PRIVATE ORDERING: A CONTRACTUAL APPROACH TO ONLINE INTERPERSONAL PRIVACY

*Patricia Sánchez Abril**

INTRODUCTION

This Article examines the power of contract to create context and change social behavior regarding online interpersonal privacy. Defining privacy as a function of four variables—content, context, control, and contract—the Article posits that the awkward translation of these variables in the digital sphere contributes to the perception (and, ultimately, reality) of an environment of carelessness vis-à-vis privacy online. Social psychology suggests that creating the perception that someone cares discourages antisocial behavior. Applying these well-established theories to the online social space, the Article argues that a user-friendly system of contracting for interpersonal privacy online would both allow individuals to convey their privacy thresholds and combat the extant "anything goes" environment that now thrives. It goes on to analyze the functioning of such a contracting model from legal and practical perspectives.

* * *

Context, the set of circumstances or environmental factors surrounding a particular situation, influences social behavior.[1] In a famous 1969 experiment led by Philip Zimbardo, two identical cars without license plates were abandoned on a street with their hoods up. One car was left on the campus of Stanford University in Palo Alto, California and the other in the Bronx, New York. While both areas had similar laws against vandalism, within twenty-six hours

* Assistant Professor of Business Law, University of Miami School of Business Administration. B.A., Duke University, 1996; J.D., Harvard Law School, 2000. The author would like to thank Professors Jacqueline Lipton and Larry DiMatteo, Dean Blake Morant, and all of the participants at the 2010 Wake Forest Law Review Symposium, *Contract Law in Context*, for their invaluable comments and support. A debt of gratitude is also owed to Alissa del Riego and Eva Merian Spahn for their research assistance.

1. Philip G. Zimbardo, *The Human Choice: Individuation, Reason, and Order Versus Deindividuation, Impulse, and Chaos*, *in* 17 NEBRASKA SYMPOSIUM ON MOTIVATION 237, 238 (William J. Arnold & David Levine eds., 1970).

of the abandonment everything of value was removed from the Bronx car, while the Palo Alto car remained untouched.[2] A week later, Zimbardo publicly destroyed part of the Palo Alto car with a sledgehammer. Within moments, the car was utterly destroyed by passersby, some of whom would "probably consider themselves law-abiding."[3] Researchers posited that vandalism occurred much earlier in the Bronx because elements in the community life—"its anonymity, the frequency with which . . . things are stolen or broken, the past experience of 'no one caring'"—reinforced social disorder.[4] The Palo Alto car was only susceptible to vandalism once Zimbardo reinforced the message of abandonment (thus releasing the inhibitions of passersby), because the surrounding community had "come to believe that private possessions are cared for, and that mischievous behavior is costly."[5] An analysis of the study concluded that social disorder "can occur anywhere once communal barriers . . . are lowered by actions that seem to signal that 'no one cares.'"[6]

In 1982, James Q. Wilson and George L. Kelling expounded on Zimbardo's work, articulating what they called the "Broken Window Theory" to explain how contextual changes can curtail social disorder.[7] "If a window in a building is broken *and is left unrepaired*," they wrote, "all the rest of the windows will soon be broken."[8] The theory posits that even the most minor evidence of communal abandonment (in the form of a broken window, graffiti, or an unchecked panhandler) creates a public perception of abandonment and lack of control, which in turn propagates antisocial behavior, disorder, and crime.[9] Wilson and Kelling proposed a simple solution to combat social disorder: make seemingly minor contextual changes that communicate that someone cares.[10] Years later, criminologists, social psychologists, and legal scholars alike pointed to the steep decrease in New York City's crime rate in the mid-1990s as validation for the Broken Window Theory.[11] In 1993, the New York City Police Department

2. *Id*. at 287–90.

3. James Q. Wilson & George L. Kelling, *The Police and Neighborhood Safety: Broken Windows*, ATLANTIC, Mar. 1982, at 29, 31, *available at* http://www.theatlantic.com/doc/198203/broken-windows.

4. *Id.*

5. *Id.*

6. *Id.*

7. *Id.* at 31–34.

8. *Id.* at 31.

9. *Id.* at 31–34.

10. *See id.* at 31–32, 38.

11. *See, e.g.*, GEORGE KELLING & CATHERINE M. COLES, FIXING BROKEN WINDOWS: RESTORING ORDER AND REDUCING CRIME IN OUR COMMUNITIES 38–39 (1996) (citing the decrease in crime in New York City as a valid reason to implement further legal restrictions on disorderly behavior); Malcolm Gladwell, *The Tipping Point*, NEW YORKER, June 3, 1996, at 32, 38 (attributing double-

implemented a broken windows policing strategy, taking a strong stance against "public order" offenses such as public urination, public drunkenness, and vandalism.[12] During the next three years of such order maintenance, New York's murder, robbery, and burglary rates declined twice as much as did crime rates nationwide.[13]

More than forty years of sociological experiments about the propagation of crime shed important light on the fundamental interdependence of context—in the form of norms—and law in establishing and maintaining order. A vigorous academic legal movement has been built around the role of norms vis-à-vis legal rules in shaping human behavior and relations.[14] On one hand, legal rules can create context by changing norms, thereby bringing about social change. In the absence of an enforceable (and enforced) legal framework, a context of communal caring and engagement will not flourish. On the other hand, the normative environment can affect the efficacy, and indeed the existence, of legal rules. Lawrence Lessig has championed the idea that when social norms gain popular momentum, legislative change may successfully come about.[15] Inversely, without popular support and respect for rules,

digit decreases in crime to implementation of policing strategies based on the Broken Window Theory and reiterating the findings of the Zimbardo study); *see also* WESLEY G. SKOGAN, DISORDER AND DECLINE: CRIME AND THE SPIRAL OF DECAY IN AMERICAN NEIGHBORHOODS (1990) (supporting the broken-windows hypothesis with empirical data on disorder and crime in forty communities across the United States). *But see* Bernard E. Harcourt & Jens Ludwig, *Broken Windows: New Evidence from New York City and a Five-City Social Experiment*, 73 U. CHI. L. REV. 271, 271 (2006) (arguing that the authors' empirical data on crime rates refutes the efficacy of Wilson and Kelling's theory as a sound basis for law enforcement policies).

12. Dan M. Kahan, *Social Influence, Social Meaning, and Deterrence*, 83 VA. L. REV. 349, 368 (1997).

13. *Id.* at 367–68.

14. *See generally* ROBERT C. ELLICKSON, ORDER WITHOUT LAW: HOW NEIGHBORS SETTLE DISPUTES (1991); ERIC A. POSNER, LAW AND SOCIAL NORMS (2000); Lisa Bernstein, *Private Commercial Law in the Cotton Industry: Creating Cooperation Through Rules, Norms, and Institutions*, 99 MICH. L. REV. 1724 (2001); Ann E. Carlson, *Recycling Norms*, 89 CAL. L. REV. 1231 (2001); Tamar Frankel, *Trusting and Non-Trusting on the Internet*, 81 B.U. L. REV. 457 (2001); Kahan, *supra* note 12; Dan M. Kahan, *Trust, Collective Action, and Law*, 81 B.U. L. REV. 333 (2001); Mark A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257 (1998); Richard H. McAdams, *Group Norms, Gossip, and Blackmail*, 144 U. PA. L. REV. 2237 (1996); Lior Jacob Strahilevitz, *Social Norms from Close-Knit Groups to Loose-Knit Groups*, 70 U. CHI. L. REV 359, 359 & nn.2–4 (2003) (collecting scholarly works on law and social norms and describing the development of legal scholarship in the field).

15. *See* LAWRENCE LESSIG, FREE CULTURE 275–305 (2004). Professor Lessig's theories on the interrelationship of norms, technology, the market, and legal rules are definitional to this area of scholarship and inspirational to this Article. *See* LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 235–38 (2000) [hereinafter LESSIG, CODE]; LAWRENCE LESSIG, THE FUTURE OF IDEAS (2002).

laws are more likely to be disregarded and social disorder will ensue.

The online social environment is suffering from a multitude of "broken windows."[16] Reports of privacy violations on social media are ubiquitous.[17] Hospital patients' information is divulged on their physicians' online social network ("OSN") profiles.[18] A public school student is suspended for expressing a negative opinion about a teacher in a Facebook group.[19] A family receives death threats after their daughter briefly posts a derogatory essay about her hometown on MySpace.[20] An autistic boy in Italy is harassed on a video seen by millions.[21] A British schoolteacher kills herself because a disgruntled ex-lover posts nude pictures of her on Facebook.[22] These reports are no longer urban legends, but daily examples of life online that communicate that dignitary and privacy violations have become the norm. Anecdotal evidence suggests that the companies hosting social networks do not monitor for privacy violations.[23] In fact, meaningful dispute resolution and redress are not available to victims of these sorts of privacy harms; they often do not even know to whom to address complaints.[24] Reluctant to take responsibility, social media companies dismiss public concern and are quick to eulogize privacy.[25] Facebook founder Mark Zuckerberg recently announced that people simply no longer value privacy.[26] The result is a context of neglect and anarchy that ultimately suppresses expression and devalues human dignity.[27] It is clear why, as one

16. One blogger, John Kottke, has suggested that the broken window theory applies to online communities as well. kottke.org, http://kottke.org/08/12/does-the-broken-windows-theory-hold-online (Dec. 1, 2008, 12:44 EST).

17. Throughout this Article, "social media" is employed to describe any Internet-based application that allows the exchange of user-generated content and socialization.

18. Sixty percent of U.S. medical schools responding to a survey reported incidents of students posting unprofessional online content, thirteen percent of which constituted breaches of patient confidentiality. Katherine C. Chretien et al., *Online Posting of Unprofessional Conduct by Medical Students*, 302 J. AM. MED. ASS'N 1309, 1309–15 (2009).

19. Evans v. Bayer, 684 F. Supp. 2d 1365, 1367 (S.D. Fla. 2010).

20. Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 861 (Ct. App. 2009).

21. Rachel Donadio, *Italy Convicts 3 Google Officials in Privacy Case*, N.Y. TIMES, Feb. 25, 2010, at A1, A3.

22. *Teacher Killed Herself "After Ex-boyfriend Posted Naked Pictures of Her on Facebook*," DAILY MAIL ONLINE, Feb. 24, 2010, http://www.dailymail.co.uk/news/article-1253486/Teacher-killed-boyfriend-post-naked-pictures-Facebook.html.

23. JOSHUA GOMEZ ET AL., UNIV. CAL. BERKELEY SCH. OF INFO., KNOWPRIVACY 11 (2009).

24. *Id.* at 30, 32.

25. Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Boss*, GUARDIAN WKLY., Jan. 15, 2010, at 6.

26. *Id.*

27. *See* Pamela Samuelson, *Privacy as Intellectual Property?*, 52 STAN. L.

commentator put it, "the Internet has upped the stakes of confidence betrayals in intimate relationships exponentially."[28]

In contrast, empirical evidence overwhelmingly indicates that social media users are very concerned about their lack of control over personal information online.[29] Surveys also suggest that many users of social media feel "hopeless" about their ability to control their privacy and reputation online, despite website terms and conditions, privacy policies, and the ability to limit access to their OSN profiles.[30] These survey responses are not incongruous with observed behavior. Facebook's unanticipated alteration of privacy settings[31] and introduction of privacy-invading features (such as Newsfeed,[32] Beacon,[33] and Instant Personalization[34]) have provoked dramatic outcries among users, suggesting that these information consumers indeed cherish privacy despite the "broken windows" in their midst.[35]

However, all may not be so grim. Perhaps those who declare privacy dead conceive of it solely in terms of permissive technology or elusive legal rules. Defeatists may legitimately point to the widespread dissemination of information and to users' inability to control its ultimate destination and the context in which it is interpreted. They may lament the ineffectiveness of privacy law in

REV. 1125, 1159–60 (2000) (noting that news coverage about privacy issues shapes societal consensus about privacy in cyberspace and that user trust and confidence increases when Internet companies take publicized measures to ensure confidentiality).

28. Andrew J. McClurg, *Kiss and Tell: Protecting Intimate Relationship Privacy Through Implied Contracts of Confidentiality*, 74 U. CIN. L. REV. 887, 887 (2006).

29. GOMEZ ET AL., *supra* note 23, at 5.

30. Avner Levin & Patricia Sánchez Abril, *Two Notions of Privacy Online*, 11 VAND. J. ENT. & TECH. L. 1001, 1036–39 (2009).

31. In late 2009, Facebook suddenly changed its privacy settings, catching many unaware and exposing a great deal of personal information that was previously private. Natalie Lester, *Facebook Users Protest Content Policy*, WASH. TIMES, Feb. 19, 2009, http://www.washingtontimes.com/news/2009/feb/19/facebook-users-speak-out-on-content-policy/.

32. In 2006, Facebook launched "Newsfeed," a default service updating and disseminating all members' activities to those in their network of "friends." Posting of Ruchi Sanghvi to The Facebook Blog, http://blog.facebook.com/blog.php?post=2207967130 (Sept. 5, 2006, 04:03 EST).

33. In 2007, Facebook introduced "Beacon," which allows advertisers to track members' activities on third-party sites (even when not logged into Facebook) and broadcast these activities. Juan Carlos Perez, *Facebook's Beacon More Intrusive than Previously Thought,* PCWORLD, Nov. 30, 2007, http://www.pcworld.com/article/140182/facebooks_beacon_more_intrusive_than_previously_thought.html.

34. In 2010, Facebook removed users' ability to control the visibility of aspects of their personal information. Posting of Kurt Opsahl to Deeplinks Blog, http://www.eff.org/deeplinks/2010/04/facebook-further-reduces-control-over-personal-information (Apr. 19, 2010).

35. GOMEZ ET AL., *supra* note 23, at 29–30.

the online context and suggest that technological solutions alone have not sufficed to protect privacy. By refocusing online interpersonal privacy[36] as a concept characterized by several variables—not just technology—we can begin to formulate options that allow individual users to manipulate those privacy variables over which they can exert influence. This Article calls on the power of contract to create context and thereby address many online interpersonal privacy concerns. It contends that by creating systems to enforce minor privacy violations, the context of abandonment on social media can be changed and the more serious breaches averted. More specifically, a standardized, user-friendly system of express confidentiality agreements between users of social media would empower individuals to communicate their expectations of privacy to each other, circumventing onerous norms and inefficient law. This system promotes user autonomy, intimacy, and expression while recontextualizing the online social space as one where people value privacy.

Part I of the Article reframes the traditional conception of online privacy as solely dependent on technology, instead conceiving it as a function of four interdependent variables—content, context, control, and contract—and demonstrating how these same four variables are the "broken windows" of online privacy. These broken windows conspire to create a public perception of ambivalence toward breaches of interpersonal privacy, perpetuating social disorder. As Part II argues, contract, unlike the other three variables, is eminently controllable at the individual level and effective in communicating privacy entitlements. Whether readily legally enforceable or not, contract has the power to create and express social norms. Some commentators have theorized that appealing to contract, rather than tort, is the only constitutionally sound way to address privacy without unduly chilling speech.[37]

36. Throughout the Article, the word "interpersonal" is used to describe privacy between persons. I have chosen to use this modifier to distinguish the topic of privacy contracts between individuals online from the bulk of the academic literature on privacy, which refers to online privacy (without a modifier) as pertaining primarily to data protection vis-à-vis the relationship between an individual consumer and a commercial entity. *See, e.g.*, Samuelson, *supra* note 27, at 1127 (proposing a licensing model to allow consumers to bargain for privacy with website owners); Steven A. Bibas, Comment, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. & PUB. POL'Y 591, 592 (1994); Craig Martin, Comment, *Mailing Lists, Mailboxes, and the Invasion of Privacy: Finding a Contractual Solution to a Transnational Problem*, 35 HOUS. L. REV. 801, 844–49 (1998) (discussing a contractual model to protect consumer privacy in the field of direct mail marketing).

37. *See, e.g.*, Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 362–65 (1983); *see also* Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right To Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1061 (2000) (touting the "free speech advantage of the

Another has suggested that implicit confidentiality contracts should govern when physical world intimacy leads to a privacy violation through an instrument of mass communication.[38] Building on the work of these legal scholars and inspired by the existing scholarship on the interplay of legal rules and normative environment, this Article goes a step further, proposing in Part III a standardized system of explicit confidentiality agreements between users for all information shared online.

I. THE BROKEN WINDOWS OF ONLINE PRIVACY

Privacy is a very complex and nuanced concept. Luminaries across academic disciplines have tried to define its precise meaning and importance, yet no singular definition has emerged.[39] Some privacy scholars have defined privacy in terms of levels, gradients, or categories, because there are many social, cultural, and psychological forces at play in shaping what each individual comes to believe is, prize as, and label "privacy."[40] Drawing on this rich tradition, this Part offers four variables that have traditionally influenced an individual's expectations of privacy offline: content, context, control, and contract. Online, however, various forces obfuscate each of the privacy variables, making the determination and communication of privacy entitlements excessively burdensome. These technological, legal, psychological, and normative forces create the public perception that anything goes online and that no one cares about privacy in the digital social sphere, thereby becoming the broken windows of interpersonal privacy online.

A. The Broken Window of Content

Privacy is a social convention. Each society and individual makes value judgments regarding the degree of privacy to which certain information is entitled.[41] Often, these assessments are based on cultural notions regarding the nature of the information or whether its disclosure has the ability to expose its subject to

contract model").

38. McClurg, *supra* note 28, at 915–17.

39. *See, e.g.*, J. THOMAS MCCARTHY, THE RIGHTS OF PUBLICITY AND PRIVACY § 5:55 (2d ed. 2005) ("The simple word 'privacy' has taken on so many different meanings in so many different corners of the law that it has largely ceased to convey any single coherent concept."); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 477 (2006) ("Privacy is a concept in disarray. Nobody can articulate what it means.").

40. *See, e.g.*, ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967); Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 425–40 (1980); Solove, *supra* note 39, at 479–80; Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1094 (2002).

41. James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1153–56 (2004).

unnecessary risks.[42] For example, our society attributes a high degree of privacy to information relating to a person's body.[43] Health, medical, sexual, and excretory information is customarily regarded as highly personal.[44] Our society also acknowledges that personal financial information is private.[45] Consequently, U.S. law, through a panoply of statutes, regulates the disclosure of both types of information in certain circumstances.[46] The degree to which societies, social groups, and individuals confer private status on types of information naturally varies.[47] Nudity is a way of life in some cultures, whereas it is criminal in others.[48] Even within the same society, some people are willing to blog about their infertility, while others sue to conceal theirs.[49] Therefore, a unitary sentiment of what is personal across contexts and audiences (grade point average? unfavorable opinions about colleagues? sexual orientation? gun ownership? allergies?) is unattainable.

Despite the lack of consensus about what is properly private, U.S. privacy tort law is configured to protect privacy as defined by content, rather than social relationships or interpersonal understandings of confidentiality.[50] The breach of confidentiality tort, for example, is generally reserved for relationships involving a well-established duty of confidentiality and over subject matter customarily accepted as private, such as in the case of physicians

42. *Id.* at 1153–54.

43. Beate Rössler, *Privacies: An Overview*, *in* PRIVACIES: PHILOSOPHICAL EVALUATIONS 1, 6 (Beate Rössler ed., 2004).

44. *See* Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (establishing that "marital bedrooms" are "sacred precincts" into which intrusion would be plainly offensive); Washington v. Berber, 740 P.2d 863, 867 (Wash. Ct. App. 1987) (holding that a toilet stall is "properly characterized as 'private'"); JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA 170–71 (2000) (discussing courts' attitudes regarding privacy of health and medical information).

45. *See, e.g.*, Milohnich v. First Nat'l Bank, 224 So. 2d 759, 762 (Fla. Dist. Ct. App. 1969) (holding that a bank has an implied contractual duty not to disclose its customers' financial information).

46. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (codified as amended in scattered sections of 26 and 42 U.S.C.); Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401–3422 (2006).

47. *See, e.g.*, Brad Stone, *Too Much Information? Hah! Sharing All Online Is the Point*, N.Y. TIMES, Apr. 23, 2010, at A1, B7 (reporting on consumers who willingly share their private lifestyle habits and details of their consumer purchases online).

48. Whitman, *supra* note 41, at 1200–02.

49. *See, e.g.*, Y.G. v. Jewish Hosp., 795 S.W.2d 488, 491–93 (Mo. Ct. App. 1990) (couple sought to maintain secrecy regarding their in vitro fertilization).

50. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 123–27 (2007) (contrasting English law's formulation of privacy as contingent on confidentiality with U.S. law's focus on the information disclosed).

and their patients.[51] The tort of public disclosure of private facts focuses on the content of the facts revealed.[52] It requires an analysis of the information disclosed: it must be "private," "highly offensive to a reasonable person," and not of "legitimate concern to the public."[53] Courts tend to construe the privacy requirement in an exceedingly narrow fashion, demanding the information's total secrecy or seclusion.[54] The offensiveness prong of the analysis is also fatal to most privacy cases.[55] Courts generally interpret "offensiveness" as universally shameful, thus excluding business matters, personal data (such as social security numbers[56] and home addresses), and idiosyncratic or group-specific expectations of privacy.[57] Finally, the information disclosed must not be of "legitimate concern to the public" or newsworthy. The Supreme Court limited the public disclosure tort when it held that lawfully obtained material of public significance could not be hushed absent a need to further "a state interest of the highest order,"[58] and later, by applying a broad "public concern" test.[59] The Court's decrees roused legal scholars to question the tort's constitutionality and viability.[60] Despite its apparent survival, the public disclosure tort has been encumbered by the newsworthiness test, a chicken-and-egg analysis that often results in courts deferring to the market-driven judgment of publishers.[61]

51. *Id.* at 158 ("The tort still applies only to a limited set of relationships, with most cases involving the patient-physician relationship."); *see also* Susan M. Gilles, *Promises Betrayed: Breach of Confidence as a Remedy for Invasions of Privacy*, 43 BUFF. L. REV. 1, 54–57 (1995).

52. Richards & Solove, *supra* note 50, at 175 (citing McCormick v. England, 494 S.E.2d 431, 438 (S.C. Ct. App. 1997) (noting that the public disclosure tort "focuses on the *content*, rather than the *source* of the information")).

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

54. *See* Nader v. Gen. Motors Corp., 255 N.E.2d 765, 770 (N.Y. 1970) (ruling that information was no longer private after it was voluntarily disclosed to friends and acquaintances); Patricia Sánchez Abril, *Recasting Privacy Torts in a Spaceless World*, 21 HARV. J.L. & TECH. 1, 23–27 (2007) (discussing secrecy and seclusion as linchpins of privacy); Richards & Solove, *supra* note 50, at 174–75.

55. Abril, *supra* note 54, at 20–21.

56. Danielle Keats Citron has suggested that the public disclosure tort might protect the privacy of social security numbers in certain cases. Danielle Keats Citron, *Cyber Civil Rights*, 89 B.U. L. REV. 61, 87 (2009).

57. Johnson v. Harcourt, Brace, Jovanovich, Inc., 118 Cal. Rptr. 370, 372 & n.3, 373–74 (Ct. App. 1974) (determining that disclosure about a man's honesty was not shameful, even though his community branded him negatively for returning a sack of money he found).

58. Smith v. Daily Mail Publ'g Co., 443 U.S. 97, 103 (1979).

59. Fla. Star v. B.J.F., 491 U.S. 524, 539 (1989).

60. *See, e.g.*, Volokh*, supra* note 37, at 1070–71 (suggesting that any right to exclude others from publishing truthful information about oneself would run afoul of the First Amendment); Zimmerman, *supra* note 37, at 362 (calling public disclosure a "phantom tort").

61. *See generally* Amy Gajda, *Judging Journalism: The Turn Toward*

The Internet and social media have arisen against this backdrop of legal and normative mayhem and complicated it even further. Content-dependent privacy tort law, which was already struggling to address privacy harms in the physical world, has been ineffectual in addressing online privacy harms between users, in great part because the privacy torts do not neatly apply in the online social context.[62] If we cannot always agree on what is properly private subject matter in the physical world, consensus online is surely impossible in a universe devoid of physical boundaries, traditional culture, and shared understandings among its participants. Some social media participants covetously guard their privacy; the more conspicuous display an "urge to divulge" everything about themselves.[63] Despite the indisputable fact that individual tolerances of transparency naturally vary, the latter group's apparent disinterest in privacy—dubbed "oversharing"—has set a very public tone for social media and an image of reckless abandon of privacy online.[64] It is not surprising, then, that courts have demonstrated an almost uniform unwillingness to acknowledge a reasonable expectation of privacy online, regardless of the information poster's subjective expectations, intended audience, or confidential relationship with the information recipients.[65]

B. The Broken Window of Context

Privacy is particularly susceptible to context: the same piece of information can be characterized as private or not depending on the circumstances that surround the situation. These norms, in turn, are based primarily on the relationship of the parties, the space they occupy, and the laws that bind them.[66] Assume you are at a cocktail party and someone you have just met asks you how much you earn ("Is that net or gross?") or why you have an unsightly cold sore ("Is it sexually transmitted?"). Although these questions are not illegal to

Privacy and Judicial Regulation of the Press, 97 CAL. L. REV. 1039 (2009) (discussing the volatility of the "newsworthiness" test).

62. *See infra* notes 87–88 and accompanying text for examples of failed tort suits alleging online privacy violations.

63. *See* Stone, *supra* note 47, at A1 (reporting on consumers who willingly share their location, purchases, and other lifestyle habits online).

64. *Webster's New World* dictionary named "overshare" 2008's "Word of the Year," defining it as "to divulge excessive personal information, as in a blog or broadcast interview, prompting reactions ranging from alarmed discomfort to approval." Webster's New World, Word of the Year, http://newworldword.com (last visited Sept. 14, 2010); *see also* Stone, *supra* note 47, at A1 (noting a "mood of online openness" that encourages sharing of personal information on social media sites).

65. *See, e.g.*, United States v. Charbonneau, 979 F. Supp. 1177, 1184–85 (S.D. Ohio 1997) (finding that the defendant had no reasonable expectation of privacy in a message sent to a chat room); Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Ct. App. 2009).

66. ROSEN, *supra* note 44, at 9–13.

ask, they would certainly unsettle most people in our society. As a result, the inquirer might suffer social consequences (such as the premature termination of the conversation or being labeled rude or nosy) of the untoward probe. If the same questions were to be asked by a financial planner or a physician in the context of the provision of professional services, our discomfort with the intrusion would likely be minimal. This is because *context*, shaped by norms, space, roles, laws, and the expectations that come with each, also situates our definition of privacy in each circumstance.[67] The ambiguity of each of these context creators online contributes to an aggravation of privacy breaches between users.

A norm has been defined as "a rule that distinguishes desirable and undesirable behavior and gives a third party the authority to punish a person who engages in the undesirable behavior."[68] Privacy norms "work to maximize group welfare by reducing inefficient disclosures of appropriately private information."[69] Group norms are effective in regulating social interactions only when "whole communities believe in them[,] apply them," and can be classified as close-knit groups.[70] A close-knit group is a set of repeat players, or "a social network whose members have credible and reciprocal prospects for the application of power against one another and a good supply of information on past and present internal events."[71] To effectively enforce privacy norms, members of close-knit groups (or an authorized third party) must react and sanction privacy norm violators when they are out of bounds.[72] To illustrate, Professor Strahilevitz points to the example of the powerful privacy norms among members of Alcoholics Anonymous, whose implicit code bars public disclosure of any revelations made within the group.[73]

Close-knit groups, however, are not common online. Most online fora do not support close-knit groups or deeply held privacy norms, as their main impetus is to share information, socialize, and gather acquaintances. Moreover, the anonymity, pseudonymity, and invisibility facilitated by cyberspace tend to loosen relational ties between members and invite people to behave with less restraint.[74]

67. *See id.*

68. Eric A. Posner, *Law, Economics, and Inefficient Norms*, 144 U. PA. L. REV. 1697, 1699 (1996).

69. McAdams, *supra* note 14, at 2280.

70. Posner, *supra* note 68, at 1708; *see also* ELLICKSON, *supra* note 14, at 177–83 (discussing the dynamics of norm enforcement within close-knit groups).

71. ELLICKSON, *supra* note 14, at 181.

72. *See id*. at 180–81.

73. Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 924–25 (2005).

74. Psychologists have found that face-to-face interaction and physical feedback help navigate the human brain through social situations, permitting empathy and defining appropriate interpersonal behavior. Daniel Goleman, *Normal Social Restraints Are Weakened in Cyberspace*, INT'L HERALD TRIB., Feb.

For example, chat-room participants under pseudonymous guise can carry on vitriolic or antisocial rants without social repercussion, and OSN members are free to engage in the digital equivalent of medicine cabinet snooping without fear of getting caught, looking through the pictures and musings of others who have not specifically invited their eyes and judgment.

The majority of online fora can thus best be classified as either loose-knit or intermediate-knit groups.[75] Many blogs, chat rooms, and comment boards are typically loose-knit settings, in which members do not usually "expect to be repeat players [and] are unable to gather accurate information about another member's reputation even if repeat-player interactions do occur."[76] The majority of OSNs are best labeled intermediate-knit groups, defined as a cohort comprised of both repeat-player companions and non-repeat-player strangers.[77] An individual's OSN profile is populated by many members from different areas of the host's life. For example, Facebook estimates that the average user has 130 friends on the site;[78] members' main link to each other is common acquaintance with the OSN host. Even vis-à-vis the network host, many of these "friends" are better classified as tenuous acquaintances rather than intimates with "credible and reciprocal prospects for the application of power against one another."[79] This "loose friendship" culture has a significant impact on privacy. Members of non-close-knit groups are more apt to misjudge the subject of a rumor or embarrassing image or memorialize a reputation based on a context-free bit of information.[80] Non-close-knit settings are not conducive to the development of strong privacy norms or efficient methods of enforcement. Without the communal reinforcement of close-knit groups, privacy violations are much less likely to be sanctioned, and thus more prone to multiply.

As online networks become less close-knit and more context-free, traditional means of norm enforcement such as reputational

20, 2007, http://www.nytimes.com/2007/02/20/technology/20iht-email.4656417.html.

75. Strahilevitz, *supra* note 14, at 359–60. Some tightly held social media profiles could be classified as close-knit groups when all of their members know and can easily identify one another.

76. *Id.* at 360.

77. *Id.* at 365.

78. Facebook.com, Statistics, http://www.facebook.com/press/info.php?statistics (last visited Sept. 14, 2010).

79. McAdams, *supra* note 14, at 2241.

80. *See* ROSEN, *supra* note 44, at 8–9 ("[W]hen intimate information is removed from its original context and revealed to strangers, we are vulnerable to being misjudged on the basis of our most embarrassing, and therefore most memorable, tastes and preferences."); Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 1035–41 (2003) (discussing the destructive potential of private information when taken out of context by nonintimates).

monitoring or cutting off friendships are less efficacious and legal rules gain prominence.[81] In addition to being a context creator, the law is a context enforcer. To date, however, the law has suffered from dubious applicability in the online social world.[82] In the absence of a clear online context, judges deciding lawsuits arising from online activity must "contextualize" the allegedly harmful conduct; that is, judges must determine whether it is properly reprehensible across contexts.

C. The Broken Window of Control

Content and context alone are not determinative of privacy because privacy is also subject to individual *control*. Alan Westin has famously described privacy as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[83] Indeed, much of American privacy law is premised on a conception of privacy as control over personal information.[84]

Control over private information is the currency of intimacy and has an important communicative function.[85] Privacy affords people the opportunity to selectively hide or share information about themselves with others. In doing so, individuals craft identities and forge intimate bonds.[86] Yet outside forces do not always allow us to maintain total control over our private information. Other than becoming invisible, we cannot control the availability of certain information about our appearance, whereabouts, preferences, associations, and habits. American law institutionalizes this logic in its well-established denial of privacy protection of anything visible or accessible from public places.[87] Although some would argue that their private OSN profiles, blog posts, or emails are intended for a

81. *See* ELLICKSON, *supra* note 14, at 283 (explaining that "disputants are increasingly likely to turn to legal rules when the social distance between them increases").

82. *See* Joshua A.T. Fairfield, *Anti-Social Contracts: The Contractual Governance of Virtual Worlds*, 53 MCGILL L.J. 427, 440 (2008) ("Tort suits for injuries that occur in virtual worlds are difficult to pursue because courts have not yet determined what is a sufficient violation of social convention to merit sanction."); Richards & Solove, *supra* note 50, at 155 ("And the privacy torts have struggled when addressing emerging privacy problems in the Information Age.").

83. WESTIN, *supra* note 40, at 7.

84. Whitman, *supra* note 41, at 1209–11; W.A. Parent, *Privacy, Morality, and the Law*, *in* PHILOSOPHICAL ISSUES IN JOURNALISM 92, 95 (Elliot D. Cohen ed., 1992) ("Indeed, definitions of privacy in terms of control dominate the literature.").

85. *See* Patricia Sánchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 85 (2007).

86. *Id.* at 83 (discussing identity creation as a benefit of privacy).

87. *See, e.g.*, Boring v. Google, Inc., 362 F. App'x 273, 279–80 (3d Cir. 2010); Condon v. Reno, 155 F.3d 453, 464–65 (4th Cir. 1998), *rev'd on other grounds*, 528 U.S. 141, 151 (2000); *see also* McClurg, *supra* note 28, at 887–88.

limited audience, courts have generally held that one cannot have a reasonable expectation of privacy in materials published online.[88]

This premise of control is thus wholly incompatible with the online context, particularly on social media because there is no way to exercise control over personal information launched into the digital netherworld. Digital disclosures are infinitely transferable, searchable, and permanent.[89] Even refusing to participate online would not make one exempt from potential digital invasions, as anyone can post images or tag a person on Facebook without his or her consent.[90] Persons whose private information, images, or videos are digitally transmitted permanently lose control over that information and can never delete, defend, or rebut it—it simply becomes part of the permanent "Google-able" fabric of their reputation.[91] They can never know who has seen the information or for what purposes. In one recent study, forty-seven percent of college-aged OSN participants surveyed expressed concern that information online about them did not originate from them and that they had no control over it.[92] Forty-five percent expressed hopelessness about protecting their reputation on OSNs for the same reason.[93] Further, they were concerned that they cannot ascertain who has access to it, for what purpose, or how the ultimate information recipient interprets the information.[94]

Aside from the current technological reality, the law offers clear disincentives for those who can technologically control information—the social media hosts—to exercise control over or become intermediaries in their participants' disputes. Section 230 of the Communications Decency Act of 1996 (the "CDA") offers immunity from liability arising from third-party postings[95] (including all information-related tort claims, such as negligence,[96] defamation,[97]

88. Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 858, 863 (Ct. App. 2009) (noting that posting an article on MySpace.com "opened [it] to the public at large"); Yath v. Fairview Clinics, N.P., 767 N.W.2d 34, 44 (Minn. Ct. App. 2009) ("[P]osting information on a publicly accessible webpage constitutes publicity."); Dexter v. Dexter, No. 2006-P-0051, 2007 Ohio App. LEXIS 2388, at *18, *19 & n.4 (Ct. App. May 25, 2007) (holding that there is no reasonable expectation of privacy in an online rant).

89. *See* Lawrence Lessig*, The Architecture of Privacy*, 1 VAND. J. ENT. L. & PRAC. 56, 60 (1999).

90. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 231 (2008).

91. *See* Levin & Abril, *supra* note 30, at 1017.

92. *Id.* at 1037.

93. *Id.* at 1038.

94. *Id.* at 1045–46.

95. Communications Decency Act, 47 U.S.C. § 230(c) (2006).

96. Lunney v. Prodigy Servs. Co., 723 N.E.2d 539, 543 (N.Y. 1999).

97. Smith v. Intercosmos Media Group, Inc., No. 02–1964, 2002 U.S. Dist. LEXIS 24251, at *14–15 (E.D. La. Dec. 17, 2002); Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998).

intentional infliction of emotional distress,[98] and invasion of privacy[99]) to websites that remain passive interactive computer services. To remain within the generous safe harbor, websites cannot become "information content providers," defined as "any person or entity that is responsible, in whole or in part, for the creation or development of information provided through the Internet."[100] In the past three years, courts have shown an increased eagerness to hold websites liable when they interfere with, influence, or exercise editorial power over a user's postings.[101]

The CDA thus provides a powerful disincentive for social media hosts to intervene in privacy disputes between users. This may explain why most social media sites do not monitor for privacy violations or manage systems for dispute resolution, and are hesitant to intercede in user-to-user disputes. Although most social media sites have terms and conditions banning privacy-invading or defamatory conduct, the sites' own disregard of these rules undermines the behavioral norms they purport to promote.[102] The facts of a recent Ninth Circuit case illustrate the lackadaisical stance of social media hosts toward interpersonal privacy.

In *Barnes v. Yahoo!, Inc.*, a woman repeatedly requested that Yahoo remove nude photos of her, which had been vengefully posted by her ex-boyfriend and were causing her to be harassed for sex by strangers.[103] Her petitions were in accordance with Yahoo policy and the ex-boyfriend's behavior contravened Yahoo's terms of use.[104] After several months of appeals and continued harassment, Yahoo did not respond to the woman's plight and the illicit photos continued to circulate the Internet until the woman sued Yahoo.[105] Unchecked privacy violations such as these give the impression that no one can control the environment and no one cares to do so.

D. The Broken Window of Contract

When content, context, and control do not adequately circumscribe our desired level of privacy in a given situation, individuals habitually rely on promises of confidentiality to secure privacy. In daily life offline, signaling for privacy occurs through a

98. *See* Schneider v. Amazon.com, Inc., 31 P.3d 37, 42–43 (Wash. Ct. App. 2001) (pointing out that under § 230, "Congress intended to extend immunity to *all* civil claims" (emphasis added)).

99. *Id*.

100. § 230(f)(3).

101. *See, e.g.*, Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1169 (9th Cir. 2007).

102. *See* Fairfield, *supra* note 82, at 450 (noting that "griefing in a virtual world usually results in little action by the virtual-world provider" despite rules to the contrary).

103. Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1098 (9th Cir. 2009).

104. *Id.* at 1098–99.

105. *Id.*

series of highly orchestrated verbal and nonverbal cues, such as prefacing a comment with "between you and me," speaking in a hushed tone or whisper, and conversing "behind closed doors."[106] Similarly, a memo marked "confidential," a written nondisclosure agreement, and the imposition of explicit conditions of confidentiality are examples of legally enforceable confidentiality contracts.[107] These contracts circumvent normative and legal privacy constraints and allow the parties to communicate their idiosyncratic expectations and agree on their own terms for information exchange.[108] In this way, *contract* is the final privacy variable.

One of the primary functions of contract is to establish context in the form of expectations, rules, and norms among contracting parties and beyond.[109] However, contracts can only be effective in cementing contextual expectations when they properly address the contracting parties' desires and are widely perceived as a mechanism for prescribing behavior.[110] In addition, entering into contracts must be relatively efficient and low cost for such agreements to affect change beyond their constituents. None of these preconditions is currently being met online, particularly with respect to privacy.

First, contracts are not widely perceived as an empowering tool for individuals online.[111] In fact, the majority of online contracts are between the individual user and the platform. These involve "take it or leave it" consent and are often not representative of the individual user's desires. Bargaining is neither efficient nor available.[112] Online contracts tend to be legalistic and unduly time-consuming to read,[113] As a result, they simply become an ignored and accepted cost of life online. It is generally acknowledged that OSN members neither read nor attempt to understand terms of service or privacy policies.[114] In addition, website terms and policies

106. Gilles, *supra* note 51, at 23–25 (pointing out that although these cues are understood between confidants, they are usually too vague to give rise to legal remedies and often occur in relationships in which confidences are not protected by law).

107. *See id.*

108. *Id.*

109. *See* Larry A. DiMatteo & Blake D. Morant, *Contract in Context and Contract as Context*, 45 WAKE FOREST L. REV. 549, 561 (2010).

110. *Id.* at 568.

111. *See* Margaret Jane Radin, *Humans, Computers, and Binding Commitment*, 75 IND. L.J. 1125, 1149–50.

112. *Id* at 1128–33 (2000) (discussing basic models of consent online).

113. GOMEZ ET AL., *supra* note 23, at 11–12.

114. *See* Susan E. Gindin, *Nobody Reads Your Privacy Policy or Online Contract? Lessons Learned and Questions Raised by the FTC's Action Against Sears*, 8 NW. J.L. TECH. & INTELL. PROP. 1, 7–8 (2009); Levin & Abril, *supra* note 30, at 1035; *see also* CHRIS JAY HOOFNAGLE & JENNIFER KING, BERKELY CTR. FOR LAW & TECH., RESEARCH REPORT: WHAT CALIFORNIANS UNDERSTAND ABOUT

often include clauses allowing the host to modify its terms at any time, exposing users to an unstable environment and calling into question the value of a promise in the medium.[115]

Second, to date, contracts have not been customarily used as vehicles to protect privacy among intimates. Keeping trusted information private is customarily a moral and casual, not a contractual, commitment. Friends do not habitually enter into legally enforceable contracts for privacy.[116] Whereas asking for confidentiality with verbal and nonverbal cues is a socially accepted convention, requesting that a friend sign (or click) a document ensuring the privacy of communications made within the relationship can signal distrust and be noxious to the friendship. When a friend breaches another's privacy through the unsanctioned sharing of her digital information, the cost of enforcement (including legal and social costs) can also be too high to justify.[117] Suing is not likely to be efficient or realistic, given the relatively low value of the information (assuming the aggrieved party is a noncelebrity and the information does not have significant economic value), the lack of verifiable or tangible damages, and the high costs of litigation.[118] Enforcement through nonlegal channels (such as formalized reputational monitoring by a third party or network participants, or online dispute resolution) is rarely available, especially in loose-knit communities in which no normative rules prevail to manifest group opprobrium.[119]

Finally, despite the fundamentally communication-oriented functions of Web 2.0, the transaction costs associated with contracting for privacy remain high. Negotiating the distinct privacy of each post or uploaded image is prohibitively costly: each month, there are an estimated thirty billion pieces of content shared on Facebook alone.[120] Drafting terms is difficult and inefficient. Yet examples of successful interuser contracting systems abound online.

PRIVACY OFFLINE 25 (2008), *available at* http://ssrn.com/abstract=1133075 (noting that people tend to think that the very existence of a privacy policy protects them from unwanted disclosure).

115. For examples of such unilateral changes, see *supra* notes 31–34 and accompanying text describing abrupt changes to Facebook's privacy policy.

116. *See* Alan E. Garfield, *Promises of Silence: Contract Law and Freedom of Speech*, 83 CORNELL L. REV. 261, 280 (1998) (noting that friendship is an "informal context[] in which people frequently do not resort to contracting").

117. *See* Abril, *supra* note 54, at 10 (attributing the lack of successful lawsuits in this context both to the infrequency of successful public disclosure suits generally and to the resulting social cost of having to disclose embarrassing facts in court as part of the public record).

118. *See id.* ("A privacy tort case, like any other, requires damages substantial enough to make the costly legal process worthwhile. As a result, defendants are usually deep-pocketed media outlets rather than individuals.").

119. *See* ELLICKSON, *supra* note 14, at 177–83, 283.

120. Facebook.com, Statistics, http://www.facebook.com/press/info.php ?statistics (last visited Sept. 14, 2010).

Low-transaction-cost contracts between users are the backbone of commercial websites such as eBay. Despite the availability of the technology to facilitate contracting online, no system of user-to-user contracts governing privacy and confidentiality has emerged.

Establishing what privacy means, who wants it, for what, and why is difficult enough. Offline, this determination is dictated by the four privacy variables of content, context, control, and contract. Online, each of these factors is somewhat altered by technological, legal, psychological, and normative forces uncontrollable at the individual level. The result places a heavy burden on individuals' communication of privacy entitlements and creates a tone of carelessness regarding privacy on social media.

II. CREATING A PRIVACY-SUPPORTIVE CONTEXT THROUGH CONTRACT

Unlike the NYPD,[121] an individual cannot singularly affect contextual change. An individual cannot control the technology offered by online service providers and OSN hosts. Individuals can exercise no influence over the privacy variables online, with the exception of one option: *contract*.

Private rule-making in the form of express user-to-user confidentiality contracts is perfectly tailored for the fickle concept of online privacy. After all, both privacy and contract are about self-determination.[122] Contract affords individuals the opportunity to autonomously circumvent uncontrollable technology and elusive norms by determining for themselves what information is to be private, communicate those expectations, and set the value of their privacy. For example: *A* would like to share personal, nonpublic information (such as pictures of his family) with *B*, and *B* wants access to that digital information. *A* offers to share the material with *B* in exchange for *B*'s agreement to respect certain restrictions on its use and dissemination—for example, refraining from forwarding it to a third party, downloading or printing it, or disclosing its contents. These contracts would then form the basis of a web of trust and explicit expectations, enforceable through legal or nonlegal sanctions.

To be sure, not every contract would have to be readily enforceable in order for contract to establish pro-privacy social norms. After all, the great majority of unwarranted, embarrassing online disclosures—one scholar amusingly termed these "pinpricks"[123]—are not harmful enough to warrant the imposition of

121. *See supra* notes 11–13 and accompanying text.

122. Paul M. Schwartz, *Free Speech vs. Information Privacy: Eugene Volokh's First Amendment Jurisprudence*, 52 STAN. L. REV. 1559, 1564–65 (2000).

123. Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. CHI. L. SCH. ROUNDTABLE 75, 100 (2002) (defining "pinpricks" as invasions of privacy that result in minimal damages, such as

traditional contractual liability. It is only the exceptional online privacy violation that involves widespread shame and substantial damage to the aggrieved, such as loss of employment or death.[124] Even when not readily enforceable by legal means, the mere existence of a contract serves the important role of expressing and establishing social norms. I contend that by creating legal and nonlegal mechanisms to enforce the pinpricks, the context of abandonment on OSNs can be changed and the more serious breaches averted. Through its context-creating and communicative functions, contract can reduce privacy breaches while allowing intimacy to flourish and respecting freedom of expression. By establishing clear rules, the sender's privacy entitlement is more likely to be respected. By the information recipient's consent, the newly formed agreement transforms a morally optional activity (keeping another's information private) into an affirmative, morally (and sometimes legally) mandatory activity.[125] The obligation to keep a promise is stronger than the obligation to respect someone's ill-defined privacy.[126] Contract is also suited to protect online informational privacy because it is an ex ante system of governance that provides incentives and predictability. Minimal benefit accrues from obtaining monetary or even injunctive relief after harmful personal information is disseminated. Given the nature of digital information, the damage is already done and no longer containable at the moment of dissemination. In this light, it makes sense to have a mechanism by which dignitary damages are minimized or avoided before they occur.

Allowing individuals to protect their personal information online through contract is also critical if we want social media to foster the development of strong social bonds (rather than simple friend collection) and healthy identity exploration (rather than profile posturing). Cementing privacy expectations safeguards intimacy, which is an essential value of privacy.[127] As Charles Fried wrote, "Intimacy is the sharing of information about one's actions, beliefs or emotions which one does not share with all, and which one has the right not to share with anyone. By conferring this right, privacy creates the moral capital which we spend in friendship and love."[128] People welcome friends into their more intimate circle by sharing with them personal information to which nonintimates are not privy.[129] Relationship building is the natural byproduct of the

disruption of personal life).

124. For examples of these substantial violations, see *supra* notes 18–22 and accompanying text.

125. CHARLES FRIED, CONTRACT AS PROMISE 16–17 (1981).

126. *Id.*

127. ROSEN, *supra* note 44, at 215–16.

128. CHARLES FRIED, AN ANATOMY OF VALUES: PROBLEMS OF PERSONAL AND SOCIAL CHOICE 142 (1970).

129. ROSEN, *supra* note 44, at 11.

ability to sort and selectively distribute information.[130] As one commentator wrote:

> If individuals cannot form relationships of trust without fear that their confidences will be betrayed, the uncertainty about whether or not their most intimate moments are being recorded for future exposure will make intimacy impossible; and without intimacy, there will be no opportunity to develop the autonomous, inner-directed self that defies social expectations rather than conforms to them.[131]

Privacy is also tied to the creation of a healthy identity through the freedom of experimentation.[132] While OSN profiles are fertile ground for exploring different behaviors and identities, the widespread publication of these explorations to multiple audiences lays one bare. The ability to screen audiences and thereby maintain multiple personas is crucial for human beings, especially for curious teens and young adults.[133]

Contracting for privacy provides OSN participants with a common understanding of their own and others' expectations of privacy. In turn, understanding creates a sense of comfort, positively influencing future behavior and allowing for more, not less, sharing of information. People, especially those "who overreact to very low probability, but high visibility, reputational harms" would be more willing to reveal private information by participating online.[134]

Confidentiality contracts also circumvent the traditional concerns endemic to privacy law—the state-imposed speech restriction.[135] The Supreme Court has repeatedly held that self-imposed speech restrictions, such as those undertaken by the parties to a confidentiality agreement, do not implicate First Amendment scrutiny.[136] This is true even when the information protected is newsworthy or of legitimate public concern. In *Cohen v. Cowles*

130. *See id.*

131. Jeffrey Rosen, *The Purposes of Privacy: A Response*, 89 GEO. L.J. 2117, 2123–24 (2001).

132. Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381, 2398 (1996) (discussing the benefits of privacy).

133. Erving Goffman proposed that human beings control others' impression of them by a series of highly orchestrated social performances that necessarily differ between audiences. ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 34–35 (1959). Through these performances, an individual's identity is honed. *Id.* at 19–20. The ability to segregate audiences allows the individual freedom to explore with different behaviors and social roles. *Id.* at 49.

134. Strahilevitz, *supra* note 73, at 926–27.

135. Richards & Solove, *supra* note 50, at 179–80; Volokh, *supra* note 37, at 1057–61.

136. *See, e.g.*, Snepp v. United States, 444 U.S. 507, 509–10 (1980).

Media Co., a newspaper reporter breached an express promise to maintain the confidentiality of a source's identity.[137] The Court held that liability for the breach of a promise of confidentiality would not trigger First Amendment analysis because the parties had consented to a waiver of their First Amendment rights.[138] Following the reasoning in *Cohen*, many legal scholars have found contracts to be a reliable and constitutionally sound alternative to the incertitude of privacy law.[139] As Professor Volokh noted, "The great free speech advantage of the contract model is that it does *not* endorse any right to 'stop people from speaking about me.' Rather, it endorses a right to 'stop people from violating their promises to me.'"[140]

Notable legal scholars have suggested that contract is an effective mechanism for protecting privacy online. Lawrence Lessig imagined giving individuals "the ability to negotiate easily over privacy rights"[141] and ex ante control to negotiate the transfer of private information and set its value.[142] Professor Pamela Samuelson also compellingly argued for a contractual approach to protecting information online.[143] Touching on each of what I have termed "broken windows of privacy"—content, context, control, and contract, she reasons:

> One of the virtues of a contractual approach to protecting information privacy is that it can accommodate the multiple interests people have in personal information, the contextual nature of determinations about the appropriateness of collection or use of personal data, the significance of consent as a factor in determining appropriate uses, and the evolutionary nature of social understanding about information privacy. It is a flexible, adaptable, market-oriented way to allow individuals to control uses of personal data.[144]

Despite the respected opinions of these legal scholars and others, no well-established contractual approach for protecting the privacy of digital information exists. Pinning online interpersonal privacy on contract law has its obvious challenges. The formalism of contract requires that promises meet certain requirements before becoming legally enforceable; contract doctrine presents several hurdles to privacy protection.[145] Most significantly, it does not clearly provide redress for nonpecuniary harms or allow the parties

137. Cohen v. Cowles Media Co., 501 U.S. 663, 665–66 (1991).
138. *Id.* at 670–72.
139. *See, e.g*., Volokh, *supra* note 37, at 1061.
140. *Id.*
141. LESSIG, CODE, *supra* note 15, at 160.
142. *Id.* at 160–61.
143. *See* Samuelson, *supra* note 27, at 1172.
144. *Id.*
145. *See* McClurg, *supra* note 28, at 916–17.

to fashion their own remedial rights for a breach.[146] The remainder of this Part will analyze privacy contracts from the legal perspective, and the following Subsections will address the technical and normative issues associated with implementing them online, proposing a workable and standardized delivery mechanism for contract that overcomes the vehicle's burdensome transactional costs.

A. Enforceability of Confidentiality Agreements

Confidentiality agreements, also termed nondisclosure agreements or contracts of silence, are an increasingly common mechanism for protecting privacy.[147] They are commonly employed in prenuptial agreements, litigation settlement agreements (including divorce), and contracts to shield the identity of media or police sources and sperm or egg donors.[148] While the specific rules for determining enforceability of these agreements vary from state to state, most courts will uphold them if they meet the formalities of contract law (i.e., mutual assent, consideration, compliance with the statute of frauds,[149] etc.), are reasonable under the circumstances,[150] are not overbroad,[151] protect information that is not generally known or easily ascertainable,[152] and are not illegal or against public policy.[153]

146. *See* RESTATEMENT (SECOND) OF CONTRACTS § 353 (1981) (limiting recovery for emotional distress); JOHN D. CALAMARI & JOSEPH M. PERILLO, CONTRACTS § 14-31, at 530 (6th ed. 2009).

147. *See* McClurg, *supra* note 28, at 917.

148. *See, e.g.*, Johnson v. Superior Court, 95 Cal. Rptr. 2d 864, 867 (Ct. App. 2000) (determining the validity of an agreement protecting the identity of a sperm donor); Trump v. Trump, 582 N.Y.S.2d 1008, 1009 (App. Div. 1992) (enforcing a confidentiality provision in a prenuptial agreement); *see also* Garfield, *supra* note 116, at 273–74 (discussing confidentiality contracts to protect the identity of media and police sources); *id.* at 332–36 (discussing confidentiality provisions in litigation settlement agreements).

149. Most confidentiality agreements do not have to be evidenced by a writing, as most are indefinite in duration and therefore capable of performance within one year. *See* RESTATEMENT (SECOND) OF CONTRACTS § 130 (1981).

150. *See, e.g.*, Henry Hope X-Ray Prods., Inc. v. Marron Carrel, Inc., 674 F.2d 1336, 1342 (9th Cir. 1982) (finding nondisclosure provisions reasonable even without time and geographical limitations); Sunstates Refrigerated Servs., Inc. v. Griffin, 449 S.E.2d 858, 860 (Ga. Ct. App. 1994) (holding a nondisclosure provision enforceable because it was reasonable as to time period covered and information protected).

151. *See, e.g.*, Serv. Ctrs. of Chi., Inc. v. Minogue, 535 N.E.2d 1132, 1137 (Ill. Ct. App. 1989) (finding that a nondisclosure provision requiring an agent to keep secret information "concerning or in any way relating" to services offered was overbroad).

152. *See, e.g.*, Am. Software USA, Inc. v. Moore, 448 S.E.2d 206, 209 (Ga. 1994) (finding reasonable a nondisclosure covenant that is limited to "trade secrets" and "confidential business information" not publicly available or properly learned from a third party).

153. For example, in *Follmer, Rudzewicz & Co. v. Kosco*, 362 N.W.2d 676,

1. Mutual Assent

Most courts have held online click-wrap or browse-wrap contracts to be enforceable based on very minimal evidence of assent.[154] Mere access can constitute legally binding consent.[155] In some cases, the courts have held browse-wrap licenses enforceable when the license was simply posted online stating that the use of the product or website would constitute acceptance of the terms by the user.[156] If these standardized mass contracts have met the standards for legally binding consent, surely a user-to-user system would. Because of their relational proximity and bargaining parity, those communicating online are in the best position to ascertain the costs and benefits of their online confidentiality contracts. Further, OSN users have direct contact with each other and are therefore in a good position to negotiate and understand their legal obligations.

As with those contracting for confidentiality in physical space, online transactors must make clear that the agreement manifests objective intent to be legally bound. Absent clear indications of intent to enter into a legally binding contract, some courts have been unwilling to enforce agreements in contexts in which casual arrangements are the norm.[157] For example, *Cohen v. Cowles Media*

684 (Mich. 1984), the Michigan Supreme Court stated, "An agreement that unduly limits a former employee's freedom to go into business for himself or another, or extracts an excessive price for the privilege of doing so, is unreasonable and hence unenforceable." *See also* Ingersoll-Rand Co. v. Ciavatta, 542 A.2d 879, 894–95 (N.J. 1988) (noting that the public's interest in safeguarding commercial information must be balanced against the interest in fostering creativity and invention).

154. *See, e.g.*, ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996); Universal Grading Serv. v. eBay, Inc., No. 08-CV-3557, 2009 U.S. Dist. LEXIS 49841, at *70 (E.D.N.Y. June 10, 2009); A.V. v. iParadigms, LLC, 544 F. Supp. 2d 473, 484–85 (E.D. Va. 2008), *aff'd*, 562 F.3d 630 (4th Cir. 2009); Forrest v. Verizon Commc'ns, Inc., 805 A.2d 1007, 1013 (D.C. 2002); Scott v. Bell Atl. Corp., 726 N.Y.S.2d 60, 63–67 (App. Div. 2001), *modified by* Goshen v. Mut. Life Ins. Co., 774 N.E.2d 1190, 1194 (N.Y. 2002).

155. RealPage, Inc. v. EPS, Inc., 560 F. Supp. 2d 539, 545 (E.D. Tex. 2007); Cairo, Inc. v. CrossMedia Servs., Inc., No. C-04-04825-JW, 2005 WL 756610, at *5 (N.D. Cal. Apr. 1, 2005); DeJohn v. TV Corp. Int'l, 245 F. Supp. 2d 913, 918–19 (N.D. Ill. 2003).

156. *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 428–30 (2d Cir. 2004). *But see* Specht v. Netscape Commc'ns Corp., 306 F.3d 17, 31–35 (2d Cir. 2002) (finding that plaintiffs who downloaded software did not consent to terms and conditions accessed via a hyperlink that required scrolling below the "Download" button).

157. *See, e.g.*, Ruzicka v. Conde Nast Publ'ns, Inc., 939 F.2d 578, 582 (8th Cir. 1991) (dismissing contract action brought by plaintiff, the subject of a magazine article on sexual abuse, for the author's revelation of the plaintiff's identity in breach of a promise that she would be unidentifiable), *vacated*, 999 F.2d 1319 (8th Cir. 1993); Doe v. ABC, 543 N.Y.S.2d 455, 455–56 (App. Div. 1989) (granting summary judgment against plaintiffs on intentional infliction of emotional distress claim based on alleged promise by TV station that plaintiffs' faces would be unrecognizable during a program on rape victims, allowing the

Co., the United States Supreme Court case discussed above, was decided on promissory estoppel grounds because the Minnesota Supreme Court was reluctant to interpret the context of newsgathering as one in which people would "ordinarily believe they are engaged in making a legally binding contract."[158] Since contracting with friends or family members for interpersonal privacy is unconventional, privacy transactors must ensure that both parties are aware of the legal nature of the promise.

2. Minors

Contracts entered into by a minor are voidable at the minor's guardian's option.[159] The minor and his guardian can therefore either avoid or enforce the contractual obligation, but such obligations cannot be enforced against them.[160] This leads to desirable results: adults cannot keep their secrets safe with minors, but minors and their parents can keep their secrets safe with adults if they so desire. There is precedent for the proposition that minors and their parents can enforce confidentiality contracts against other adults.[161] Contracts for confidentiality would be a valuable resource for teenagers, who predominantly populate social networking sites and are apt to overshare.[162] The ability to contract for interpersonal privacy could protect minors from sexual predators, overzealous school officials, and the permanent tarnishment of their reputations.

3. Proprietary Versus Nonproprietary Information and Consideration

Confidentiality agreements are common in the commercial context, such as in employment relationships, in which proprietary information and trade secrets are established as economic interests that warrant protection.[163] The trade secret model of confidentiality agreements is a mixed bag of contract, tort, and property rights.[164] Other enforceable confidentiality agreements protect nonpecuniary interests; these include security, reputation, identity, intimacy,

action to proceed on grounds of breach of contract and negligent infliction of emotional distress).

158. Cohen v. Cowles Media Co., 457 N.W.2d 199, 203 (Minn. 1990), *rev'd on other grounds*, 501 U.S. 663 (1991).

159. RICHARD A. MANN & BARRY S. ROBERTS, BUSINESS LAW AND THE REGULATION OF BUSINESS 260 (9th ed. 2008).

160. ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 6, at 11 (1992).

161. Keltner v. Wash. County, 800 P.2d 752, 753 (Or. 1990) (seeking to enforce a confidentiality promise by a police officer to a mother and her fourteen-year-old daughter).

162. According to the Pew Internet and American Life Project, seventy-three percent of wired American teenagers use social networking sites. AMANDA LENHART ET AL., PEW RESEARCH CTR., SOCIAL MEDIA AND YOUNG ADULTS 4 (2010).

163. *See* Volokh, *supra* note 37, at 1071.

164. *Id.* at 1070–71.

peace of mind, and other values associated with privacy.[165]

The subjects of confidentiality agreements governing privacy are primarily noneconomic and nonproprietary.[166] This, of course, does not mean they are exempt from the requirement of consideration.[167] In the majority of these cases, the very exchange of the desired information constitutes consideration.[168] For example, private thoughts and opinions, personal images of oneself or one's family members, and locational information are not property interests and, for the most part, are highly valued only by their subjects.[169] While the privacy proponent may not have intellectual property rights to, say, a photograph of his infant daughter (taken by someone other than himself), he has a valuable privacy interest in it. Limiting its dissemination may bring him security and peace of mind; sharing it with a select few will bring him pleasure and emotional well-being. A promise of confidentiality is given as a precondition of receiving the benefit or the information. Being granted access to the subject information is a benefit that would not otherwise exist. Once the subject information is in the recipient's possession, however, she obtains the default right to disseminate it.[170] By promising to forego this right, she is undertaking an obligation that would not otherwise exist and is cementing binding consideration.

4. Information Not Generally Known or Readily Ascertainable

As one court put it, "[A]n agreement cannot make secret that which is not secret."[171] Fundamentally, a confidentiality agreement cannot shield information that is publicly available.[172] This limitation places the burden on the privacy proponent to limit the accessibility of the subject information to those who have agreed to his terms. In a social world, this can get quite messy. For example, assume two people have jointly filmed a video of themselves dancing at a party.[173] Person *A* wishes to keep the contents of the video a

165. *See* Garfield, *supra* note 116, at 272–73.

166. *See id.*

167. *See, e.g.*, *id.* at 268; *see also* Pressman v. United States, 33 Fed. Cl. 438, 444 (1995) (declaring confidentiality agreement void for lack of consideration).

168. McClurg, *supra* note 28, at 917.

169. There may be a property interest in certain private information. In these cases, copyright could serve as a "back door" to protect privacy. However, the property model does not apply to the majority of information one might desire to keep under wraps. For example, an individual does not have a proprietary interest in his own image (unless he somehow took the picture of himself and thereby gained the copyright), in his locational information, or in his financial or health information.

170. *See* Gilles, *supra* note 51, at 23–25.

171. Dynamics Research Corp. v. Analytic Scis. Corp., 400 N.E.2d 1274, 1288 (Mass. App. Ct. 1980).

172. *See id.*

173. The entanglement of rights is messy, indeed. For purposes of focusing

secret. *B*, who is less inhibited than *A* and also has access (and intellectual property rights) to the video, makes it publicly available on her OSN profile. *A* and *B* have the same rights to the video, but by making it publicly available, *B* has limited *A*'s rights significantly. In this case, *A* can no longer control the subsequent transfer of the video through contract, as it is otherwise accessible to potential transferees and they would not need to bargain with him over limitations on its dissemination in order to obtain access. This problem is best solved through explicit understandings at the time the image or video is captured. Of course, while the images of the video can be kept under wraps, the bare fact that *A* was dancing with *B* may not be if this was done in public and the information has become part of the public domain.

5. Illegality and Public Policy Considerations

Like other contracts, in order to be enforceable, confidentiality agreements must be legal and cannot contravene public policy.[174] For example, in jurisdictions where "sexting" is illegal, a confidentiality agreement purporting to cover the digital dispatch of nude photographs is not enforceable.[175] Although the Supreme Court has held that promises of confidentiality are exempt from First Amendment scrutiny, contracts designed to limit expression are particularly vulnerable to attack on public policy grounds, especially those protecting nonpecuniary interests such as privacy and reputation.[176] One can easily imagine confidentiality agreements that protect reputation at the cost of negative societal consequences: a service provider buying a consumer's silence regarding a dangerous product defect or a person with a contagious sexually transmitted disease seeking to hide his condition so as not to limit his pool of potential sexual partners. The public policy analysis acts to ensure that socially valuable speech is not unduly silenced by private law. This scrutiny involves a balancing of the need to protect the secrecy of the information against society's

on each party's privacy rights, I have chosen to assume away the intellectual property issues that commonly arise in these situations. For an incisive analysis of intellectual property and privacy rights in video, see Jacqueline D. Lipton, *"We, the Paparazzi": Developing a Privacy Paradigm for Digital Video*, 95 IOWA L. REV. 919 (2010).

174. RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981).

175. Sexting has been defined as "the practice of sending or posting sexually suggestive text messages and images, including nude or semi-nude photographs, via cellular telephones or over the Internet." N. Pieter M. O'Leary & Kathryn M. Caretti, *When Clean Kids Take Dirty Pictures: The Sexting Phenomenon and Its Impact on American Teenagers, the Criminal Justice System, and Parental Responsibility*, CHILD. LEGAL RTS. J., Winter 2009, at 65, 66 (citing Miller v. Skumanick, 605 F. Supp. 2d 634, 637 (M.D. Pa. 2009)). Many jurisdictions have turned to various existing statutes in an effort to find sexting illegal. *Id.* at 71–72.

176. Garfield, *supra* note 116, at 266, 323.

competing need for disclosure.[177] Courts have routinely set aside confidentiality agreements in instances when silence would have permitted suppression of criminal activity[178] or discreditable facts,[179] when the information was properly sought by the government under a federal statute,[180] or simply when a celebrity plaintiff failed to present evidence "establishing an overriding interest in keeping his lifestyle private."[181]

B. The Doctrinal Shortcomings of Contract in Addressing Privacy

Contract best protects only those transactors who obtain commitments in the appropriate legal form. Its successful execution and enforcement carries considerable costs that are not justifiable or available for every instance of psychological discomfort.

1. Lack of Privity with Third Parties

Only transacting parties may benefit from contract rights.[182] When a contract governs the disclosure of information, the individual seeking protection is charged with obtaining the consent of everyone to whom the information is disseminated.[183] One break in the chain of trust is all it takes for the subject information to become freely distributable and viral. Consider the following scenario: *A* secures a privacy promise from *B* in exchange for giving her access to details about his marital strife. *B* breaches the contract by copying and pasting *A*'s thoughts and sending the information to *C*, *D*, and *E*, who each share the digital information

177. Town of Newton v. Rumery, 480 U.S. 386, 392 (1987) ("[A] promise is unenforceable if the interest in its enforcement is outweighed in the circumstances by a public policy harmed by enforcement of the agreement."); *see also* RESTATEMENT (SECOND) OF CONTRACTS § 178 (1981).

178. *See, e.g.*, Lachman v. Sperry-Sun Well Surveying Co., 457 F.2d 850, 854 (10th Cir. 1972) (permitting disclosure of misappropriation of oil from neighboring property); Bowman v. Parma Bd. of Educ., 542 N.E.2d 663, 666 (Ohio Ct. App. 1988) (setting aside confidentiality agreement in order to investigate child molestation charges against a teacher).

179. *See, e.g.*, Allen v. Jordanos' Inc., 125 Cal. Rptr. 31, 34 (Ct. App. 1975) (refusing to uphold an employee's complaint for breach of contract and defamation against his former employer and others); Carol M. Bast, *At What Price Silence: Are Confidentiality Agreements Enforceable?*, 25 WM. MITCHELL L. REV. 627, 661–91 (1999) (discussing confidentiality agreement enforceability vis-à-vis whistleblowers).

180. *See, e.g.*, EEOC v. Astra USA, Inc., 94 F.3d 738, 745 (1st Cir. 1996) (holding confidentiality agreement void when employees agreed not to disclose their sexual harassment claims to the EEOC).

181. *See, e.g.*, Kerkorian v. Kerkorian, No. B158182, 2003 Cal. App. LEXIS 2539, at *47 (Ct. App. Mar. 17, 2003) (discussing billionaire Kirk Kerkorian's divorce).

182. Niva Elkin-Koren, *What Contracts Cannot Do: The Limits of Private Ordering in Facilitating a Creative Commons*, 74 FORDHAM L. REV. 375, 406 (2005).

183. *Id.* at 402–07.

at will. Although *A* has an actionable claim for breach of contract against *B*, he has no recourse against subsequent disseminators with whom he has not secured confidentiality promises.

For this reason, some have argued that contract alone cannot solve privacy issues in the information age; rather, it should be complemented by property law, which allows covenants to run with the assets. As one commentator put it, "Can contracts alone change social norms? Yes, they can. Many of our social practices are rooted in basic voluntary agreements. Yet, to be successful, this strategy requires that contracts . . . be made enforceable against third parties."[184]

Indeed, other systems of law embrace the extension of the duty of confidentiality beyond the parties to the original contract. Under English law, which gives much more deference to confidentiality than American law, a third party will owe an equitable obligation of confidence to the information's originator if the third party receives it with notice of its confidentiality.[185] If he knows the information is subject to a confidentiality agreement, the third party is bound to refrain from making unauthorized use of it.[186] Under the English rule, the third party may even be liable in tort for inducing a breach of a confidentiality contract.[187]

Where contract law falls short in the United States, nonlegal mechanisms exist for creating a downstream chain of trust. For example, law firms and businesses routinely include lengthy clauses at the end of their emails flagging confidentiality of their written communications and requesting that unintended readers respect it.[188]

2. Damages and Remedies

When promises to keep something secret are broken, society attributes moral blame to the "blabbermouth," regardless of the

184. *Id.* at 402.

185. Attorney Gen. v. Observer, Ltd., (1990) 1 A.C. 109, 268 (H.L.) (appeal taken from Eng.); Campbell v. MGN Ltd., [2002] EWCA Civ 1373, [2003] Q.B. 633, 662.

186. *Campbell*, [2003] Q.B. at 662.

187. Normann Witzleb, *Justifying Gain-Based Remedies for Invasions of Privacy*, 29 OXFORD J.L. STUD. 325, 329 n.5 (2009) (Eng.). This is seldom the case under U.S. law, although some third parties have been held liable in tort when they intentionally induced the breach. *See* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617, 661–65 (2002) (discussing cases of third party tort liability for breach of confidentiality in the medical context).

188. Such language typically reads, "If the reader of this electronic message is not the named recipient, or the employee or agent responsible to deliver it to the named recipient, you are hereby notified that any dissemination, distribution, copying or other use of this communication is strictly prohibited and no privilege is waived."

damage actually incurred by the disclosure's victim.[189] An apology, an explanation, or acts of contrition ensue. Friendship ties might be severed and the discloser may gain a reputation for being loose-lipped or untrustworthy. When a promise of confidentiality is also a contract, the promise becomes enforceable as a legal duty as well as a moral one.[190] The aggrieved in this latter case must prove either that he incurred measurable, verifiable, and compensable harm as a result of the breach in order to receive monetary damages, or that such damages are likely to occur absent injunctive relief.[191] For the victim of an online privacy breach, proving damages may be an insurmountable task, and even if these were proven, neither remedy may be wholly satisfactory.

Injunctive relief is the most common remedy imposed for a breach of a confidentiality agreement, particularly when dissemination is not yet widespread.[192] When discussing contracts to ensure privacy, a primary concern is the chilling of speech through contract.[193] One commentator has suggested injunctive relief as an appropriate remedy once a digital disclosure has been made "to prevent further, ongoing harm where damages will be inadequate to protect the expectation interest of the injured party."[194] Although generally available for contract and property-related breaches, injunctive relief may not be adequate to limit the damage caused by an online disclosure that has already gone viral. The inherent nature of information precludes repossession as an option, especially online. The online context guarantees that widespread dissemination is inevitable, regardless of whether the original divulger is legally restricted from further spreading the damaging information.[195]

Once information is widely published, most victims of online confidentiality breaches are likely to seek damages for emotional distress, reputation loss, job loss, and value of time spent evaluating potential harm incurred by the dissemination—all consequential in nature and seemingly tort-like.[196] In contrast, the damages recoverable in contract are generally restricted to expectation damages for pecuniary harm.[197] In *Keltner v. Washington County*,

189. *See* McClurg, *supra* note 28, at 905–06.
190. *Id.* at 888–89.
191. *See id.* at 934–37.
192. *See* E.I. DuPont de Nemours & Co. v. Am. Potash & Chem. Corp., 200 A.2d 428, 431 (Del. Ch. 1964); Concept, Inc. v. Thermotemp, Inc., 553 So. 2d 1325, 1327 (Fla. Dist. Ct. App. 1989); Gonzales v. Zamora, 791 S.W.2d 258, 267 (Tex. App. 1990).
193. *See* McClurg, *supra* note 28, at 908.
194. *See id.* at 936.
195. ROSEN, *supra* note 44, at 7–8.
196. *See* McClurg, *supra* note 28, at 887–88.
197. 11 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 59.1, at 539 (Joseph M. Perillo ed., 2005).

the Supreme Court of Oregon refused to grant contract damages for the mental suffering caused by a breach of confidentiality.[198] In that case, a police officer breached a promise of confidentiality to a fourteen-year-old girl who had agreed to divulge information about a murder after the police agreed to not divulge her name. Despite the psychological discomfort caused by the revelation of her identity to the accused perpetrator and the fact that emotional security was the "very object of the promised confidentiality," the Supreme Court of Oregon refused to grant relief, reasoning that contract damages were not within the contemplation of the parties and too remote and consequential to be actionable.[199] Although contract law is not accustomed to providing redress for dignitary harms, other courts have granted relief when the measure of damages was foreseeable in light of the subject matter of the contract.[200] Such is the case when morticians mishandle bodies,[201] caretakers are negligent with children,[202] contractors build defective homes, and employers engage in wrongful firing.[203] In fact, the *Restatement (Second) of Contracts* provides two important exceptions to the general rule against awarding contract damages for emotional disturbance: damages may be proper if "the breach also caused bodily harm" or "the contract or the breach is of such a kind that serious emotional disturbance was a particularly likely result."[204]

198. Keltner v. Wash. County, 800 P.2d 752, 758 (Or. 1990).

199. *Id.* at 757–58 (quoting Adams v. Brosius, 139 P. 729, 731 (Or. 1914)). Other states, such as South Carolina, also have rules absolutely forbidding the award of emotional distress damages in contract actions. *See* Whitten v. Am. Mut. Liab. Ins. Co., 468 F. Supp. 470, 479 (D.S.C. 1977), *aff'd*, 594 F.2d 860 (4th Cir. 1979).

200. *See, e.g.*, Huskey v. Nat'l Broad. Co., 632 F. Supp. 1282, 1293 (N.D. Ill. 1986) ("[C]ontracts not to invade privacy are contracts whose breach may reasonably be expected to cause emotional disturbance . . . ."); Stockdale v. Baba, 795 N.E.2d 727, 744 (Ohio Ct. App. 2003) (permitting the recovery of emotional distress damages for breach of contract given the "intensely personal" nature of a contract for privacy).

201. *See, e.g.*, Lamm v. Shingleton, 231 N.C. 10, 13–14, 55 S.E.2d 810, 812–13 (1949).

202. Lane v. KinderCare Learning Ctrs., Inc., 588 N.W.2d 715, 717–18 (Mich. Ct. App. 1998).

203. Fogleman v. Peruvian Assocs., 622 P.2d 63, 65 (Ariz. Ct. App. 1980).

204. RESTATEMENT (SECOND) OF CONTRACTS § 353 (1981). Scholars have suggested taking the *Restatement (Second)* rule a step further by advocating that contract accommodate nonpecuniary interests such as pleasure, relaxation or peace of mind, and others typically secured by confidentiality contracts. Professor Tomain suggested that damages for nonpecuniary losses should be awarded through breach of contract "when the parties enter into a bargain which has as its principal function the exchange of a non-pecuniary interest." Joseph P. Tomain, *Contract Compensation in Nonmarket Transactions*, 46 U. PITT. L. REV. 867, 903–04 (1985). Professor Whaley proposed granting relief for emotional distress in contract actions any time damages are foreseeable and established with reasonable certainty. Douglas J. Whaley, *Paying for the Agony: The Recovery of Emotional Distress Damages in Contract Actions*, 26

Both *Restatement (Second)* exceptions are applicable to sensitive information shared online in the context of a confidentiality agreement. Examples abound of physical dangers resulting from online disclosures.[205] Further, the damages arising from a breach of online confidentiality are eminently foreseeable by both parties, especially when the information exchanged is particularly sensitive or embarrassing in nature and this is made clear to the promisor before transmittal.

Although potential damages are likely to be foreseeable given the nature of the contract, embarrassed plaintiffs still face an uphill battle establishing and quantifying their emotional distress to a reasonable certainty. Shame, or a more generalized injury to the mind, is easily feigned and difficult to prove, even though it may be very real.[206] The determination of monetary damages is particularly difficult given the relatively low objective economic value of the types of information typically shared online[207] versus their high subjective value to the victim.[208] Parties could go as far as agreeing on reasonable liquidated damages for a breach of confidentiality, although this would increase transaction costs.[209]

Even when the formal requirements of contract are deficient, privacy promises can be enforceable under the theory of promissory estoppel.[210] If contract theories fail, the existence of explicit promises can go a long way toward proving a reasonable expectation of privacy in a tort suit for public disclosure or breach of confidence.

Both legal and practical challenges exist to employing contract to protect personal privacy. Although the ideal would be a legally enforceable contract, not all promises of confidentiality must be formal contracts in order to effectively safeguard privacy and counteract an "anything goes" attitude toward online privacy. Sociolegal scholarship indicates that the very existence of a promise or obligation can change social norms.[211] In that vein, the following Part proposes a workable model for conveying privacy preferences and promises in the online social world.

SUFFOLK U. L. REV. 935, 950–51 (1992).

205. *See supra* notes 20–22 and accompanying text (providing examples in the introduction).

206. Virginia E. Nolan & Edmund Ursin, *Negligent Infliction of Emotional Distress: Coherence Emerging from Chaos*, 33 HASTINGS L.J. 583, 620 (1982).

207. Most shared bits of information are not inherently economically valuable. One exception is images of celebrities, which sell on the open market to tabloids. In this case, the aggrieved celebrity might be able to claim lost profits as well. Keith D. Willis, Note, *Paparazzi, Tabloids, and the New Hollywood Press*, 9 TEX. REV. ENT. & SPORTS L. 175, 177–78 (2007).

208. *See* Weiser, *supra* note 123, at 81.

209. *See* Follmer, Rudzewicz & Co. v. Kosco, 362 N.W.2d 676, 679–80 (Mich. 1984) (assessing agreement on liquidated damages); *see also* McClurg, *supra* note 28, at 934–36 (discussing damages generally).

210. *See* Gilles, *supra* note 51, at 16.

211. *Id.* at 16.

III. FIXING THE BROKEN WINDOWS: A STANDARDIZED SYSTEM OF ONLINE USER-TO-USER CONFIDENTIALITY AGREEMENTS

Thus far, the apparent refusal of social-media hosts to intervene in interuser privacy disputes has led to an obvious lack of recourse for privacy matters, which, like social disorder, seems to breed in an environment of neglect and anarchy. As a result, there is currently no well-accepted enforcement mechanism for guarding privacy on social media fora in the United States.[212]

Any feasible proposal to protect privacy through contract must overcome the practical and legal hurdles discussed above. Professor McClurg has suggested legally enforcing privacy between intimates online by way of implied contracts of confidentiality.[213] His creative approach seeks to circumvent the need for an explicit meeting of the minds and thereby bind parties who are in a confidential relationship in the physical world to a fundamental agreement—not to harm each other by misusing or disseminating relationship-specific confidential information through an instrument of mass communication. In contrast, the proposal offered herein relies on express contracting between parties. In an environment of normative flux, explicit understandings are necessary, especially when it comes to an amorphous and capricious concept like privacy. Moreover, in a social world in which everyone is termed a "friend," privacy cannot hinge on the "default settings" of physical-world confidential relationships. Express contract obviates the hefty decisions of what content is appropriately private or what relationships merit confidentiality, turning these instead into factual determinations regarding the intent of the parties.[214] In an informal, interpersonal context in which people do not conventionally resort to contract, an explicit contract is ideal to manifest objective intent to be legally bound.[215] Finally, explicit contracts reduce negotiation and enforcement costs, as parties are not charged with reconstructing and proving their understandings at the time of contract.[216] For a formal standardized confidentiality system to emerge online, existing contract models must be married with existing technology for online contracting and dispute resolution.

A. Forming Online Confidentiality Agreements

The Creative Commons, a social movement and nonprofit organization founded in 2001 by Professor Lawrence Lessig, has set

212. *See* Jonathan Zittrain, *Privacy 2.0*, 2008 U. CHI. LEGAL F. 65, 106.
213. McClurg, *supra* note 28, at 915–17.
214. Gilles, *supra* note 51, at 24.
215. *Id.* ("A written agreement to keep a confidence seems to preclude any claim that there was no intent to contract and minimizes the chances that the terms are vague or unprovable.").
216. *Id.* at 24–25.

out to influence the legal environment of intellectual property by altering social norms.[217] It seeks to empower creators of intellectual property to grant tailored copyright permissions to their work while balancing the social interest in maximizing the flow of information.[218] To achieve this daunting task, the Creative Commons takes a bottom-up approach: introduce a user-friendly alternative convention for intellectual property exchange.[219] Creative Commons licenses enable copyright owners to easily change their copyright terms from the default of "all rights reserved" to "some rights reserved."[220] Creators may choose from a set of conditions that they may wish to apply to their work, such as "Attribution" (permission to copy, display, and perform, provided the author is credited) and "No Derivative Works" (all uses permitted with the exception of derivative works).[221] The creator's preferences are communicated by way of short phrases accompanied by icons, which are now nearly ubiquitously recognized.[222] Prospective licensors may access the detailed licenses online.[223] These licenses are legally enforceable in both contract and property.[224]

As Jonathan Zittrain has casually suggested, a similar system for privacy can change the social landscape online.[225] As with Creative Commons licenses, the creator, in this case referred to as the "privacy proponent," would attach certain restrictions or conditions of use to the proposed information or material to be shared. These would be represented by short phrases and icons, each representing the terms of a confidentiality agreement accessible online. Privacy-related conditions could include: "Unlimited Share" (permission to view, disclose, disseminate, download, and print); "Share Only Within My Network" (permission to share and disclose within a group predefined by the privacy proponent); "View Only" (permission to view but not to share, forward, disseminate, download, or print); and "Confidential"

217. Creative Commons, History, http://creativecommons.org/about/history (last visited Sept. 14, 2010).

218. Creative Commons, FFAQ, http://wiki.creativecommons.org/FFAQ (last visited Sept. 14, 2010).

219. Creative Commons, What Is CC?, http://creativecommons.org/about /what-is-cc (last visited Sept. 14, 2010).

220. *Id.*

221. Creative Commons, Licenses, http://creativecommons.org/about/licenses (last visited Sept. 14, 2010).

222. *Id.*; *see also* Association Littéraire et Artistique Internationale, *Memorandum on Creative Commons Licenses*, 29 COLUM. J.L. & ARTS 261, 265 (2006).

223. Creative Commons, Licenses, http://creativecommons.org/about/licenses (last visited Sept. 14, 2010).

224. *See, e.g.*, Jacobsen v. Katzer, 535 F.3d 1373 (Fed. Cir. 2008).

225. Zittrain, *supra* note 212, at 106 ("There is no Privacy Commons license to request basic limits on how one's photographs ought to be reproduced from a social networking site. There ought to be.").

(permission to access information, but recipient may not disseminate, disclose, or discuss its contents). The prospective recipient of the information is given the opportunity to review the detailed terms online and manifest consent by accepting the information exchange, thereby promising to abide by the information restriction and entering into a legally enforceable contract.

Privacy is, of course, not intellectual property. Although both represent nontangible interests, privacy is based on dignitary rights while intellectual property is based on proprietary rights; the law covering each area offers distinct protections to each.[226] That said, the Creative Commons system sets out to kick-start creativity by calibrating information dissemination, which is unduly restricted by default intellectual property rules.[227] Privacy law defaults, on the other hand, are unduly permissive and therefore are also in need of calibration.[228] The Creative Commons model could do for intimacy and human dignity what it has heretofore accomplished with creativity.

Unlike the Creative Commons licenses—enforceable in property as well as contract law—the basis of user-to-user confidentiality agreements is solely in contract. Individuals do not have a proprietary interest in their images, their observations, or their opinions, just as they have no privacy interest in their publicly available names, telephone numbers, and addresses.[229] They therefore cannot impose unilateral use restrictions that run with the protected information, such as those that ring in property law. Individuals seeking to protect their information from reaching unintended destinations are required to secure the consent of everyone to whom the information is disseminated.[230]

Such a standardized system allows individuals to communicate and control the terms of their privacy expectations and information flow in the form of an express offer to contract. It is user-friendly, nonlegalistic, and reduces the significant transaction costs relating to express contracts discussed above. Since the terms are imposed by their friends and loved ones, individuals are less likely to ignore them because they may have a meaningful opportunity to control the terms through bargaining. Although the system enables the privacy proponent to restrict the flow of his information through promises, it will not chill speech. Instead, the comfort provided by explicit promises is likely to promote online interactions of a more intimate and confidential nature.

226. Volokh, *supra* note 37, at 1051–52.

227. Creative Commons, FFAQ, http://wiki.creativecommons.org/FFAQ (last visited Sept. 14, 2010).

228. *See* Abril, *supra* note 54, at 3.

229. *Id.* at 5.

230. Elkin-Koren, *supra* note 182, at 406.

By employing short phrases and icons, and interpreting acceptance as consent, this system bypasses the social negotiation costs inherent in asking friends for privacy and overcomes the burden of reading privacy policies. Several notable consumer-oriented projects have recently advocated the use of simple graphic representations to clarify privacy policies.[231] Others have proposed employing such icons in email.[232]

While agreements made between intimates are not usually made with legal enforceability in mind, a new set of norms must emerge to address breaches of privacy online and foster online intimacy. There is certainly precedent for social norms influencing contract law, as is clear from emerging private law in traditionally privately enforced matters such as paternity, surrogacy contracts, and negotiated access to sexual intimacy.[233] A widespread framework for privacy agreements is a logical social reaction to the need for increased privacy vis-à-vis technology.

B. Enforcing Online User-to-User Confidentiality Agreements

A confidentiality agreement can, of course, be enforced through traditional legal channels. Such would foreseeably be the case when a user-to-user confidentiality agreement results in significant economic damage. In the case of the more common "pinpricks" of privacy, however, a system of third party dispute resolution is best suited to remedy online privacy incursions. In the absence of a perfect system of redress for confidentiality agreements, contract law should acknowledge nonlegal sanctions such as reputation monitoring and enforcement in this context.[234] Contract does not allow transactors to fashion their own remedies (such as banishment from an OSN or reputational sanction) for breach.[235]

231. *See, e.g.*, TRUSTe Blog, http://www.truste.com/blog/?p=531 (last visited Sept. 14, 2010). KnowPrivacy's website tracks and analyzes the privacy policies of leading websites, coding them with easy-to-understand icons. KnowPrivacy, Policy Coding Methodology, http://www.knowprivacy.org/policies_methodology.html (last visited Sept. 14, 2010); Aza Raskin, http://www.azarask.in/blog/post/is-a-creative-commons-for-privacy-possible/ (last visited Sept. 14, 2010).

232. The Privicons Project describes its approach as "washing instructions for email." Privicons.org, Why Privicons?, http://privicons.org/projects/why-privicons/ (last visited Sept. 14, 2010).

233. Michelle Oberman, *Sex, Lies, and the Duty to Disclose*, 47 ARIZ. L. REV. 871, 872–73 (2005) (discussing the emergence of these new types of contracts).

234. Volokh, *supra* note 37, at 1061 ("[P]erhaps there may even be special defaults related to such promises [of confidentiality] or special remedies for breaches of such promises.").

235. CALAMARI & PERILLO, *supra* note 145, § 14-31, at 530 (noting remedies for breach of contract are a matter of public, not private law); Fairfield, *supra* note 82, at 451 ("Would a court order a virtual-world provider to take specific action (ban a bad actor, return virtual objects or land) based on one user's assertion of contract claims against another user? These questions remain unsettled at best.").

However, under existing doctrine, parties to an agreement can contractually defer judgment to an arbitrator or mediator who is entitled to determine appropriate remedial rights, which can include nonlegal sanctions.[236] In fact, contract scholars have long recognized the ability of nonlegal sanctions to improve the welfare of transactors.[237] There is now abundant precedent for the successful establishment of systematized nonlegal sanctions and dispute resolution among online transactors.[238] These third-party systems are proven to reduce transaction costs and legal hurdles and instill confidence online.[239] By leveraging reputation, they compress loose-knit groups into close-knit ones. Commercial auction giant eBay established an electronic reputation system in which members rate and document their experiences with others.[240] This system has succeeded in creating context for what has become a close-knit group of over ninety million active users.[241] Wikipedia has also incorporated a successful collective self-policing mechanism for information-related violations that includes systems for interpersonal negotiation, solicitation of third party opinions, surveys among a jury of peers, and both formal and informal mediation.[242]

236. *See* Garrity v. Lyle Stuart, Inc., 40 N.Y.2d 354, 357 (Ct. App. 1976) ("It is also true that arbitrators generally are free to fashion the remedy appropriate to the wrong . . . but an authentic remedy is compensatory and measured by the harm caused and how it may be corrected.").

237. *See, e.g.*, David Charny, *Nonlegal Sanctions in Commercial Relationships*, 104 HARV. L. REV. 373, 375–79 (1990). Even before the Internet upsurge, Professor David Charny analyzed the paradigms for nonlegal enforcement, which include reputational enforcement by third parties and market participants. Charny discusses four nonlegal paradigms, two of which are "Third-Party Decisionmaking with Reputational Enforcement" (the community of transactors recognizes an authoritative nonlegal decision maker and reputational sanctions force transactors to comply with the decision makers' judgments) and "Reputational Monitoring by Market Participants" (a large number of potential transactors monitor conduct and the "collective decisionmaking process causes reputation to adjust stochastically over a range of possible values"). *Id.* at 409–20.

238. *See infra* notes 245–48 and accompanying text.

239. *Id.*

240. The ratings then translate into graphical and numerical references signaling the transactor's reliability and trustworthiness. Negative feedback is the equivalent of a normative sanction. *See* Audun Jøsang et al., *A Survey of Trust and Reputation Systems for Online Service Provisions*, 43 DECISION SUPPORT SYST. 618, 631 (2007).

241. *See generally* Paul Resnick et al., *The Value of Reputation on eBay: A Controlled Experiment*, 9 EXP. ECON. 79, 79–101 (2006) (conducting extensive analysis on the use of eBay and the normative effect of user feedback); eBay, Inc., Who We Are, http://www.ebayinc.com/page/who (last visited Sept. 14, 2010).

242. The colossal open source online encyclopedia relies exclusively on user-generated content for its fifteen million articles, making unilateral verification and monitoring impracticable. Wikipedia, Wikipedia Statistics—All Languages, http://stats.wikimedia.org/EN/TablesWikipediaZZ.htm (last visited

C. An Ambitious Proposal?

Inspired by sociolegal scholarship on norms and enforcement, the foregoing proposal calls for the creation of a standardized system of user-to-user agreements that govern the confidentiality of information shared through OSNs. In the normative sense, it is ambitious: it calls for the employment of written promises in an area customarily governed by informal trust and goodwill. Legally and practically, it is not revolutionary, as existing legal and technological models for its implementation have long been available. Although confidentiality contracts are subject to close public policy scrutiny, their use to protect privacy has traditionally been upheld.[243] From a practical perspective, it is envisioned that an organization akin to Creative Commons would offer users a set of legally enforceable nondisclosure agreements covering a wide range of situations and with differing sample terms.[244] The agreements must make clear the foreseeable emotional or reputational consequences of breach, or perhaps establish reasonable, nonpunitive, liquidated damages in the event of disclosure. Users could either select from these terms to create individual End User License Agreements for their social networking profiles (consent to which would be a prerequisite to adding another user as a friend)[245] or pick and choose terms depending on the level of protection warranted for each confidence shared. A standardized system of icons communicates the user's contractual offer; accepting the information constitutes assent.

In the event of breach, an established convention of contract provides predictability and gravitas for online promises. While contract formalism does not impede the creation of such contracts, flexible interpretations of extant contract doctrines, such as the award of monetary damages for dignitary harms and the embrace of nonlegal sanctions, would facilitate contract creation. Technology and precedent exist for the successful administration of online dispute resolution or reputation systems. What is necessary is a party willing to administer it.[246] Social networking websites in the

Sept. 14, 2010). Parties disputing the accuracy of an article are first asked to negotiate with each other on the article's "Talk Page." They can request editor assistance, a third opinion, a survey, informal mediation, and formal, nonbinding mediation. Disputing parties arguing over user misconduct on Wikipedia opt for binding arbitration conducted by an internal arbitration committee. Wikipedia, Arbitration Committee, http://en.wikipedia.org/wiki/Wikipedia:Arbitration_Committee (last visited Sept. 14, 2010).

243. *See supra* notes 149–57 and accompanying text.

244. Professor McClurg has proposed a sample confidentiality agreement for intimates. McClurg, *supra* note 28, at 933.

245. This would be enforceable assuming the terms are not overbroad and the scope of the protected information is reasonable.

246. For example, this is the role SquareTrade played for eBay. SquareTrade, About Us, http://www.squaretrade.com/pages/about-us-overview

United States do not seem to be willing, given the sizable task and the fear of jeopardizing their CDA immunity. Perhaps an exception to the CDA could be carved out—one that would allow social network hosts to administer privacy-friendly systems of dispute resolution and reputational monitoring without fear of liability.

A combination of these existing models of communicating and enforcing entitlements empowers individuals while respecting people's differing need for privacy. Moreover, the mere existence of a network of promises can reduce the privacy risks in online communities.

CONCLUSION

Trust everybody, but cut the cards.[247]

For the past half century, sociologists and sociolegal scholars have explored how environment—everything from visual cues to legal rules—influences behavior. The Broken Window Theory posits that even minor, but perceptible, changes in the environment are likely to change behavior. While most of this scholarship has addressed the offline context, I contended in this Article that it equally applies to the online social world, which is suffering multiple "broken windows" that impact interpersonal privacy and intimacy online. I began by defining the dependent concept of privacy in terms of four variables—content, context, control, and contract—and argued that it is these same variables that are lost in translation on the digital medium, a universe subject to the fluctuations of normative and technological uncertainty. The result is an environment of social contagion in which privacy is devalued as an assumed risk, and therefore, anything goes. As evidenced by the Broken Window Theory, this context of carelessness only propagates privacy breaches.

Unlike the inherent volatility of privacy, contract provides predictability. Explicit confidentiality contracts communicate expectations of privacy, tailoring them beyond absolute terms while encouraging speech and intimacy between online participants. While individuals have little or no control over technology or how it is employed by host websites, individuals can influence the behavior of their counterparts through the legally binding promises afforded by contract. Users would no longer be uniquely bound to the vicissitudes of corporate terms of service and technology or the inadequacies of privacy tort law; they would be empowered to form, pursue, and enforce their own conceptions of privacy online. Ultimately, private ordering can change social norms. It acts as a

(last visited Sept. 14, 2010).

247. Adapted from FINLEY PETER DUNNE, MR. DOOLEY'S PHILOSOPHY 260 (Literature House 1970) (1900).

behavior control device: its very existence encourages parties to perform their promises and minimize their disputes. Enforcement of interpersonal promises, no matter how minor, cultivates an atmosphere of trust and intimacy where carelessness now thrives.