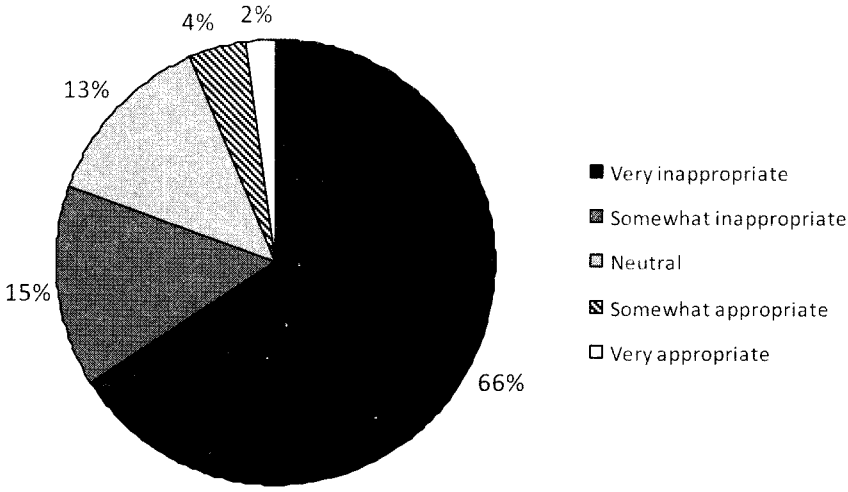
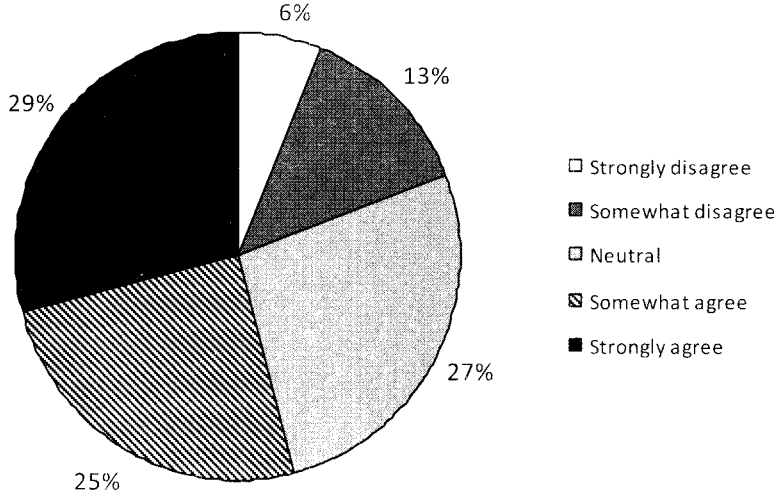


Figure 28: OSNs and Work
"Work life is completely separate from personal life: what you do in one should not affect the other."



These observations support a more general conclusion regarding the notions of privacy of OSN users. Online socializers have

a notion of privacy based firmly in both control over information and dignity. The following section expands upon this theory of network privacy.

IV. A NEW NOTION OF PRIVACY? NETWORK PRIVACY

The data demonstrates that respondent online socializers have a penchant for disclosure. However, they are aware of the risks involved in online socialization and cherish the ability to shield their multiple social personae and communicate with only intended audiences. Though seemingly incompatible with their behavior, this contradiction could reflect the young cohort's lack of work and life experience. This purported contradiction could be also indicative of an emerging notion of privacy online, one rooted more in dignity than in control over personal information. This Article refers to this construction as "network privacy."

Network privacy is a notion of privacy based on the expected accessibility of personal information to social constituencies. These expectations are grounded in the need to maintain discreet social identities, or situational personalities. When online socializers perceive a threat to privacy, it is really their reputation, dignity, persona, or online identity that is in peril.

The results of the study depict a group primarily concerned about privacy as it relates to the presentation of the self. Respondents acknowledge the probability of damage to their reputation and dignity on OSNs. Damage to dignity and reputation were repeatedly identified top concerns. Respondents also demanded the ability to create distinct personae, i.e., to sustain "firewalls" between social, work, and familial groups. Finally, the data reveals that online socializers generally share the perception that information shared on OSNs is intended only for members of the network.

Lack of control over personal information does not seem to preclude participation in OSNs. In fact, the inability to control personal information does not figure prominently among the major concerns of OSN members. Online socializers are, unsurprisingly, interested in socialization to the point that they are willing to take on acknowledged privacy risks. They are highly cognizant that they are relinquishing control over their information and its destination. Few believed that they could take appropriate steps to control what is posted about them and almost half reported feeling helpless about protecting their character on OSNs.

Online socializers are concerned not only about the extent of the dissemination of their personal information (how many people

know), but also about their information's destination (who knows). This understanding of privacy is complementary to recent explanations of privacy in traditional offline contexts, which place an emphasis on an individual's expectation of the extent of the dissemination of his private information, rather than on whether the individual expects his private information to be disseminated at all.[110]

Network privacy may be a product of new social media and traditional social norms. Online socializers seem to be transferring offline expectations of privacy into their online social experiences. Offline, individuals belong to many social networks and present different personae in different contexts. Individuals can share personal information selectively and discriminately between networks. In a sense, the information shared within a social network is no longer private, since it becomes known to members of the social network. Yet, in another important sense, it remains confined to the network by implicit understandings of confidentiality and trust. Offline, norms often dictate that personal information not be disclosed beyond the network in which it was originally shared.[111] These norms are more difficult to enforce on larger, less intimate online networks. The degree to which the information remains "private" once disclosed is dependent upon the size of the network and the intimacy among its members. Even offline, this is a difficult determination, since the boundaries of social networks are interconnected and porous. Moreover, it is nearly impossible to control information once disclosed online.

V. CONCLUSION

Protecting privacy in an online social network involves more than control. This is especially true when the information is in digital form. For several reasons, dignity is a more appropriate theoretical basis for privacy protection on OSNs than control. Dignity provides clear, simple rules on which to base privacy protection and behavior on OSNs. Simply stated, dignity-based privacy protection dictates that any sensitive information disclosed within a social network should be kept within the social network regardless of its source. This is consistent with the network privacy model described in the survey results.

---

110. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919 (2005).

111. The popular slogan "What Happens in Vegas Stays in Vegas" appropriately illustrates this point.

Solutions must be implemented to address the dignitary, social, and economic damages arising from networker-to-networker privacy breaches. These solutions could be legal or non-legal, technological or norm-based. The survey results demonstrate privacy values that are not compatible with the control-focused privacy tools currently available on OSNs and reflected in law and policy. OSN privacy policies and terms of service do not adequately protect the dignity of members nor do they address the common scenario of networker-to-networker disclosures. The essence of OSNs from a privacy perspective lies in the social interaction they provide, rather than in the information they collect as an organization. OSNs should therefore support network privacy as much as, if not more than, the traditional measures of control over personal information.

It is clear that OSNs have strong incentives against interfering with the exchange of information they facilitate. Individuals who socialize online expect their networks to improve rather than impede social interaction. However, it is equally clear that OSNs are able to provide their consumers with a measure of dignity protection their members cannot provide for themselves.

Unlike traditional facilitators of social networks, OSNs are well-positioned to protect the dignity of their participants. Both the technology and demand are in place for these businesses to provide stronger privacy protection tools and procedures to their members through technology, norms, and meaningful systems of dispute resolution and redress. There are also many possible regulatory measures for breaches of network privacy, ranging from the creation of new cyber-torts to non-litigious solutions, such as the imposition of a legal obligation on OSNs to participate in a "notice and takedown" regime similar to the Digital Millennium Copyright Act.

Given that there is no technological control over the dissemination of information online, the law and OSN policies must refocus on protecting a construction of privacy as dignity—a notion of network privacy that is already embraced by online socializers.

APPENDIX A

Methodology

The survey discussed in this article was conducted at Ryerson University, Canada, and the University of Miami in Coral Gables, Florida. The methodology for both locations was similar, except where noted below. The survey instrument was developed through reference to existing survey instruments[112] and five focus groups that provided insight into the ways in which young adults use OSNs, their thoughts about privacy and security issues, and the language they use to communicate in the online environment. The resulting 122-item, self-complete questionnaire contained a series of mainly closed-ended questions relating to demographics, attitudes, beliefs and behaviors around online socializing and the perceptions of risk associated with this activity. In addition, respondents were asked to complete two open-ended questions to indicate their primary concern with OSNs, first in relation to their personal life and again in relation to their professional or work life. The questionnaire is available online.[113]

The Sample

A total of 2,763 questionnaires were distributed by hand during the fall of 2007 to undergraduate students on the campuses of Ryerson University and the University of Miami. Ryerson University is an urban Canadian university located in Toronto, Canada, with an enrolment of 23,000. The University of Miami is a private university with approximately 15,400 undergraduate and graduate students located in Coral Gables, Florida.

Of the 2,763 questionnaires received, 294 submissions were eliminated because they were either incomplete or illegible, resulting in a total of 2,469 questionnaires that were used for the final analysis. As illustrated in the figures below, students ranged in age from 17 to 39, with over 94 percent falling into the 18 to 24 year-old category. The figures confirm the sample represented an almost equal representation of males and females. Furthermore, the majority of students (67%) work in paid employment on average for at least a few hours per week while going to school.

---

112. For groundbreaking quantitative research, see ALESSANDRO ACQUISTI & RALPH GROSS, PROCEEDINGS OF THE 6TH WORKSHOP ON PRIVACY ENHANCING TECHNOLOGIES, IMAGINED COMMUNITIES: AWARENESS, INFORMATION SHARING AND PRIVACY ON THE FACEBOOK (2006), *available at* http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.

113. To view the original survey, visit http://law.vanderbilt.edu/publications/journal-entertainment-technology-law/archive/download.aspx?id=3900.

Figure A1: Respondent Age

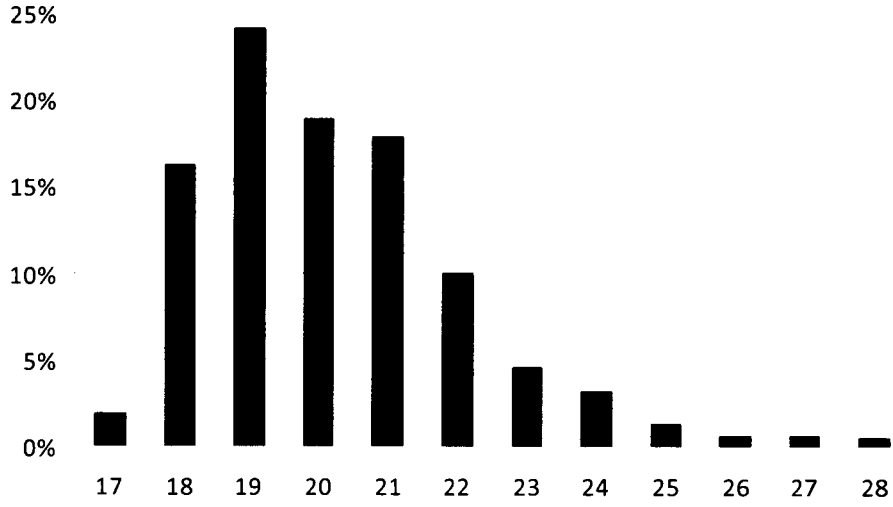


Figure A2: Respondents by Gender

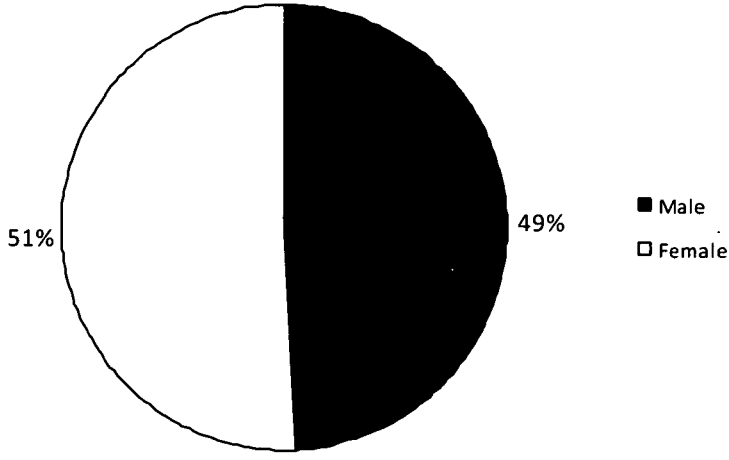
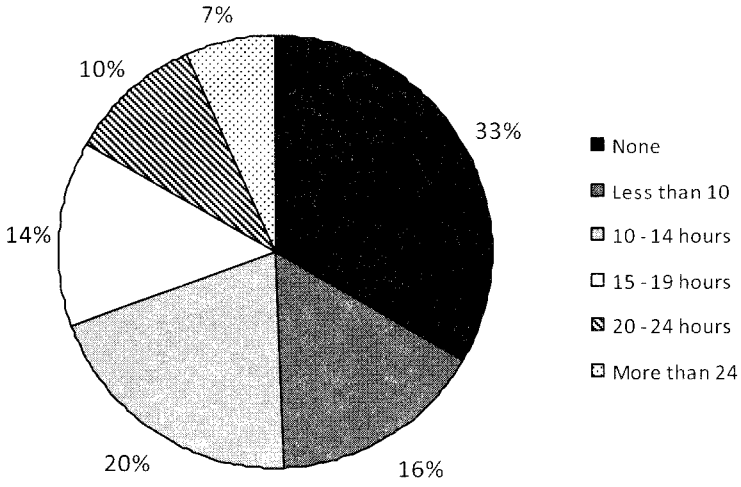


Figure A3: Respondent Weekly Work Hours



Analysis

The results of the closed-ended questions from the quantitative survey were analyzed using SPSS Version 16. Basic summary statistics included frequency distributions and mean values for scale questions. In addition, cross-tabulations with Pearson chi-square tests for significance and one-way ANOVA tests were performed to investigate response differences by gender, age, year of study and employment. These variables were chosen for the purposes of subgroup analysis as our initial focus group research seemed to indicate attitudinal and behavioral differences between males and females, as well as possible differences among older students who were closer to graduation and therefore likely more concerned than their younger counterparts about their projected online image among potential employers. In addition, students who were already working in part-time positions, particularly those with more than entry-level responsibilities, seemed to show greater awareness of and concern for their reputation. Despite these anecdotal findings, our analysis shows no significant differences by age, year of study or employment in the quantitative study. Although a significant difference did exist on the basis of gender, it was not considered insightful or sufficiently novel to warrant further discussion here.

Responses to the two open-ended questions were reviewed and grouped according to common themes by a team of three research associates, in consultation with members of the research team. In

order to protect the confidentiality of students, direct quotes presented in this article are attributed by field group number rather than by using personal information.