THE POSTER'S PLIGHT: BRINGING THE PUBLIC DISCLOSURE TORT ONLINE

*JAIME A. MADELL**

INTRODUCTION

On December 26, 2009, "Lee" posted the following to a Facebook[1] discussion board:

> Recently, someone I had denied acces [sic] as a friend wound up friending a friend of mine and gained access to my pictures and videos. She then posted them on her wall and now everone [sic] can see them. These are pictures and videos of my kids. I contacted facebook and I see the account is no longer valid. My suspicion is that she will create a new profile with different information and repost the videos/pictures as they are surley [sic] saved to her hard drive. Is this illegal and what can I do about it. The person in question is my mother and me and my siblings were taken away as a result of neglect. This was close to 16 yrs [sic] ago and I do not want any contact with her.[2]

Lee's question is remarkably nuanced. We might rephrase it like so: Can I hold somebody legally liable for (a) downloading a picture I have posted to an online social network (OSN) with the intent that it be viewed only by a specified group of people and (b) re-posting it so that it can be seen by people to whom I have not provided access?

There are two answers here, one more obvious than the other. The simple answer can be found on the discussion board itself. A sympathetic "Mathew" responded that: "The reality is you should not post stuff to the Internet you are worried about people seeing.

* J.D. Candidate 2011, New York University School of Law; Notes Editor, New York University Annual Survey of American Law; M.M., Honors, Northwestern University School of Music; B.A., *summa cum laude*, Columbia University. The Author wishes to thank Katherine Strandburg for her dedicated advising, the staff of the *New York University Annual Survey of American Law* for their assiduous editing, and Helen Nissenbaum, Ira Rubinstein, and the Privacy Research Group for their helpful comments.

1. As most readers know, Facebook is a popular online social network. For a discussion of online social networks, see *infra* Part I.

2. Posting of Lee, to *Stealing Pics from Someone and Reposting Them on Your Wall.*, FACEBOOK (Dec. 26, 2009, 4:07 PM) (on file with author).

Once it's online, it's almost impossible to keep it contained."[3] There's a lot right about this straightforward answer. Broadly speaking, the law does not protect information that people freely disclose, even if the extent of that disclosure is not commensurate with the eventual scope of dissemination. This is because privacy law in the United States is defined in large part by what many privacy scholars have termed the public–private dichotomy.[4] This dichotomy stems from a notion, embedded in Fourth Amendment jurisprudence, that what one discloses to third parties is no longer private in the eyes of the law. According to this line of thinking, the answer to Lee's question is simply "no."

This is not to say that Lee does not have a cause of action to pursue. Hence the second answer: Lee might look to the public disclosure tort for help. A relatively recent addition to American tort law, this tort aims to police those who give publicity to private facts.[5] In practice, however, the tort is both weak and doctrinally unstable, due in large part to varying approaches to its "legitimate concern" and "reasonableness" prongs.[6] Even before the days of the Internet, these requirements—protected information must be (a) non-newsworthy and (b) reasonably expected to remain private—were vague. This lack of clarity has been exacerbated by recent technological developments, many of which pose serious challenges to norms of information flow. For example, whereas it was once possible to assume that the newsworthiness of a given piece of information could be determined by using the media's decision to publish it as a benchmark, the proliferation of blogs and microjournalists has trounced the media-as-gatekeeper norm and rendered this proxy unreliable. The interpretative morass that has followed such developments significantly hampers the ability of harmed individuals to seek and receive legal redress.[7]

The failure of the public disclosure tort might not be a devastating loss in the online context, were information flows on online utilities to more thoroughly protect and preserve users' privacy ex-

3. Posting of Mathew, to *Stealing Pics from Someone and Reposting Them on Your Wall.*, FACEBOOK (Jan. 9, 2010, 2:58 PM) (on file with author).

4. *See, e.g.*, HELEN NISSENBAUM, PRIVACY IN CONTEXT 141 (2010).

5. The tort is thusly defined in the Second Restatement:

> "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter published is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public."

RESTATEMENT (SECOND) OF TORTS (1977). *See infra* Part II.

6. *See infra* Part II.A.

7. NISSENBAUM, *supra* note 4; *see infra* Part II.

pectations. A "perfect" Facebook would have preserved Lee's expectation that his posting decision would not result in sharing with his mother. This hypothetical Facebook would implement principles of information flow that satisfy a user's expectation that his decision to share only with specific parties will be respected.

If principles of information flow (expressed through OSN source code) preserved such expectations perfectly, there would perhaps be no need for law—technology would suffice. Unfortunately, prevailing code falls far short of such a lofty goal. Instead of bridging the gap between online information handling and individuals' expectations, code widens the divide. As Helen Nissenbaum explains in her book *Privacy in Context*, technologies such as OSNs handle information in ways that conflict with prevailing norms of information flow.[8] Unlike OSN policies,[9] these highly specific norms develop within a particular context (e.g., friendship) to match the expectations of those contexts (e.g., a photo shared with a close friend will not be disseminated).

Broadly speaking, this Note explores how law and code can help each other protect privacy online. As Lee's story demonstrates, technological change can encroach upon our entrenched notions of privacy. But by updating law and code to better match the behavioral realities of online culture, we can ensure that people do not find themselves caught in a web of unfamiliar norms. More specifically, this Note aims to demonstrate how the law-and-code collaboration can reinvigorate the public disclosure tort and help plaintiffs in Lee's situation.

Thus, though the problem of privacy online is far-reaching, this Note deals with only the issue of nonconsensual re-posting described in Lee's thread, a problem I call the Poster's Plight. I focus on the Poster's Plight for two reasons. First, the lack of legal protection for victims of nonconsensual re-posting clearly demonstrates the inadequacy of the current public disclosure tort. This inadequacy is troubling, as the public disclosure tort is one of the few legal tools available to plaintiffs in situations such as Lee's. Second, the Poster's Plight sheds light on the intersection of four important issues in the analysis of online privacy: (1) technological developments and the privacy risks they pose, (2) legal doctrines and their

8. *Id.*

9. For the purposes of this Note, a "policy" can be defined as a technologically determined principle of information flow. An example familiar to most readers would be the policy—built into email protocol—that senders cannot tell if their emails have been received.

ability to mitigate those risks, (3) code-based structures that mediate such risks, and (4) prevalent notions of privacy.

In Part I of this Note, I examine the psychology of privacy on OSNs and the divide between the contextually rich public perceptions of privacy and the dichotomous view built into OSN code. In particular, I demonstrate how OSN privacy controls fail to provide users with protections that fit their complex expectations of privacy. I also argue that because code alone cannot solve OSN privacy problems, law must intervene. In Part II, I examine the use of the public disclosure tort as a privacy tool, explain how its unstable doctrine fails to capture our basic intuitions of privacy, and suggest a more context-friendly approach to the reasonableness analysis. In Part III, I develop a hybrid legal–technical solution to the problem of nonconsensual picture re-posting on OSNs; in short, I propose a new OSN functionality that allows users to explicitly express disclosure preferences for the pictures they post.[10] I argue that, in conjunction with a modified reasonableness analysis, this functionality can go a long way to resuscitating the public disclosure tort in the digital age and helping restore context to interactions on online social networks.

I.
CONTEXTUALIZING THE PROBLEM

A. OSNs, Picture Posting, and Related Risks

This Section provides a brief overview of OSNs and some basic functionalities central to the present discussion. We start with a basic definition: "[OSNs are] web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and

10. It is important to stress that this Note deals only with the re-posting of pictures. One might reasonably ask why this would be so, as the re-posting of text is obviously possible and problematic. My answer stems from an intuitive sense that pictures convey information with more immediacy than text. This intuition is at least partly reflected in the psychological literature. *See, e.g.*, Kevin S. Douglas, David R. Lyon & James R. P. Ogloff, *The Impact of Graphic Photographic Evidence on Mock Jurors' Decisions in a Murder Trial: Probative or Prejudicial?*, 21 LAW & HUM. BEHAV. 485, 492 (1997) (showing that mock jurors arrive at more guilty verdicts when shown explicit photographs of mutilated victims than when simply given textual descriptions of a victim's physical condition); Adina Shmidman & Linnea Ehri, *Embedded Picture Mnemonics to Learn Letters*, 14 SCIEN. STUD. READING 159 (2010) (finding that children learn letter-sound combinations more efficiently when letter orthography is mapped onto familiar pictures).

those made by others within the system."[11] Depending on the OSN, other functionalities can enrich this basic design.[12] Most OSNs allow users to decide who can access the material they share. The typical default setting ensures that "friends" have access to information, and strangers do not.

Although Facebook and MySpace tend to garner the most media attention, there are hundreds of OSNs in operation.[13] OSN use represents a significant, and continually growing, portion of the leisure time pie. According to The Nielsen Company, as of December 2009, Internet users in the United States, the United Kingdom, Australia, Brazil, Japan, Switzerland, Germany, France, Spain, and Italy spend more than 5.5 hours per month on OSNs. This represents an 82% increase from 2008.[14] Facebook, the top-ranked social networking destination, received approximately 109 million unique visitors in the month of December alone.[15] According to Facebook, its members spend more than fifty-five minutes per day on the site.[16]

Nearly all OSNs provide an opportunity for users to submit small personal pictures to adorn their profiles. Facebook boasts particularly extensive photo features,[17] allowing users to upload hundreds of high-resolution digital photos to their accounts. These photos are organized into albums, each of which features its own

11. danah boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

12. Facebook, in particular, offers users a multitude of communicative tools. Basic user activities include posting status updates (e.g., "I'm cooking dinner"), commenting on users' home pages, posting pictures, playing games, and searching the full user database. FACEBOOK, http://www.facebook.com (last visited Oct. 7, 2010).

13. *List of Social Networking Websites*, WIKIPEDIA, http://en.wikipedia.org/wiki/List_of_social_networking_websites (last visited Jan. 18, 2011).

14. *Led by Facebook, Twitter, Global Time Spent on Social Media Sites up 82% Year over Year*, NIELSENWIRE (Jan. 22, 2009), http://blog.nielsen.com/nielsenwire/global/led-by-facebook-twitter-global-time-spent-on-social-media-sites-up-82-year-over-year.

15. *Top U.S. Web Brands and Site Usage: December 2009*, NIELSENWIRE (Jan. 14, 2010), http://blog.nielsen.com/nielsenwire/online_mobile/top-u-s-web-brands-and-site-usage-december-2009/. Facebook's in-house statistics are equally impressive. Facebook claims to have 500 million active users, 250 million of whom update their status posts every day. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 7, 2010).

16. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 7, 2010).

17. *See, e.g.*, *Help Center*, FACEBOOK, http://www.facebook.com/help/?page=830 (last visited Oct. 7, 2010).

customizable privacy profile; that is, users can dictate exactly who can view each specific album. After the pictures are posted, those with access can comment on the pictures or "tag" people they recognize in the pictures.[18] Tagging has the effect of making pictures searchable by the name(s) of the depicted person(s). Facebook allows tagging not only of Facebook users, but also of members of the general public. All users are able to "untag" themselves from photos (though non-members are required to join before they can untag themselves). For the purposes of clarity, I will refer to this sort of tagging as "name-tagging."

A more advanced feature of Facebook allows a user to "share" a photo belonging to someone else. This means that the photo is displayed on the sharer's page, though it cannot be viewed by those not granted access by the original poster. This form of re-posting respects the poster's original privacy preferences. This is not to say, however, that Facebook has solved the re-posting problem. A user may circumvent privacy preferences by executing a print-screen command while viewing a photo to which he has access, saving it to his hard drive, and then uploading it to his own account over which he retains control of privacy settings. Alternatively, a user could simply click the "download" link that appears underneath photos in the Facebook viewing console.

Even if we ignore overt circumventions of expressed privacy preferences, each sharing decision on an OSN such as Facebook is loaded with risk. This is because OSN privacy settings are often not user-friendly. On Facebook, for example, a fair degree of technological competence is required to effectively calibrate privacy settings. Given the ease of information flow on Facebook, even a small technical oversight could lead to oversharing of private information. Such missteps are easy to make. Facebook itself encourages oversharing. First, default privacy settings upon joining Facebook are minimal, at best.[19] Second, Facebook's "recommended" settings provide very weak barriers to information flow. This perhaps reflects Facebook's vested interest in keeping information flow on the site fluid, so as to encourage repeat visits to stay abreast of social "news" and content.

18. Recently, Facebook revised its photo viewing console. The newest version enables users to download photos posted to Facebook. This is particularly troubling from the perspective of the Poster's Plight.

19. The All Facebook site chronicles Facebook's default settings in graphic form. Nick O'Neil, *INFOGRAPHIC: The History Of Facebook's Default Privacy Settings*, ALL FACEBOOK, http://www.allfacebook.com/infographic-the-history-of-facebooks-default-privacy-settings-2010-05 (last visited Feb. 21, 2011).

One need only skim the headlines for tales of inadvertent oversharing. Take the case of high school teacher AP, for example, who was forced to resign in November 2009 after school officials received an anonymous email complaining that she posted inappropriate language and photographs on her Facebook page.[20] The allegedly inappropriate photographs (only 10 out of 700 posted) merely depicted AP, apparently sober, visiting beer gardens on a trip abroad.[21] According to news reports, AP's profile was visible only to a select group of friends that did not include students or parents.[22] Furthermore, her status post simply remarked that she was on her way to "Bitch Bingo" at a local bar.

It is hard to find the justly punishable transgression here. AP seemingly took a great deal of care to maintain her Facebook privacy. If indeed she used the full panoply of technical protections offered by Facebook to block students from accessing her information, holding her responsible for a leak that could well have been the result of malicious intermeddling is patently unfair. Countering this intuition is an equally strong belief that what is online is not private. This belief fits neatly within the United States' model of at-will employment—a simple Google search for "fired because of Facebook" will reveal that surveillance of online postings has become standard practice.

Employment disputes are only a subset of the privacy mayhem fostered by picture posting on OSNs. It is beyond the scope of this Note to address the full range of privacy concerns stemming from OSN picture posting. It suffices to say that OSN picture posting is a widespread activity with significant risks to privacy. Given the popularity of OSNs and the expectations of their users, these are risks that both the code underlying OSNs and privacy law should mitigate.

In the following pages, I focus on code's role in mediating OSN privacy. In Part B, I argue first that code should be recognized as a malleable design feature and not an immutable characteristic. I also introduce the theory of contextual integrity to frame the potentially transformative effects of new technologies such as OSNs on prevailing norms of information flow. In Part C, I explain how current OSN code does not map adequately onto users' deeply contextual notions of privacy and thus violates contextual integrity.

20. Maureen Downey, *Facebook Flap in Barrow Raises Troubling Fairness Issues*, GET SCHOOLED (Nov. 13, 2009, 4:44 PM), http://blogs.ajc.com/get-schooled-blog/2009/11/13/facebook-flap-in-barrow-raises-troubling-fairness-issues/.

21. *Id.*

22. *Id.*

B. The Digital Difference

In 1996, when Amazon.com still looked a little bit like a Geocities homepage,[23] Judge Frank Easterbrook sparked a debate. Speaking at a conference on cyberlaw, Easterbrook suggested that rather than develop new modes of legal analysis specific to cyberlaw, legal scholars should simply apply existing doctrine to the novel problems posed by the Internet.[24] Easterbrook advanced a Coasean solution to the problems at the intersection of technology and copyright law. Instead of attempting to anticipate the effects of technology on marketplace outcomes and tailor policy to those predictions, Easterbrook suggested that we simply provide parties with a stable set of rules and an opportunity to bargain.[25]

Easterbrook reasoned that "if we are so far behind in matching law to a well-understood technology such as photocopiers . . . what chance do we have for a technology such as computers that is mutating faster than the virus in *The Andromeda Strain*?"[26] This statement depends on a flawed assumption about the relationship between law and technology, namely, that technology exists as a complex creature beyond our control and elusive of law. As Lawrence Lessig pointed out in rebuttal to Easterbrook's speech, many people assume either that "the nature of cyberspace is fixed—that its architecture, and the control it enables, cannot be changed—or that government cannot take steps to change this architecture."[27] This is not the case. Human beings create code. And as a result, "code can change."[28] In assessing the frequent collisions between privacy and technology, we should keep in mind that the systems we

23. *How 20 Popular Websites Looked When They Launched*, TELEGRAPH (Sep. 2, 2009, 5:04 PM), http://www.telegraph.co.uk/technology/6125914/How-20-popular-websites-looked-when-they-launched.html.

24. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207 (1996).

25. *Id.* at 210.

26. *Id.*

27. Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501, 505 (1999). For a more thorough discussion of the relationship between code and law, see LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0 (2006). For a similar discussion of code, architecture, and OSNs, see Gordon Hull, Heather Richter Lipford & Celine Latulipe, *Contextual Gaps: Privacy Issues on Facebook*, ETHICS & INF. TECH. 6–7 (April 2010), *available at* http://www.springerlink.com/content/072730305020wm26/. Because "the architecture of an online environment is a function of the code that creates it, and because that code can be changed, the coding and interface of a site can make an enormous difference both in how much privacy users have, and how they experience their privacy." *Id.* at 7.

28. Lessig, *supra* note 27, at 506.

confront are not autonomous, natural, or immutable. They are subject to our control and influence.

Easterbrook's speech is problematic in another important regard. Implicit in Easterbrook's argument that there should not be a distinct law of cyberspace is the suggestion that principles of law can be developed outside the technological context in which the law applies. With regard to copyright law, Easterbrook suggested that in reducing the effective cost of copying, contemporary computing technology simply "continues a trend that began when Gutenberg invented movable type."[29] Turning to privacy, a similar point could be made about posting pictures online; in reducing the effective cost of sharing pictures, picture posting continues a trend that began when people started sharing pictures.

These assertions are weak because they overlook the fact that the internet has done far more than lower transaction costs. Rather, by lowering transaction costs, it has also effectuated a degree of information transfer and processing that alters the nature of contemporary data-handling protocol. Consider the practice of "aggregation," defined as "the gathering together of information about a person."[30] While data aggregation is not a new practice, today "the data gathered about people is significantly more extensive, the process of combining it is much easier, and the computer technologies to analyze it are more sophisticated and powerful."[31] Even if all the aggregated information is in the public domain, the aggregation still presents a challenge to individual privacy insofar as the very nature of that information is altered. It is a difference of kind *and* degree.

Aggregation, readily accessible database technologies, easily portable data, and statistical-analysis and data-mining tools represent technological transformations that "shape the many different ways computerized record-keeping systems and practices impinge on privacy and affect experiences."[32] By changing the way information can be accessed and used, these transformations "have affected the state and practice of electronic engagement with personal information, which, in turn, are experienced as threats to privacy."[33] In other words, as technological transformation continues to accelerate, people find themselves racing to rein technology

29. Easterbrook, *supra* note 24, at 208.

30. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 506 (2006).

31. *Id.*

32. NISSENBAUM, *supra* note 4, at 38–42.

33. *Id.* at 44–45.

back within boundaries that fit prevailing privacy norms.[34] If and when they are unable to do so, they might be forced to accept new, less optimal privacy norms. Often, new norms are "forced" to develop because people simply don't realize that their offline expectations are violated by online policies of information flow.

Consider the example of courtroom videotaping. Unlike many countries, the United States guarantees its citizens a front-row seat to the criminal adjudication process. As recently emphasized in *Presley v. Georgia*,[35] both the First and Sixth Amendments require trial courts "to take every reasonable measure to accommodate public attendance at criminal trials."[36] In January 2010, Judge Vaughn Walker suggested videotaping the now-famous Proposition 8 case, *Perry v. Schwarzenegger*.[37] Although this idea might seem like a logical step forward in light of the public's right to view a trial, when considered with an eye to technology's ability to transform norms, the notion of videotaping becomes much more troublesome. Imagine the effect of a piece of testimony taken out of context. Were a courtroom visitor to transmit a videotape to friends and colleagues, the information would likely enjoy limited viewership and do little damage to the witness. In contrast, were a fifteen-second clip of the same testimony distributed on YouTube, the scope of dissemination and its resultant effects could be astounding. What is in one case harmless gossip can, via technological magnification, become a potentially damning news story at a national level.

We have arrived at two important principles. First, the drawbacks, benefits, and features of web-based technologies (including OSNs) are mediated by code. This code is within our control. Second, new technologies can violate and transform established pri-

34. In attempting to understand the implications of such rapid transformation, Viktor Mayer-Schönberger's work on digital memory is helpful. He contextualizes the history of technology in the human species' collective effort to remember. He writes: "Since the early days of humankind, we have tried to remember, to preserve our knowledge, to hold on to our memories, and we have devised numerous devices and mechanisms to aid us." VIKTOR MAYER-SCHÖNBERGER, DELETE: THE VIRTUE OF FORGETTING IN THE DIGITAL AGE 48–49 (2009). Language, books, and computers all facilitate memory, to a different degree. Whereas "through millennia, forgetting has remained just a bit easier and cheaper than remembering," we are now, by virtue of the switch from analog to digital technology, required to confront the question "of whether we would like to remember everything forever if we could." *Id.*

35. 130 S. Ct. 721 (2010).

36. *Id.* at 725.

37. Lisa Leff, *Judge: Gay Marriage Trial Can Be Shown on YouTube*, ABCNEWS (Jan. 7, 2010), http://abcnews.go.com/Business/wireStory?id=9501129 (discussing *Perry v. Schwarzenegger*, 704 F. Supp. 2d 921 (N.D. Cal. 2010)).

vacy norms that people might reasonably assume still prevail despite technological transformation. How can we methodically apply these principles to specific cases, such as picture posting on OSNs? Here is where contextual integrity comes into play.

Contextual integrity provides a heuristic for both predicting when a given transformation tramples upon existing norms and concluding normatively whether the underlying technology's benefits outweigh its detrimental impact on norms. The normative analysis centers on the relationship between new technologies and "context-relative information norms" (information norms).[38] Information norms are made up of four components: contexts, actors, attributes, and transmission principles. Contexts are defined as "structured social settings" that give rise to particular roles and relationships.[39] Actors fall into one of three categories: senders, receivers, or subjects.[40] Attributes are types of information transferred (e.g., "medical information" or "contact information").[41] Transmission principles are constraints on information flow; the notion of confidentiality is a clear example of such a principle.[42] When a technology impinges on any of these information-norm components as they existed prior to that technology, the technology "is flagged as violating entrenched informational norms and constitutes a prima facie violation of contextual integrity."[43]

The normative analysis compares "entrenched normative practices [and] novel alternatives or competing practices on the basis of how effective each is in supporting, achieving, or promoting relevant contextual values."[44] According to Nissenbaum, "if the practices prescribed by entrenched informational norms are found to be less effective . . . than challengers . . . [or] novel practices," existing norms and practices can be justifiably replaced.[45] Procedurally, this analytic method should sit comfortably with legal scholars, given its use of a balancing test. Substantively, however, the normative component of contextual integrity will likely run up against objections.

Skeptics might complain that contextual integrity merely creates problems to solve. In other words, some shifts in norm struc-

38. NISSENBAUM, *supra* note 4, at 140.
39. *Id.* at 132.
40. *Id.* at 141.
41. *Id.* at 143.
42. *Id.* at 145.
43. *Id.* at 150.
44. *Id.* at 166.
45. *Id.*

tures are entirely natural. Take instant messaging, for example. As any user of Google Chat or America Online Instant Messenger knows, the rules of etiquette online are quite different from those in physical space. Consider the common acronym "brb." Although this expands to "be right back," people use "brb" for a wide variety of purposes. While they sometimes use it to pause a conversation while they do something quickly away from the computer, they might actually use it to terminate a conversation indirectly. Such callous behavior would never be tolerated in physical space—imagine calling someone and then leaving them on hold for two hours.

To the extent that people have grown accustomed to these new rules of conduct, they have arguably been forced into a new set of norms by the underlying technology. Yet not all shifts in norm structure are unnatural. The semantics of instant messaging—the creation of "lol," "brb," and their cousins—developed from within the instant messaging user community itself. And while this new semantics was born in response to new technology, it was not dictated to the masses by that technology; in other words, people didn't develop "lol" because they were prohibited from typing "laughing out loud."

Contextual integrity does not police such user-motivated behaviors. On the contrary, contextual integrity is about challenges to norm structure that are made through top-down technology-to-user mandates. Whereas instant messaging provides a good example of the former, OSN privacy represents the latter. As explained below, OSN users are not collectively developing notions of online privacy that are blended into OSN code structure. Users' notions are being excluded from the code structure, and users are not always aware of the forced norm shift.

To use an example discussed in more detail below, when users post pictures on an OSN, they might assume that the norms that govern offline sharing apply equally on the OSN, despite the fact that the OSN code does not let them express such norms. Because users cannot express these norms, over time, the community might assume they simply do not apply. Eventually, a new set of norms will develop in response to the technical limitations of the OSN code. Because this new set of norms will be born from technical limitation, not user preference, it will be both artificial and suboptimal from a privacy perspective. This is the dangerous process that contextual integrity attempts to prevent.

Even accepting this, one can still mount what Solove calls an "I've got nothing to hide" argument.[46] Solove notes that in the context of government surveillance, "many people believe that there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that the [activity] remain private."[47] The argument is that if you have not posted pictures or statements that could tarnish your image or land you in trouble if revealed, you have no reason to be worried that the information will reach a broader audience than you originally anticipated.

This argument fails because it assumes "that privacy is about hiding bad things."[48] As Solove notes, the harm here is not a question of "dead bodies."[49] Rather, the harm is a matter of dignity and autonomy as enshrined in contextually relevant norms of information transfer. And, to the extent that users might actually share less and refrain from maximizing the full communicative and creative potential of OSNs for fear of privacy violations, it is a question of social utility.[50] If, as contextual integrity argues, people rely on contextually relevant and community-prevalent norms of information flow to mitigate harms to autonomy and dignity, then understanding when technological systems violate these norms is an important social goal. When, as is the case with OSNs, such a violation takes place, a remedy is necessary. If no remedy is provided, the technological transformations might end up forcing users to adopt new, less optimal information norms.

To review, applying the contextual integrity heuristic to OSNs requires a comparison of information norms as they exist in users' collective conscious and the norm-impinging features of OSN code. Insofar as they exist before the technological transformation, such previously entrenched norms can be understood to cognitively predate the transformation. In the next section, I will attempt to high-

46. Daniel J. Solove, *"I've Got Nothing To Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

47. *Id.* at 746.

48. *Id.* at 764.

49. *Id.* at 768.

50. Readers will likely note the apparent contradiction between this assertion and the argument below that OSN users are myopic. *See infra* Part I.C. A point of clarification is useful here. In arguing that users are myopic, I am not suggesting that they all are actively aware of the privacy risks of OSN participation or the technologically driven shift in norms. Rather, I am arguing that, even if users understand the privacy risks, the free market will be unable to select for privacy-friendly firms because users will irrationally discount all long-term privacy costs (including the ones they thoroughly understand).

light and identify information norms that cognitively predate OSNs, explain how OSNs violate contextual integrity by forcing users to unwittingly abandon these information norms, and explain the particular role code plays in effecting this violation.

C. What Web Am I Surfing?

Recall Mathew's response to Lee's post: if you want something kept private, do not put it on the web. The implication here is clear. Assuming that the user has perfect information about the prevailing norms and technical details of an OSN, the user can be counted on to make rational decisions protecting her privacy. However convenient, this "user beware" attitude only holds if the web the user *thinks* he is surfing is the one that he *is* surfing. In other words, Mathew's logic is only appropriate if Lee's intuitions with regard to the relationship between privacy norms on Facebook and those that cognitively predate Facebook's code are respected by the prevailing code structure. As it turns out, this essential condition is not satisfied by current Facebook code; to understand why, we need to look at both empirical evidence on information norms that predate Facebook and the transformations effected by current code.

Revealing information norms is difficult detective work. It is no easy task to understand exactly what people expect from OSNs in terms of privacy, even when we ask them. For example, despite expressing significant privacy concerns, people seem to love to disclose information. The popular press likes to call this apparent contradiction the "privacy paradox."[51] Examples abound in the academic literature. For example, Acquisti and Gross report that nearly 16% of surveyed members of an American university who expressed concern for a hypothetical scenario in which a stranger discovered his or her schedule of classes and home address on an OSN nevertheless listed *both* pieces of information on their OSN profiles.[52] This same study revealed that over 89% of undergradu-

51. *See, e.g.*, Andy Greenberg, *The Privacy Paradox*, FORBES.COM (Feb. 15, 2008, 6:00 AM), http://www.forbes.com/2008/02/15/search-privacy-ask-tech-security-cx_ag_ 0215search.html; Brad Stone, *Our Paradoxical Attitudes Toward Privacy*, BITS BLOG (July 2, 2008, 3:56 PM), http://bits.blogs.nytimes.com/2008/07/02/our-paradoxical-attitudes-towards-privacy/.

52. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PRIVACY ENHANCING TECHNOLOGIES: SIXTH INTERNATIONAL WORKSHOP 36, 51 (George Danezis & Philippe Golle eds., 2006), *available at* http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf.

ate respondents who expressed the most concern for threats to personal privacy joined Facebook.[53]

Similarly, Stutzman found that while undergraduate and graduate students expressed concern about the consequences of sharing identity information on OSNs, more than 50% of these respondents listed their name, academic classification, gender, email, picture, major, birthday, home town, high school, relationship status, address information, interests, and political views on their Facebook profiles.[54] While Stutzman does not directly address privacy settings, Gross and Acquisti do: they were able to publicly view all but three of over 4000 profiles studied on their school network.[55] Govani and Pashley report similar results. While 84% of undergraduate respondents were aware that they could restrict who could view their Facebook profiles, fewer than 48% actually used Facebook's privacy settings.[56]

Despite these 2005 findings, there is a fair amount of evidence that the use of privacy settings to mediate the openness of OSNs is on the rise. A 2007 report by the Pew Internet & American Life Project notes that 59% of teens with active profiles on OSNs claim that these profiles are visible only to friends.[57] Similarly, Young and Quan-Haase found that while large percentages of undergraduate survey participants included school name, email address, birth date, personal photos and photos of friends on their Facebook profile, 64% limited profile visibility to "only friends."[58] This trend seems equally prevalent on European OSNs.[59]

---

53. *Id.* at 46.

54. Frederic Stutzman, *An Evaluation of Identity-Sharing Behavior in Social Network Communities*, 3 J. INT'L DIGITAL MEDIA & ARTS ASS'N 10, 15–16 (2006).

55. Ralph Gross & Alessandro Acquisti, *Information Revelation and Privacy in Online Social Networks*, *in* PROCEEDINGS OF THE WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 71, 77 (Sabrina De Capitani di Vimercati & Roger Dingledine, eds., 2005).

56. Tabreez Govani & Harriet Pashley, Student Awareness of the Privacy Implications When Using Facebook 8 (2005) (unpublished manuscript), *available at* http*://lorrie.cranor.org/courses/fa05/tubzhlp.pdf*.

57. Amanda Lenhart & Mary Madden, *Teens, Privacy, and Online Social Networks: How Teens Manage Their Online Identities and Personal Information in the Age of MySpace*, PEW INTERNET AND AMERICAN LIFE PROJECT 26 (2006).

58. Alyson L. Young & Anabel Quan-Haase, *Information Revelation and Internet Privacy Concerns on Social Network Sites: A Case Study of Facebook*, *in* C&T '09: PROCEEDINGS OF THE FOURTH INTERNATIONAL CONFERENCE ON COMMUNITIES & TECHNOLOGIES 268 (2009).

59. Sonja Utz & Nicole Krämer, *The Privacy Paradox on Social Network Sites Revisited: The Role of Individual Characteristics and Group Norms*, CYBERPSYCHOLOGY: J. PSYCHOSOCIAL RES. ON CYBERSPACE (2009), http://cyberpsychology.eu/view.php?cisloclanku=2009111001&article=2.

It is certainly good news that people are becoming more active in protecting their privacy on OSNs. Yet this trend, however fortunate, does not offer much insight into how OSN users psychologically relate to the often-fragile balance between public and private information online—it might just show that, by means of using privacy settings, OSN users are explicitly recognizing that the degree of publicity or privacy on OSNs is, to some degree, within their control. Put differently, unless the privacy settings examined are coextensive with users' actual notions of privacy, evidence of their use or neglect tells us little about what web users think they are surfing.

Filling this data void, numerous cutting-edge studies demonstrate that people expect congruence between the information norms that cognitively predate OSNs and the transmission principles that OSN code allows.[60] Reporting results from interviews with teenage OSN users, Livingstone found that users' notion of "friends" online tracks similar offline notions.[61] For example, one student drew a distinction between "best friends," "friends I'm good friends with," "friends that I see every so often," and "people that I do not really talk to."[62] Similarly, Lampe, Ellison, and Steinfield found that "despite changes in the technical ability of non-university people to join Facebook," student users feel that Facebook is a "student-only" site.[63] Thus, students seem to expect student-centric offline information norms to persist in the online context.

As several commentators have pointed out, OSN code has failed to respect these expectations.[64] One of the most powerful examples springs from the very nature of online social engagement. In describing OSNs, danah boyd has used the term "networked publics."[65] A networked public is at least in part defined by its mediated nature—"the network mediates the interactions between members of the public."[66] In unmediated environments, "the boundaries and audiences of a given public are structurally defined" by the real-world physics. Thus, as boyd points out, the audi-

60. *See supra* notes 55–57 and accompanying text.

61. Sonia Livingstone, *Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy, and Self-Expression*, 10 NEW MEDIA & SOC. 393, 405 (2008).

62. *Id.*

63. Cliff Lampe, Nicole B. Ellison & Charles Steinfield, *Changes in Use and Perception of Facebook*, ASS'N FOR COMPUTING MACHINERY CONF. 721, 729 (2008).

64. *See generally* NISSENBAUM, *supra* note 4, at 231–56.

65. danah boyd, *Social Network Sites: Public, Private, or What?*, 13 KNOWLEDGE TREE 6 (2007), http://kt.flexiblelearning.net.au/tkt2007/wp-content/uploads/2007/05/edition_13.pdf.

66. *Id.* at 8.

ence that watches you trip on the curb is "restricted to those present in a limited geographical radius at a given moment in time." Mediating technologies such as OSNs, in contrast, "change everything." In short, the "scale of the public" becomes magnified—now you have to worry about "all the people who might witness a reproduction" of your fall.[67]

Note the symmetry between boyd's point that technology changes everything and the notion of transformation central to contextual integrity. How information is actually handled is changing, not necessarily our expectations of how that information will be handled. Boyd's falling example demonstrates how the visibility of OSNs broadens the scope of actors, increasing the number of information receivers; alters transmission principles, encroaching on the physical-space notion of reciprocity, where you see the people who see you fall; and conflates contexts, blurring the limited public sphere of the curb location with the unlimited public sphere of the online forum.

These transformations are not obvious. Rather, "the abstraction involved in asynchronous, online social networking encourages a gap between a user's perceived audience and actual audience."[68] A more specific example of violation can be seen in OSNs' tendency to flatten the "nuances of face-to-face interactions" by forcing users to classify fellow OSN members as friends and non-friends.[69] Nissenbaum notes that this binary approach represents "a failure to grasp some of the subtle ways people share and withhold certain types of information in the complex web of their relationships."[70] As Hull, Lipford, and Latulipe point out, in requiring users to stuff people into two categories, OSNs such as Facebook force users to "determine a set of *ex ante* rules for determining how information should flow in and between contexts . . . before knowing any of the details about the information itself."[71] Offline, we are able to adjust these transmission principles on a more flexible, case-by-case basis in accordance with our expectations of relevant information norms.

One important takeaway from all this is that the problem with privacy on OSNs—specifically, Lee's problem—is not so much that there is a cognitive disconnect between what OSN users want (privacy) and what they do (disclose information) in binary terms as it is that OSN users are applying a multicolor privacy approach to a

67. *Id.*
68. Hull, Lipford & Latulipe, *supra* note 27, at 6.
69. *Id.* at 12–13.
70. NISSENBAUM, *supra* note 6, at 226.
71. Hull, Lipford & Latulipe, *supra* note 27, at 6.

functionally dichromatic (private vs. public) system that doesn't accommodate it.[72] As the contextual integrity heuristic reminds us, we should support only those transformations that preserve the spirit of information norms that cognitively predate such transformations, *unless* new norms offer a benefit that outweighs the privacy costs. To return to boyd's falling example, we would have to balance the benefit to society of sharing a humorous photo with the violence done to principles of dignity enshrined in the original information norms. As explained above, OSNs clearly do not meet this standard; as a result, contextual integrity guides us to seek a remedial strategy.

One such strategy would be to educate consumers and allow them to select the most privacy-conscious firms on the open market. Assuming that consumers will act rationally (in the economic sense), we would predict that they will "pay" an amount of privacy commensurate with the utility they receive from the OSN they "purchase."[73] Assuming a competitive market, the privacy cost to join an OSN would drop to the marginal cost of maintaining an OSN that provides the demanded utility. Those OSNs that "charge" a higher privacy price (or a privacy price not aligned with users' expectations) will perish.[74]

As researchers in behavioral economics have recognized, however, people do not always behave rationally.[75] For example, scholarly research suggests that consumers tend to be myopic—that is to say, they focus more on the here-and-now than the apparently dis-

72. *Id.* at 6–7, 12. Nissenbaum points out that the public–private dichotomy "can be understood as a cruder version of contextual integrity, postulating only two contexts with distinct sets of informational norms for each—privacy constraints in the private, anything goes in the public." NISSENBAUM, *supra* note 4, at 141.

73. As any Facebook or MySpace member knows, most OSNs are nominally free. The quotes above are included to underscore the fact that the illusion of a free lunch obscures high privacy costs. Viewed in this light, it is appropriate to consider the OSN signup process as tantamount to a point of sale transaction.

74. *See, e.g.*, Oren Bar-Gill, *Seduction By Plastic*, 98 NW. U. L. REV. 1373 (2004). "When price equals marginal cost, a buyer will buy if and only if she values the good or service more than its cost. Marginal-cost pricing aligns private incentives with the social objective of welfare maximization. Goods and services are produced only when the benefit exceeds the cost, and an optimal allocation of resources is achieved." *Id.* at 1377.

75. *See, e.g.*, Daniel Kahneman, Jack L. Knetsch & Richard H. Thaler, *Experimental Tests of the Endowment Effect and the Coase Theorem*, *in* BEHAV. L. & ECON. 211 (Cass R. Sunstein ed. 2000).

tant future.[76] If offered a product with a benefit of x at T1 and a total cost of zero at T1 and $x + 1$ at a later time T2, consumers will likely choose to purchase the product at T1 despite the fact that its total cost outweighs its benefit. For example, when deciding whether to obtain a credit card, consumers are likely to focus more on the high up-front benefits (e.g., rewards points) than on the high back-end costs (e.g., high interest rates).[77]

In the OSN context, this means that consumers are likely to focus more on the features being offered (the T1 benefit) and the up-front price (the T1 cost) than on the privacy cost (the T2 cost), which is by nature a long-term cost. Reacting to this, OSNs will compete on features and up-front prices—not on privacy costs, which matter less to consumers. To compensate for the low up-front price and extensive features, which have high production costs, OSNs will backload the production costs to the price dimension that consumers heavily discount (i.e., the privacy price). In light of this distortion, the market will fail to select adequately for privacy-friendly firms. From an OSN's perspective, this strategy works best when users do not understand privacy risks at all; but the discounting effect holds even when consumers understand the nature of the risk.

Even if consumers behave rationally, they might not end up choosing the most privacy-conscious OSNs. Consider, for example, two OSNs—one with abysmal privacy protections and a million users and another with ideal privacy protections but only fifty users. If offered a choice between these two networks, most users would choose the former. The explanation for this decision is fairly straightforward. OSNs are fun and socially valuable because they allow users to benefit from shared information and experiences; thus, the more people that use the network, the more valuable the network becomes.[78] Such effects are particularly significant given the fact that the US OSN market is dominated by a few key players with hundreds of millions of users.[79]

76. Oren Bar-Gill, *The Law, Economics and Psychology of Subprime Mortgage Contracts*, 94 CORNELL L. REV. 1073, 1120 (2009).

77. *See* Bar-Gill, *supra* note 74.

78. In the terminology of economics, OSNs are subject to network effects. OSNs become harder to leave as the number of users increases because "each user's payoff from the adoption of [the OSN], and his incentive to adopt it, increase[s] as . . . others adopt [the OSN]." Paul Klemperer, *Network Effects and Switching Costs*, (The New Palgrave Dictionary of Economics, Working Paper, 2005), *available at* www.paulklemperer.org.

79. *See, e.g.*, *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 7, 2010).

Alternatively, the administrative state could force more contextual privacy controls. Of course, barring a perfect match between privacy settings and privacy expectations, conflict will still arise. Consider the Poster's Plight: The re-poster might be distributing because the OSN did not allow the poster to convey a context-specific transmission principle—"please do not spread this around." But the re-poster might also just be ignoring all the signals the poster provided. Thus a full consideration of the Poster's Plight requires both a technical and a legal analysis. So where does the law fit in?

As mentioned earlier, one weapon that the law provides for plaintiffs suffering from the Poster's Plight is the public disclosure tort. While hypothetically available to plaintiffs such as Lee, the public disclosure tort is of limited use in the OSN context. This is largely the result of vague elements that were built for a pre-internet age and that have not been adequately updated to accommodate contemporary technology. Understanding how these elements work is a prerequisite of our analysis of the tort's interaction with the Poster's Plight.

In the next Section, I outline the public disclosure tort, focusing predominantly on the reasonableness and legitimate concern prongs, the diversity of interpretative approaches to these prongs, and the transformative effects of OSN technology on the underlying analyses. Chief amongst these effects is the fundamental alteration of information norms that have accreted in response to existing doctrine.

II.
CONTEXTUALIZING THE LAW

It is quite difficult to saddle OSNs with liability. This difficulty stems from section 230 of the Communications Decency Act, which provides an extremely powerful shield for providers of interactive computer services (i.e., OSNs).[80] Our discussion of the law should therefore start with this important provision.

Because OSN providers are responsible for the code that makes our online experiences possible, it might seem reasonable to hold them accountable for the shortcomings. Section 230 of the Communications Decency Act and recent section 230 jurisprudence, however, make it clear that targeting the OSN provider is a wasted effort. Motivated by an intent to "promote the continued

80. 47 U.S.C. § 230 (2006).

development of the Internet,"[81] section 230 holds that "no provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[82]

In short, what this means is that platforms such as Facebook are largely immune to liability for the torts of clients and users. For example, in *Doe v. MySpace, Inc.*,[83] the Fifth Circuit refused to hold MySpace liable for negligent failure to "implement basic safety measures to prevent sexual predators from communicating with minors on its web site."[84] Similarly, in *Chicago Lawyers' Committee for Civil Rights Under Law, Inc. v. Craigslist, Inc.*,[85] the Seventh Circuit refused to hold Craigslist liable for hosting housing advertisements in violation of The Fair Housing Act. Although by no means bulletproof,[86] section 230 is undoubtedly robust. For example, in *Finkel v. Facebook, Inc.*,[87] the New York Supreme Court recently held that section 230 protects Facebook from liability for a third party's defamatory statements despite the fact that Facebook retains an ownership interest in information posted on its site.

Our search for liability therefore should focus on the re-poster, not the OSN. The privacy torts defined by Prosser in the Second Restatement of Torts[88] and inspired by Samuel Warren and Louis Brandeis's classic article *The Right to Privacy*,[89] are the chief weapons in this fight. The tort most relevant to the Poster's Plight is the pub-

81. *Id.* § 230(b)(1).

82. *Id.* § 230(c)(1).

83. 528 F.3d 413 (5th Cir. 2008).

84. *Id.* at 416.

85. Chicago Lawyers' Comm. for Civil Rights Under Law, Inc. v. Craigslist, Inc., 519 F.3d 666 (7th Cir. 2008).

86. For a detailed overview of section 230 jurisprudence in 2009, see Eric Goldman, *47 USC 230 Year-in-Review for 2009*, TECH. & MARKETING L. BLOG (Jan. 5, 2010), http://blog.ericgoldman.org/archives/2010/01/47_usc_230_year_2.htm. As the cases listed demonstrate, section 230 remains a strong but not impermeable bar to liability. Of particular interest are cases such as *Almeida v. Amazon*, in which the potential application of section 230's intellectual property exception to privacy torts is given somewhat detailed theoretical treatment. 456 F.3d 1316 (11th Cir. 2006).

87. Finkel v. Facebook, Inc., No. 102578/09, 2009 WL 3240365 (N.Y. Sup. Ct. Sept. 15, 2009).

88. RESTATEMENT (SECOND) OF TORTS § 652A-E (1977).

89. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890). Solove and Richards stress that "Warren and Brandeis did not invent the right to privacy from a negligible body of precedent but instead charted a new path for American privacy law." *See* Neil. M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 125 (2007).

lic disclosure tort. The Second Restatement provides the following explanation:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter published is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.[90]

As this description makes clear, the public disclosure analysis is tricky business. "Private life," "reasonable," "highly offensive," and "legitimate concern" are concepts that beget uncertainty and awaken judicial imagination. Imagination, which thus far has been used in many jurisdictions to shape these terms to restrict the tort's overall ambit.[91] As a result, public disclosure suits are all but impossible to win in more restrictive jurisdictions. What motivates this interpretative trend? As Lior Strahilevitz explains, while "[o]n one hand, the law seeks to encourage the expressive and psychological benefits that people derive from disclosing sensitive information about themselves to others," on the other hand, "the law seeks to regulate the further dissemination of this information."[92]

The doctrinal ambiguities concerning the elements themselves, and the jurisdictional inconsistencies in interpretation, result in a tort that Solove aptly calls "one of the most fascinating puzzles of tort law."[93] The puzzle originates in the fundamental tension between our dedication to free speech on one hand and the inevitable feeling that we have a "right to be let alone," on the other.[94] This tension is most explicitly felt in the public disclosure tort's "legitimate concern" element, which the Supreme Court has broadened to include many pieces of information that we wouldn't expect to see on the eleven o'clock news. It also comes to bear, though less immediately, on the necessary determination of what, precisely, "private life" means.

I discuss each element separately. In Part A, I describe the current state of the legitimate concern test and explain the transforma-

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

91. *See, e.g.*, Patrick J. McNulty, *The Public Disclosure of Private Facts: There is Life After* Florida Star, 50 DRAKE L. REV. 93, 100 (2001).

92. Lior J. Strahilevitz, *A Social Networks Theory of Privacy* (Univ.of Chi. Law Sch. Pub. Law & Legal Theory, Working Paper No. 79, 2004), *available at* http://ssrn.com/abstract_id=629283.

93. Daniel J. Solove, *The Virtues of Knowing Less: Justifying Privacy Protections Against Disclosure*, 53 DUKE L.J. 967, 971 (2003).

94. *See* Warren & Brandeis, *supra* note 89 (citing THOMAS M. COOLEY, A TREATISE ON THE LAW OF TORTS: OR THE WRONGS WHICH ARISE INDEPENDENT OF CONTRACT, 29, 2d ed. 1888).

tive effects of technology on the analysis. In Part B, I do the same for the reasonableness prong.

A. All the News that's Fit (or Not) to Print

In light of the First Amendment, it is both constitutionally and ethically difficult to determine when a given piece of information is so newsworthy that the value of disclosure trumps the privacy interests of those who wish to keep the information secret. To the extent that courts have settled on a few approaches to this challenge, information norms that stem from the legal tests have developed. For example, where a community standard is applied, that community standard dictates the expectations of the population with respect to disclosures. In disrupting the technological-media framework that gave rise to these legal rules, OSNs threaten information norms that developed in response to the old framework and thereby violate contextual integrity. The present Section will chronicle this violation. Before breaking the doctrine apart, however, let us first take a look at how it plays out in real cases.

On September 22, 1975, Oliver Sipple saved President Gerald Ford's life. Just before Sara Jane Moore pulled the trigger on her .38 caliber revolver, Sipple, a decorated Vietnam War veteran living on 100% disability, somehow managed to push Moore's arm down just enough to reroute her shot and save the President from a potentially fatal wound.[95] After the dust settled, Sipple was questioned by the Secret Service and the FBI for three hours; he was interviewed by reporters sporadically for days. When asked what he wanted in return for his heroic deed, Sipple replied: "I just want a little peace and quiet."[96] What he got was the full scrutiny of the press with regard to his sexuality.

Despite Sipple's refusal to answer questions regarding his sexuality, the news media continued to press the issue and eventually "outed" Sipple. In retaliation, Sipple filed a lawsuit against several newspapers and other involved parties for publication of private facts.[97] Sipple lost the suit, in part because the court determined that the facts running to Sipple's sexuality were of legitimate public concern. In reaching this holding, the court noted that "the record shows that the publications . . . were prompted by legitimate politi-

95. Richard West, *President Escapes Assassin's Bullet*, L.A. TIMES, Sept. 23, 1975, at 1.

96. Daryl Lembke, *Hero in Ford Shooting Active Among S.F. Gays*, L.A. TIMES, Sept. 25, 1975, at A3.

97. Sipple v. Chronicle Publ'g Co., 201 Cal. Rptr. 665, 666–67 (Cal. Ct. App. 1984) (upholding trial court's grant of summary judgment for defendants).

cal considerations"[98] such as the need "to dispel the false public opinion that gays were timid, weak and unheroic figures and to raise the equally important political question whether the President of the United States entertained a discriminatory attitude or bias against a minority group such as homosexuals."[99]

The *Sipple* court applied the legitimate concern, or newsworthiness, test described in the Second Restatement.[100] The Second Restatement states that "when the publicity ceases to be the giving of information to which the public is entitled, and becomes a morbid and sensational prying into private lives for its own sake, with which a reasonable member of the public, with decent standards, would say that he had no concern," information ceases to be newsworthy.[101] This is only one way to answer the newsworthiness question. Commentators have identified no fewer than five prominent approaches to the question,[102] including simply rejecting the public disclosure tort outright.[103]

An alternative approach is marked by deference to the media—the "leave it to the press approach." As Diane Zimmerman describes, this approach is rooted in the belief that "social norms that govern acceptable behavior in the exchange of information are better communicated through the marketplace than through the courtroom."[104] Because "the economic survival of publishers and broadcasters depends upon their ability to provide a product that the public will buy," the press "must develop a responsiveness to what substantial segments of the population want (and perhaps

98. *Id.* at 670.

99. *Id.*; *see* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 122 (3d ed. 2009) (noting that the President hadn't taken time to call Sipple and thank him).

100. *Id.* at 669–70.

101. RESTATEMENT (SECOND) OF TORTS § 652D cmt. h (1977).

102. *See* Geoff Dendy, Note, *The Newsworthiness Defense to the Public Disclosure Tort*, 85 KY. L.J. 147, 157–64 (1997) (describing five approaches to newsworthiness question). Daniel Solove offers a different categorization in his recent article on the public disclosure tort and the First Amendment. *See* Solove, *supra* note 93, at 1001. Solove presents three approaches: (1) deferring to the media; (2) focusing on the status of the individual; and (3) examining the nature of the information. *Id.*

103. Although most states recognize the tort, Nebraska, New York, North Carolina, North Dakota, Rhode Island, Utah, and Virginia do not. *See* SOLOVE & SCHWARTZ, *supra* note 99, at 106.

104. Diane L. Zimmerman, *Requiem for a Heavyweight: A Farewell to Warren and Brandeis's Privacy Tort*, 68 CORNELL L. REV. 291, 354 (1983). *See, e.g.*, Berg v. Minneapolis Star & Tribune Co., 79 F. Supp. 957, 960–61 (D. Minn. 1948) (asserting that under law of supply and demand, what press publishes can be seen as proxy for what people want reported).

even need) to know."[105] In short, if it is in the news, it is there because people want it there.

Yet another approach joins a "nexus" component to the Restatement test. As articulated by the Fifth Circuit in *Campbell v. Seabury Press*,[106] privacy can be protected "by requiring that a logical nexus exist between the complaining individual and the matter of legitimate public interest."[107]

Although these tests stifle at least some intrusive reporting at the fringes of reasonableness, they all provide news media with a fair degree of leeway. The strength of this leeway is obvious in the Supreme Court's privacy jurisprudence, which holds that "where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order . . . ."[108] Yet, in marking the boundaries with respect to community norms, the predominant Second Restatement test at least recognizes the sorts of entrenched values central to contextual integrity. This is a tenuous shield for prospective plaintiffs, to be sure. But in an era in which violations were limited to major institutional actors (e.g., newspapers, magazines, and TV stations), people enjoyed the benefit of reinforcing community norms via decisions that reward good reporting (by purchasing a paper or watching a broadcast) and punish bad reporting (by ignoring it).

All of this changes in the digital age, given the democratizing effect of blogging and microblogging.[109] As Lauren Gelman has eloquently argued, Internet technologies have provided a "technological megaphone" that individuals can use to "broadcast their story [and those of others] to the world." Prior to widespread use of the Internet, "content was filtered through news or other publishing

105. Zimmerman, *supra* note 104, at 353–54.

106. 614 F.2d 395 (5th Cir. 1980).

107. *Id.* at 397. The Tenth Circuit treads a similar path. As the court explained in *Gilbert v. Medical Economics Co.*, a "newsworthy publication must have some substantial relevance to a matter of legitimate public interest." 665 F.2d 305, 308 (10th Cir. 1981). Applying this test in *Shulman v. Group W Productions*, the California Supreme Court held that video and audio footage depicting a car crash victim's "injured physical state" and "disorientation and despair" were "substantially relevant" to an emergency response documentary's inherently "newsworthy subject matter," despite the fact that the victim never consented to the broadcast. 955 P.2d 469, 488 (Cal. 1998).

108. Florida Star v. B.J.F., 491 U.S. 524, 541 (1989).

109. Microblogging is a relatively recent phenomenon, epitomized by services such as Twitter, which allow users to broadcast short messages. *See Microblogging*, WIKIPEDIA, http://en.wikipedia.org/wiki/Microblogging (last visited Oct. 13, 2010); TWITTER, http://twitter.com (last visited Feb. 22, 2010).

intermediaries." These intermediaries "played an important social role in balancing the newsworthiness of information against the privacy interests of third parties who were indentified."[110] Now that anyone can effortlessly broadcast to the world, a more precise notion of newsworthiness is required.[111] It is necessary both because people have lost the protection of an institutional news media and because the very essence of a community-norms approach is obliterated by the global context of the Internet.

Prior to the internet era, newsworthiness determinations relied on a particular set of information norms tailored to the prevailing news media business model and technological infrastructure. Blogs and OSNs tore open transmission principles at the core of these old-fashioned information norms. For example, whereas in the old model citizens were receivers, in the new model they can be both receivers and senders. Traditionally, when a newspaper made a decision based on community norms, it could apply a local context tailored to its circulation area. Now, a conceivably massive number of diverse communities can be served information.[112] The result is a clear prima facie violation of contextual integrity.

The problem is not limited to the newsworthiness analysis. Technological transformation has also affected the publicity requirement, a close cousin of newsworthiness. According to the Second Restatement, publicity "means that the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge."[113] Courts tend to take two approaches to this, one quantitative and one qualitative. The quantitative test hews to the line drawn in the Restatement and "contemplates that a large number of persons must be aware of the intimate and embarrassing information before an actionable claim of invasion of privacy exists."[114] The qualitative test ignores the magnitude of the disclosure

110. Lauren Gelman, *Privacy, Free Speech, and "Blurry Edged" Social Networks*, 50 B.C. L. Rev. 1315, 1333 (2009).

111. It should be noted that Internet-era developments also have implications for the disclosure tort's publicity requirement. *See infra* Part II.A.

112. Note the clear parallel to similar problems with community-based obscenity standards. As Justice Breyer explained in *Ashcroft v. American Civil Liberties Union*, "adopting the community standards of every locality in the United States would provide the most puritan of communities with a heckler's Internet veto affecting the rest of the Nation." 535 U.S. 564, 590 (2002) (Breyer, J., concurring).

113. Restatement (Second) of Torts § 652D cmt. a (1977).

114. McNulty, *supra* note 91, at 100. Under the first test, courts have not held the publicity requirement satisfied when a defendant discloses plaintiff's debts to an employer, Yoder v. Smith, 112 N.W.2d 862, 864–65 (Iowa 1962); when a defen-

and holds that the publicity requirement "may be satisfied by proof that the plaintiff has a special relationship with the public to whom the information is disclosed."[115]

As Gelman's "megaphone" metaphor makes clear, the publicity requirement changes dramatically in the Internet age. Consider these numbers: USA Today has a daily circulation of about two million, and the New York Times has a daily circulation of about one million.[116] Facebook, in contrast, claims that more than 50% of its 500 million users sign in on any given day. These users collectively upload more than three billion photos each month, post sixty million status updates each day, and share five billion pieces of content (including photos) each week.[117] As these statistics demonstrate, the information posted to popular OSNs can, depending on the poster's privacy settings, reach an audience larger than that of the print versions of major domestic and international newspapers.[118] Given the danger that a re-poster can circumvent privacy settings to broadcast information beyond the scope originally intended by the poster, this disclosure risk reaches beyond the limits of current OSN security measures.

Under a quantitative test, satisfaction of the publicity requirement in an OSN case will likely hinge on factors such as the privacy settings of the original poster's account. For example, if the origi-

dant contacts plaintiff's employer in an attempt to collect a debt, Vogel v. W.T. Grant Co., 327 A.2d 133 (Pa. 1974); or when a defendant discloses to plaintiff's superiors information relevant to a decision to terminate for cause, Rogers v. Int'l Bus. Machs. Corp., 500 F. Supp. 867, 870 (W.D. Pa. 1980). In contrast, courts have upheld a suit when a creditor posted a large sign on his shop window publicizing plaintiff's debt, Brents v. Morgan, 299 S.W. 967 (Ky. 1927), and when a store employee loudly and obviously interrogated and accused a patron of shoplifting in front of the store, Bennet v. Norban, 151 A.2d 476, 479 (Pa. 1959).

115. McNulty, *supra* note 91, at 100. *Miller v. Motorola* provides a good example of how the second test works. Joy Miller underwent a mastectomy and reconstructive surgeries and had to take three leaves of absence from her job as a result. Although Motorola's resident nurse assured Miller that her medical information wouldn't be disseminated, a co-employee informed Miller that she knew about the mastectomy. Miller's subsequent belief that other employees surely must have known as well caused her to prematurely retire from her twenty-three-year employment with Motorola. The court upheld Miller's privacy claim against a motion to dismiss. Miller v. Motorola, Inc., 560 N.E.2d 900, 904 (Ill. App. Ct. 1990).

116. Joseph Plambeck, *Newspaper Circulation Falls Nearly 9%*, N.Y. TIMES, April 26, 2010, at B2, *available at* http://www.nytimes.com/2010/04/27/business/media/27audit.html.

117. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Oct. 7, 2010).

118. Whether this information will actually spread depends on a variety of factors, such as the nature of the information and the popularity of the poster.

nal poster allows friends *and* friends of friends to view the material in question, far more people will likely view the material than if the original poster had allowed viewing access to her friends alone. Under the qualitative test, in contrast, the question of "special relationships" as they exist in the OSN context will dominate the issue. The archetypal qualitative case involves a defendant whose disclosure was to a party "whose knowledge of [the] facts would be embarrassing to the plaintiff."[119] How this will play out in OSN cases will likely depend on the degree of knowledge required of the defendant.

While *Miller v. Motorola*, the seminal case on the issue, does not clearly establish the degree of knowledge required by a defendant in a privacy suit, certain jurisdictions seem to consider whether or not the defendant knew about the special relationship.[120] Under a strict liability framework, the issue is resolved easily, as the outcome will not depend on whether the re-poster knew that the people to whom he was disclosing information had a relationship with the plaintiff. Yet if the re-poster discloses the information to a contact under a negligence framework, how much due diligence must he complete before he will escape liability? If the threshold is low (e.g., merely checking if the contact and the plaintiff list similar schools or communities in their profiles), the publicity test will provide minimal protection. If the threshold is high, the test will provide more protection—however, it should be noted that a too-burdensome "checking" requirement risks overly chilling the sharing that is central to OSNs' psychological and social-economic benefits.

How all this comes together in Lee's case is difficult to predict. In light of the standards established above, it would seem that the identity of the people to whom Lee's re-poster disseminated the photographs and the nature of their relationship with Lee (and the subjects of the photograph) would critically affect the publicity analysis. Unfortunately, Lee's post gives us no details on who the re-poster's target audience was. If we apply a quantitative analysis, publicity will likely be satisfied regardless. Even if the re-poster's initial dissemination provided access only to a few people, the re-posting actions of those subsequent actors would lead to an exponential increase in viewers. A qualitative approach, in contrast, would need

119. *See Miller*, 560 N.E.2d at 903 (holding both that "an invasion of a plaintiff's right to privacy is important if it exposes private facts to a public whose knowledge of those facts would be embarrassing to the plaintiff," and that said public might be "fellow employees, club members, church members, family, or neighbors, if the person [is] not a public figure").

120. *See, e.g.*, Pachowitz v. Ledoux, 666 N.W.2d 88 (Wis. Ct. App. 2003).

to consider the relationship between Lee and those given viewing access by the re-poster. We do not have this information either, though one could surmise that because Lee's mother has acted as re-poster, there is some substantial relationship between Lee and those people to whom his mother permitted access.

Our hands are similarly tied with respect to the newsworthiness question. This is largely because most public disclosure cases center on news media. Unlike a typical re-poster, newspaper publishers, bloggers, and television stations do not just broadcast pictures—there's usually a story attached. Applying any of the tests to the Poster's Plight is thus incredibly difficult. It is hard to contemplate, however, what interest the public would have in photos of Lee's children; unless there is a cloud hanging over the situation not revealed in Lee's post (such as parental abuse), it strains credulity to believe that Lee's photos are newsworthy.

I have outlined the degree to which OSN technology exerts a transformative effect both on the newsworthiness and the publicity requirement of the public disclosure tort. In the next section, I consider another critical element of the tort—the privacy requirement itself. Like the newsworthiness test, the privacy inquiry is fraught with difficulty (even outside the Internet context). This difficulty stems from the necessary analytic step of determining whether an individual who discloses information retains a reasonable expectation of privacy in that information.

Faced with this difficult decision, some courts prefer hard line rules that treat the precipitating context (and any information norms that go along with it) as irrelevant. Other courts appear to attempt a more contextual analysis but do so in a haphazard manner. Whether these courts consciously are applying a contextual decision heuristic is unclear. Nevertheless, they offer evidence that a contextual reasonableness test is not wholly impracticable. In the next Section, I outline both approaches to demonstrate this point.

B. Beyond Binary Notions of Privacy

Earlier in this Note, I concluded that a binary notion of privacy lacks the fidelity of a more robust, context-dependent approach. The same story plays out in courts' attempts to decide why a given fact is private rather than public. While it is generally acknowledged that American courts are all over the map when it comes to "determining whether an individual has a reasonable expectation of privacy in a particular fact that has been shared with one or more

persons,"[121] what Strahilevitz calls a "hard-line"[122] approach seems to have developed a significant following. This hard line approach is isomorphic with the public-private dichotomy discussed above; it takes as its general assumption that disclosure—even to a few people—precludes any future privacy interest in the disclosed information.

In the Fourth Amendment context, the hard line approach is referred to as the third-party doctrine.[123] The basic idea is that if you disclose private information to one person, you bear the risk that that person will further broadcast the information. As Justice White explained in his concurrence in *Katz v. United States*, "[W]hen one man speaks to another he takes all the risks ordinarily inherent in so doing, including the risk that the man to whom he speaks will make public what he has heard."[124] Thus, the Court has held that parties do not have reasonable expectations of privacy in dialed phone numbers because the numbers have already been dis-

121. Strahilevitz, *supra* note 92, at 3.

122. *Id.* at 22.

123. *See, e.g.*, SOLOVE & SCHWARTZ, *supra* note 99.

124. 389 U.S. 347, 363 n.** (1967) (White, J., concurring). *Katz* established the framework under which modern Fourth Amendment privacy analysis has evolved. In *Katz*, the Court determined that the "Fourth Amendment protects people, not places." *Id.* at 351. Thus, the government invaded Katz's privacy when it surreptitiously placed (without a warrant) a recording device outside a phone booth that Katz used to transmit wagering information in violation of a federal statute, even though there was no physical intrusion into the booth during the call. *Id.* at 348–51. In his famous concurrence, Justice Harlan explained that for Fourth Amendment purposes, privacy is established only when a person shows "an actual (subjective) expectation of privacy. . .that society is prepared to recognize as 'reasonable.'" *Id.* at 361 (Harlan, J., concurring).

The third-party doctrine has come under considerable fire for the problems it presents in the digital age. *See, e.g.*, David Couillard, Note, *Defogging the Cloud: Applying Fourth Amendment Principles to Evolving Privacy Expectations in Cloud Computing*, 93 MINN. L. REV. 2205, 2215 (2009) (noting that the doctrine "is particularly relevant in the cloud-computing world, where information is turned over to cloud service providers for remote storage and other quasi-transactional purposes with increasing frequency"). *See also* Matthew D. Lawless, Note, *The Third Party Doctrine Redux: Internet Search Records and the Case for a "Crazy Quilt" of Fourth Amendment Protection*, 11 UCLA J.L. & TECH. 1, 15 (2007) (arguing that a pragmatic "operational realities" test is more equitable than the third-party doctrine in determining a person's reasonable expectation of privacy).

Note, however, that the doctrine is not without its supporters. Orin Kerr has written an article defending the doctrine both for its value in maintaining the "technological neutrality of Fourth Amendment rules" and providing "ex ante clarity" of Fourth Amendment doctrine. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564–65 (2009).

closed to the phone company;[125] nor do they have reasonable expectations of privacy in bank records, for the same reason.[126]

One of the most famous hard-line cases is *Nader v. General Motors*.[127] In 1965, Ralph Nader published *Unsafe at Any Speed*, a book detailing the dangers of the Chevrolet Corvair. In retaliation, General Motors embarked on a smear campaign to undermine Nader's credibility.[128] According to the complaint, General Motors conducted interviews with Nader's associates and friends, questioning them about his political, social, racial, and religious views, his integrity, his sexual inclinations, and his personal habits. General Motors also allegedly spied on Nader in public places, made threatening phone calls to him, and tapped his phone.[129] Nader sued for, among other things, invasion of privacy.

Predictably, the court had no problem analyzing the wiretapping claim.[130] The interviews with Nader's associates, however, was a more bitter pill to swallow. The court found it "difficult to see how [the interviews] may be said to have invaded [Nader's] privacy." Because Nader "had previously revealed the information to such other persons," he "necessarily assume[d] the risk that a friend or acquaintance in whom he had confided might breach the confi-

125. *See* Smith v. Maryland, 442 U.S. 735, 743-45 (1979).

126. United States v. Miller, 425 U.S. 435, 442-45 (1976). The Court notes that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed." *Id.* at 443.

Note that the holdings in *Miller* and *Smith* have been limited by statutes. Two years after *Miller* was decided, Congress enacted the Right to Financial Privacy Act of 1978 (RFPA). 12 U.S.C. §§ 3401–22 (2006). The RPFA prohibits a search of "the financial records of any customer [held by] a financial institution" unless the customer has authorized disclosure, the Government has obtained a subpoena or court order, or the Government acts by formal written request in limited circumstances. 12 U.S.C. §§ 3401–22. Following the decision in *Smith*, Congress passed the Pen Register Act, which holds that "no person may install or use a pen register or a trap and trace device without first obtaining a court order." 18 U.S.C. § 3121 (2006).

127. Nader v. Gen. Motors Corp., 255 N.E.2d 765 (N.Y. 1970).

128. *See* Ian McDonald, *Nader's Raiders*, TIMES (Lon.), Feb. 6, 1971, at 15, *available at* http://archive.timesonline.co.uk/tol/viewArticle.arc?articleId=ARCHIVE-The_Times-1971-02-06-15-001&pageId=ARCHIVE-The_Times-1971-02-06-15.

129. *See Nader*, 255 N.E.2d at 767.

130. The court upheld Nader's wiretapping claim, noting that the claim "most clearly meets" the requirements of an actionable invasion of privacy claim. *Nader*, 255 N.E.2d at 570.

dence."[131] And here's the kicker: "[I]nformation about the plaintiff which was already known to others could hardly be regarded as private to the plaintiff."[132]

The court directly endorsed the third-party doctrine and indirectly endorsed the practice of unmitigated aggregation. As discussed earlier, aggregation is only weakly justified by the fact that aggregated information, whether in the form of court records, addresses, phone numbers, college degrees, or email addresses, is technically public information; far from simply taping things together, aggregation makes the end product far more informative than the sum of its component parts.

Judge Breitel, in a concurring opinion, located this weakness in the court's conclusion that "the mere observation of the plaintiff in a public place does not amount to an invasion of his privacy:"[133]

> Although acts performed in "public," especially if taken singly or in small numbers, may not be confidential, at least arguably a right to privacy may nevertheless be invaded through extensive or exhaustive monitoring and cataloguing of acts normally disconnected and anonymous.[134]

History has proven Breitel's point. It is hardly news that by statistically analyzing impersonal user profile data such as friend lists on OSNs such as Facebook, computers can draw inferences about very personal characteristics (such as political party preference or sexual orientation).[135] Yet the binary distinction—public versus private—that the *Nader* court applies cannot accommodate such nuanced analysis; to be more specific, the *Nader* court disregards the possibility that particular information norms existed between Nader and his friends that mediated Nader's privacy expectations about the likelihood of disclosure.

In adopting the third-party doctrine and forcing Nader to shoulder the risk of confiding in friends, the court neatly sidesteps a more complex, context-dependent analysis. Not all courts, however, draw such sharp lines. Consider *Sanders v. American Broadcasting Companies*.[136] Mark Sanders was a telepsychic employed by a Los Angeles company. He worked in a large room with approximately

131. *Id.*

132. *Id.*

133. *Id.* at 771.

134. *Id.* at 772 (Breitel, J., concurring).

135. Carolyn Y. Johnson, *Project 'Gaydar,'* BOSTON GLOBE, Sept. 20, 2009, http://www.boston.com/bostonglobe/ideas/articles/2009/09/20/project_gaydar_an_mit_experiment_raises_new_questions_about_online_privacy/.

136. Sanders v. ABC, 978 P.2d 67 (Cal. 1999).

ninety-nine other psychics, each of whom took calls in a personal cubicle. As part of an exposé for *PrimeTime Live*, ABC reporter Stacey Lescht applied for a job at the same outfit. Without telling Sanders, Lescht recorded her conversations with Sanders using a hidden camera and subsequently included portions of the video in the *PrimeTime Live* broadcast. Sanders sued ABC for, among other things, intrusion upon seclusion.[137]

A close cousin of the tort of public disclosure, the tort of intrusion upon seclusion requires a plaintiff to show that the defendant intruded, physically or otherwise, upon the solitude or seclusion of the plaintiff or his private affairs or concerns, and that such intrusion would be highly offensive to a reasonable person.[138] Although this tort features elements different from those required by the public disclosure tort, it relies on a similar determination of whether the plaintiff had a reasonable expectation of seclusion or solitude in the place, conversation, or data source in question.[139]

The key factual issue in *Sanders* was that, given the office environment, it was quite likely that someone other than Sanders or Lescht would have overheard the videotaped conversation. Under a third-party doctrine approach, Sanders would have had no claim—the conversation would be deemed public because it had been already revealed to the office at large. But the California Supreme Court thought otherwise:

> [P]rivacy, for purposes of the intrusion tort, is not a binary, all-or-nothing characteristic. There are degrees and nuances to societal recognition of our expectations of privacy: The fact that the privacy one expects in a given setting is not complete or absolute does not render the expectation unreasonable as a matter of law.[140]

In other words, the California court was reluctant to adopt a purely binary attitude. As the court asserted, "[T]he possibility of being overheard by coworkers does not, as a matter of law, render unreasonable an employee's expectation that his or her interactions within a nonpublic workplace will not be videotaped in secret by a journalist."[141]

There is a hint of contextual integrity in the *Sanders* opinion. As the *Sanders* court suggests, our disclosure decisions are not decisions to open or close an information faucet to the world. They are

137. *See id.* at 69–71.
138. *See* RESTATEMENT (SECOND) OF TORTS § 652B (1977).
139. *See Sanders*, 978 P.2d at 71–72.
140. *Id.* at 916.
141. *Id.* at 923.

decisions to share particular pieces of information with others pursuant to the belief that the people with whom the information is shared operate under similar transmission principles, roles, and other contextual values. Solove frames the issue of transmission principles nicely, stressing that "not all people and entities have the same obligations in maintaining the confidentiality of information."[142] One would expect more of her parent or best friend, regardless of the lack of a legal fiduciary relationship.

Although confidentiality is clearly at play in the public disclosure tort, it is not the only active transmission principle. Disclosure decisions are also linked to culture-mediated judgments about how well the recipient can handle the information disclosed and to what degree the recipient will want that information. Thus, as Katherine Strandburg highlights, "[T]he interplay between self-control, temptation, human cognitive limitations, and the theory of social norms" fosters the development of a natural hesitation to accept "too much information" in a given context.[143] This natural hesitation leads to the creation of another important transmission principle—the willpower norm.[144]

Strandburg's theory of willpower norms brings us to a separate analysis of *Sanders*. Because the conversation between Sanders and Lescht involved "ordinary workplace chat," it was thus "a socially acceptable discussion within the workplace community of matters that might be expected not to be shared with the world at large."[145] Because "the social norms that might ordinarily restrict disclosure of workplace discussions to outsiders were ineffective against the defendant journalist," the court needed to step in to fill the norm gap. At least insofar as the *Sanders* court was concerned, the "law protects the social norms of workplace discourse from an intruder who is not reachable by those norms."[146]

Obviously, the scope of information norms is vast. The point in this Section is not to pick and choose. Rather, the goal is to demonstrate how essential the preservation of context is to a realistic assessment of privacy. Consider Lee's situation: The *Nader* court would throw the case out immediately because, in posting the photos online, Lee crossed the third-party doctrine's threshold of

142. Solove, *supra* note 93, at 1014.

143. Katherine J. Strandburg, *Privacy, Rationality, and Temptation: A Theory of Willpower Norms*, 57 RUTGERS L. REV. 1235, 1238 (2005).

144. *See id.*

145. *Id.* at 1300.

146. *Id.* at 1301.

privacy. In binary speak, he flipped from private to public.[147] Such an approach would deny Lee the opportunity to prove that his mother's use of a common "friend" connection to view the photos violated an offline confidentiality norm.[148]

Under a *Sanders*-style analysis, Lee would at least get a chance to argue that his partial disclosure did not vitiate a privacy claim. Instead of asking only whether Lee disclosed the pictures to anyone, a court would likely investigate both the nature of the relationship between Lee and those to whom he provided viewing access and the disclosure norms (i.e., transmission principles) undergirding those relationships. The court in *Multimedia Wmaz v. Kubach*[149] provides a stellar example of such an analysis in its determination that an HIV patient's disclosure of his condition to friends, family, medical personnel, and members of a support group did not preclude him from suing a TV station when it failed to adequately blur his face in an AIDS documentary. Relying on the implicit understanding of confidentiality between Kubach and those to whom he disclosed his condition, the court stressed that the two disclosures (close contacts versus TV audience) "were similar in neither degree nor context."[150]

However encouraging, the approach taken in cases such as *Sanders* and *Kubach* falls short of ensuring adequate protection, especially in light of the transformative effects of OSNs. This is primarily because the analysis is, at its core, unprincipled. Although judges seem to be exploring the contextual values at stake, they are doing so on the basis of intuition, not through consistent application of a clearly expressed and thoroughly considered decision heuristic. Thus, it is conceivable that a court that treats one case contextually will, by virtue of a lack of familiarity with underlying technology, apply a less contextually appropriate analysis to another case.

147. This prediction is not a flight of fancy. In a recent case involving a college student who briefly posted a derogatory poem about her hometown on an unprotected MySpace page, the court determined that the student had no reasonable expectation of privacy in the disclosure. *See* Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858, 862–63 (Cal. Ct. App. 2009). The determination was made solely on the grounds that the student "made her article available to any person with a computer and thus opened it to the public eye." *Id.*

148. Recall that Lee was not linked to his mother as a "friend." Lee's mother was linked to one of Lee's friends as a friend. Because Lee presumably set his privacy settings such that "friends of friends" could see posted pictures, Lee's mother was able to view the pictures without becoming Lee's "friend."

149. 443 S.E.2d 491, 493 (Ga. 1994).

150. *Id.* at 494.

An alternative account of judicial thought focuses on probabilities of disclosure. Judges might, as Strahilevitz suggests, actually be asking themselves, "Had the defendant not become involved, would I have expected this information to remain private were I in the parties' shoes?"[151] The appeal of such an approach lies in its attachment to a basic and empirically verified premise of social networks theory—namely, that information flows through human networks in predictable ways. Of course, contextual integrity would hold that the principles dictating these flows stem from entrenched information norms. Therefore, insofar as judges applying this approach fail to consciously, transparently, and methodically confront contextual values, decisions will hew to a court's personal understanding of social dynamics, not the organic reality of information norms as they exist in the relevant social space.

In the final analysis, it is possible that courts are doing none of these things— they could simply be going with what "feels right." It is clear that even the most open-minded courts have not thoroughly embraced contextual integrity as a decision heuristic. Formal adoption of a reasonableness analysis that centralizes questions of contextually rooted values would grant public disclosure cases a much needed degree of predictability and, more importantly, congruence with peoples' actual privacy values. One possible approach would require the deciding court to ask if, in light of prevailing information norms, the plaintiff was justified in expecting the disclosed information to remain private absent the defendant's actions. Such an approach would join the intuition of the probabilistic method with the guidance of contextual integrity.

Most importantly, the reasonableness analysis should measure behavior against prevailing information norms. Thus, in Lee's case, the court should not simply ask: What was the probability that Lee's picture would reach the public absent the re-poster's actions? Rather, the court should ask: Given the information norms that obtained between Lee and those to whom he provided access, what was the probability that Lee's picture would reach the public absent the re-poster's actions?

The approach just outlined requires some judicial access to contextual information. Unfortunately, as I highlighted in Part I, new technologies such as OSNs frequently impose new principles of information flow on users who either have not yet adjusted or do not fully appreciate that the rules of the game have changed. Therefore, a court that looks to evidence of a plaintiff's privacy set-

151. Strahilevitz, *supra* note 92, at 14–15.

tings for contextual information, for example, will end up with a grossly inadequate and unrealistic determination of operative information norms. As a result, any reasonableness analysis predicated on these false information norms will be deeply flawed.

If we want courts to embrace an analytic approach that recognizes realistic information norms, we should encourage parties to create objective evidence of such information norms at the time of original disclosure, not merely after the fact at the evidence stage, when the pressure of litigation might cause parties to be less than candid about their norms, values, and expectations. With respect to the Poster's Plight, we should encourage OSNs such as Facebook to allow users to express more than just a binary "post/do not post" or "friend/not friend" preference when deciding whether to upload a picture. This objective is motivated by two important points. First, contextually accurate privacy settings are needed to preserve fundamental dignity and autonomy values and to ensure a safer and more consumer-friendly social environment that maximizes social utility through sharing. Second, a revamped public disclosure analysis that relies on contextual values needs ex ante evidence of those values. By recording preferences at the time of information disclosure, OSNs can help build a valuable record of evidence.

Our goal should be to add context to the OSN privacy regime. In the next section, I propose a preference expression tool that I hope will throw at least a few hues on the canvas. In Part A, I outline a tool that will help picture posters more thoroughly express their privacy preferences with regard to posted pictures. In Part B, I discuss how this tool can be expected to meet both objectives discussed above.

III.
PUTTING THE BLURRY EDGES IN FOCUS

Let us start by examining how the law interacts with posting decisions on OSNs. Taking our lead from law and economics literature, we assume that all OSN members are perfectly rational, utility-maximizing, and self-interested actors.[152] We begin our analysis with a three-person hypothetical OSN, of which X, Y, and Z are members (fig. 1). X is the picture poster. X and Y are offline friends. Y and Z are offline friends. X does not know Z. Assume that the OSN, like Facebook, gives users the ability to determine who

152. *See* Robert H. Frank, *Departures from Rational Choice: With and Without Regret*, *in* THE LAW AND ECONOMICS OF IRRATIONAL BEHAVIOR 13 (Franceso Parisi & Vernon L. Smith eds., 2005) (summarizing classical theory of law and economics).

can view their pictures. Assume also that the OSN, like Facebook, does not allow users to convey any privacy preferences relevant to the posting decision other than access. Finally, assume that all photos posted on this OSN feature only the poster.

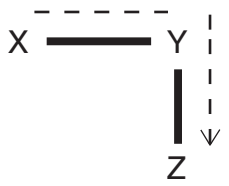

Figure 1: OSN schematic. Solid lines indicate offline friendships; dotted lines indicate (1) X's willing online disclosure to Y and (2) Y's deceptive online dissemination to Z.

Imagine further that X posts a picture and gives only Y viewing access. At this stage, Y must rely exclusively on contextual cues (i.e., transmission principles) that obtain in X and Y's offline relationship in deciding whether or not to re-post the picture. Recall that Y's re-posting decision is not limited by OSN technology. If Y so desires, she can download the photo to her hard drive and re-post it via her own account. In this case, the picture will be subject to only Y's privacy preferences. If Y decides to allow Z to view the picture, X's preference that only Y should have access will be vitiated. Furthermore, if a friend of Z's joins the network and Z follows the same re-posting procedure as Y, Z's contacts will have access to the picture.

X thus runs the risk that Y will misinterpret the disclosure norms implicit in their offline relationship or that Y will maliciously breach these norms. Because the OSN does not allow expression of any privacy preference outside of "share this with Y" or "do not share this with Y," Y's knowledge of operative norms is only as strong as her offline relationship with X. If X and Y are best friends, the likelihood of norm misinterpretation is fairly low. But if X and Y are not particularly close, the probability of misinterpretation markedly increases. Thus, assuming she is perfectly rational, X will base her decision whether to share on a calculation of the expected probability that Y will non-consensually re-post, the expected probability of prevailing in litigation precipitated by the re-posting, the expected privacy cost of a non-consensual re-posting incident, and the expected benefits obtained by sharing with Y.

This calculation works out differently depending on the jurisdiction's treatment of the privacy torts. Under a binary regime, there is no chance that X will prevail in litigation because X has no

legally cognizable expectation of privacy (disclosure to one friend is viewed as tantamount to disclosure to the general public). Under such a regime, X will share if, and only if, the expected probability of Y's re-posting multiplied by the expected cost of Y's nonconsensual re-posting is less than the expected benefit of sharing with Y. Given the significant costs of privacy breaches (think about the school teacher who was fired), we would expect members of this OSN to be fairly timid sharers of information. Such an OSN would likely have no party pictures, no lively political commentary, and no flirting—it would be a communicative graveyard.

Like X's OSN, today's prominent OSNs (Facebook included) exist in a binary privacy space. Yet they are hardly barren and antisocial landscapes. We're left, then, with a pressing question: If OSNs do not provide a context-friendly privacy regime, and the law does not reliably take into account contextual information, why are people willing to share so much on OSNs? In other words, why are OSNs the bustling, vivid, and powerful sources of digital life that they are? Assuming that participation in OSNs is voluntary and not necessary, the most plausible explanation is that people simply aren't perfectly rational. In other words, whereas traditional law and economics assumes that individuals are "possessed of sufficient cognitive capacity to solve relatively simple optimization problems,"[153] individuals might actually be imperfect in their ability to consistently choose the efficient solution.

As discussed earlier, one irrational tendency is myopia. The benefits of joining an OSN (fun applications, increased social capital, romantic flings, etc.) dwarf the up-front costs of joining ($0 + time spent registering and linking to OSN friends). Because the larger costs of joining (privacy risks down the line, commercial trading of user information by the OSN, etc.) are not usually felt until well after the time of registration, people have a tendency to discount them. To return to the example above, prospective OSN users may irrationally deflate the expected cost of a non-consensual re-posting incident. Thus, even if the cost to X is quite high (again, remember the school teacher who lost her job), it will appear small to X in comparison to the up-front benefit.

Another irrational tendency is optimism. Researchers in behavioral economics have identified an optimism bias in a variety of contexts, including criminal justice, litigation, and credit card

153. *Id.*

borrowing.[154] Put simply, "people exhibit a strong tendency to underestimate the probability that negative events will happen to them as opposed to others."[155] The difference between myopia and optimism is subtle; whereas myopia acts on the total expected privacy cost (the probability of a nonconsensual re-posting incident multiplied by the expected cost of such an incident), optimism acts on the expected probability of a nonconsensual re-posting incident.[156] In the example above, an optimistic X will underestimate the probability of Y's nonconsensual re-posting. This judgment error will distort X's decision whether to participate in an OSN and share information.

At least on Facebook, these psychological tendencies are likely exacerbated by the OSN provider's dauntingly complex approach to privacy. Over the course of Facebook's ascent, the site's privacy policy has expanded from 1004 words to 5830 words. As the New York Times pointed out in a recent article, this makes it longer than the United States Constitution, sans amendments.[157] The document is dense, technical, and by no means easy to navigate. As Oren Bar-Gill has argued in the context of subprime mortgage contracts, while "the rational [actor] is unfazed by complexity, the imperfectly rational [actor] might be misled by complexity."[158] The New York Times reported in May 2010 that there were no fewer than fifty privacy settings on Facebook's privacy page, with more than 170 options total.[159] While the rational OSN user will have no problem

154. *See* Oren Bar-Gill, *The Evolution and Persistence of Optimism in Litigation*, 22 J.L. ECON. & ORG. 490 (2006); Bar-Gill, *supra* note 74; Christine Jolls, *On Law Enforcement with Boundedly Rational Actors*, *in* THE LAW AND ECONOMICS OF IRRATIONAL BEHAVIOR 268 (Franceso Parisi & Vernon L. Smith eds., 2005).

155. Jolls, *supra* note 154, at 270.

156. *Id.* at 271 ("At least in some contexts, the empirical evidence makes clear that optimism bias reflects not only underestimation of the probability of a negative event relative to the average person's probability of that event, but also underestimation of the probability of a negative event relative to the actual probability of that event.").

157. Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES, May 12, 2010, http://www.nytimes.com/2010/05/12/technology/personaltech/13basics/html.

158. Bar-Gill, *supra* note 76, at 1122.

159. Bilton, *supra* note 157. Some readers might find confusing the dual assertions that OSNs sponsor a "dichotomous" approach to privacy and also feature complex and numerous privacy controls. The argument is not that OSNs feature only two options—"privacy off" versus "privacy on." The argument is that OSNs feature numerous options that are expressed in binary terms. In physical space, we make disclosure decisions by relying on norms of information flow (e.g., when we tell our best friends secrets, we rely on the relationship of trust to prevent further disclosure). Ideally, our online decisions could rely on the continued operation of

navigating these privacy settings and arriving at her personal optimal expected privacy result, the imperfectly rational user, intimidated by complexity, will ignore or weakly apply these privacy settings (and will suffer down the line as a result).[160]

Of course, before we can confidently apply such an analysis, we need more empirical data linking OSN use patterns with the predictions and expectations of behavioral economics. Nevertheless, myopia, optimism, and irrational handling of complexity do offer a compelling set of explanations for why OSN users brave the privacy storm despite the immense privacy costs; in short, they just do not accurately perceive these costs. Yet the cost-benefit analysis proposed above is relevant only if OSN participation is viewed as a voluntary action and not something required of life in contemporary society.

As evidenced by the usage statistics, OSNs are central to modern life. [D]anah boyd makes this point by comparing Facebook to a utility company. She argues that "[p]eople's language suggests that people are depending on Facebook just like they depended on the Internet a decade ago."[161] While boyd acknowledges that "Facebook may not be at the scale of the Internet (or the Internet at the scale of electricity)," she stresses that this size differential "doesn't mean that [Facebook is] not angling to be a utility or quickly becoming one."[162] In making this point, boyd doesn't merely rely on "people's language." Rather, she highlights the fact that despite Facebook's multiple privacy faux pas,[163] people still use the service. According to boyd, there is no longer any reason to waste time wondering whether or not there will ever be enough user revolt to make Facebook turn back from its privacy-threatening policies— "there won't be."[164]

---

such norms. At present, however, we must make a multitude of binary decisions (e.g., "share with best friend X," "let X share with Y," "do not let Y share with Z") that are based on OSN codes' dichotomous (i.e., "off versus on") approach to privacy.

160. *Id.* In response to such reports and user discontent, Facebook recently implemented a more streamlined privacy setting interface. While marginally better, it still is far from simple.

161. danah boyd, *Facebook is a utility; utilites get regulated*, ZEPHORIA.ORG (May 15, 2010), http://www.zephoria.org/thoughts/archives/2010/05/15/facebook-is-a-utility-utilities-get-regulated.html.

162. *Id.*

163. A full history of Facebook privacy disputes is well beyond the scope of this Note. Many websites have chronicled Facebook's struggle with privacy issues. *See, e.g.*, Caroline McCarthy, *Facebook's follies: A brief history*, THE SOCIAL (May 13, 2010, 4:00 AM), http://news.cnet.com/8301-13577_3-20004853-36.html.

164. boyd, *supra* note 161.

If we assume that "buying" from Facebook is like buying from the local energy company, risky OSN participation becomes much easier to understand. As boyd explains, "when it comes to utilities like water, power, sewage, Internet, etc., I am constantly told that I have a choice. But like hell I'd choose Comcast if I had a choice. Still, I subscribe to Comcast. Begrudgingly. Because the 'choice' I have is Internet or no Internet."[165]

Necessity aside, it is at least plausible that the benefits of using OSNs such as Facebook really are significant, even in light of the hefty risks. Thus a third explanation might simply be that OSNs provide users high utility. In a recent post, technology blogger Nancy Baym explains why she hasn't yet withdrawn from the Facebook community. In her eyes, Facebook provides a platform through which she "gain[s] real value."[166] She writes:

> I actually like the people I went to school with. I know that even if I write down all their email addresses, we are not going to stay in touch and recapture the recreated community we've built on Facebook. I like my colleagues who work elsewhere, and I know that we have mailing lists and Twitter, but I also know that without Facebook I won't be in touch with their daily lives as I've been these last few years. I like the people I've met briefly or hope I'll meet soon, and I know that Facebook remains our best way to keep in touch without the effort we would probably not take of engaging in sustained one-to-one communication.[167]

As Baym explains, the value of Facebook is immense. For her, at least, this value exceeds the expected costs of membership and participation. Yet despite her tech savvy, Baym confesses to some irrationality, pointing out that "the rewards of Facebook are concrete and immediate," and the "costs are abstract and ideological."[168]

It is likely that each of these explanations tell a piece of the overall story. What is important for our present purposes is not to identify a precise answer, but rather to appreciate that all these explanations are predicated on the assumption that there is at least *some* benefit to OSN use, and that this benefit entails *some* privacy tradeoff. This becomes clear upon revisiting our simple OSN. Just

165. *Id.*

166. Nancy Baym, *Why, despite myself, I am not leaving Facebook. Yet.*, ONLINE FANDOM (May 13, 2010, 12:40 PM), http://www.onlinefandom.com/archives/why-despite-myself-i-am-not-leaving-facebook-yet.

167. *Id.*

168. *Id.*

as there is information that X might not want re-broadcasted or re-posted, there is also information that X might not care to protect. Existence-on-the-network is a good example of this. If X is interested in the music of Arnold Schoenberg, for example, she might welcome the ability to sift through her OSN's member pages to find someone else (the proverbial needle in a haystack) who shares her atypical interest (atonal music is not exactly easy listening). Taking another step, she might also want other Schoenberg fans to be able to find her. A privacy solution that locks down all information would destroy the permeability that makes a good OSN work.

Lauren Gelman makes a similar argument in her piece on "blurry edged" social networks.[169] Addressing the question of why people "post content on a medium available to the whole world when that content is not intended for the whole world," Gelman argues that "Internet users are calculating that they are unlikely to identify *a priori* all the people they intend to reach with their posts because their social network is undefined." Thus, because X is unlikely to be able to identify all the Arnold Schoenberg fans on her OSN, she might be willing to unprotect the information on her profile running to her Schoenberg interest. In other words, X recognizes that the boundaries of the set "people I know who are interested in Schoenberg" are best left blurry (or permeable) to leave open the possibility that others with a shared interest can join the group.

So how do we simultaneously encourage socially optimal sharing and discourage socially troublesome over-sharing? One way would be through contract law. Woodrow Hartzog has suggested a "privacy box" application that would allow users to "enter information they wish to share with other connected 'friends' but request a promise of confidentiality before the information is divulged."[170] These promises of confidentiality could then be used to invoke reliance via the equitable remedy of promissory estoppel.[171] This is a clever solution, if a slight miss. I would argue that by requiring users to entangle their interactions in a web of contracts, such a solution would not only take the fun out of networking online, but would also itself exert a transformative effect on norms. Confidentiality agreements are the stuff of business transactions; widespread appli-

169. *See* Gelman, *supra* note 110, at 1317. In fact, the Schoenberg example here is a riff off Gelman's own explanatory device.

170. Woodrow Hartzog, *The Privacy Box: A Software Proposal*, FIRST MONDAY (Nov. 2, 2009), http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2682/2361.

171. *Id.*

cation of these agreements to a social context would ultimately conflate two separate spheres of interaction that do not belong together.

A more context-friendly solution would preserve the social nature of OSNs, while still giving users an opportunity to put the contextual stuffing back into transactions contextually eviscerated by OSN technology. Gelman's suggestion is spot on:

> One option would be a tool for users to express and exercise privacy preferences over uploaded content. It would permit users to express their intentions by tagging any uploaded content with an icon that immediately conveys privacy preferences to third parties.

As Gelman points out, this tool "would provide immediate visual feedback to third parties about the content owner's preferences." Thus, just as search engines skip over certain webpages that contain privacy-requesting metatags, individuals can be generally expected to be "hesitant to abuse user privacy preferences when such preferences appear clearly alongside the relevant content."[172] Returning to our basic example, if X can tag her content with extra guidance for Y, the risk that Y will make a disclosure decision based on a misinterpretation of prevailing norms will be significantly reduced. This matters because the less worried X is about unwanted disclosure, the more X will engage in socially optimal posting behavior.

The devil, of course, is in the details. The success or failure of such a tool will depend greatly on its narrow tailoring to the privacy problem it aims to solve. Our chief concern here is the Poster's Plight. To refer back to our basic model, we want to reduce the risk that Y will misperceive the norms on which X is relying when she posts her picture. We also want to generate a body of evidence that will chronicle X's expectations at the time of posting the picture. We have been spending a fair amount of time in the air; let us now move into the weeds.

A. Color-Coding Privacy

Currently, OSNs protect photo privacy by allowing users to limit viewing access either to OSN friends generally (MySpace) or to particular, handpicked users (Facebook). I propose that OSNs take another step and provide picture posters with an opportunity to disclose highly detailed preferences prior to (and after) posting pictures. The system would work as follows: Upon uploading a

172. Gelman, *supra* note 110, at 1343.

photo, users would receive a stock privacy warning, reminding them of the potential downsides of disclosure (lost job, information leakage, etc.). Such a warning would have a link to the OSN's privacy policy page. After checking a checkbox labeled "I understand the potential risks of disclosure," the user would be presented with five descriptive choices, each placed next to a checkbox and a corresponding color. In the Facebook layout style, the chosen color would appear either next to the poster's name below the photo (if he or she is name-tagged in the photo) or in the place where the name would otherwise be (if he or she is not name-tagged) (fig. 2).

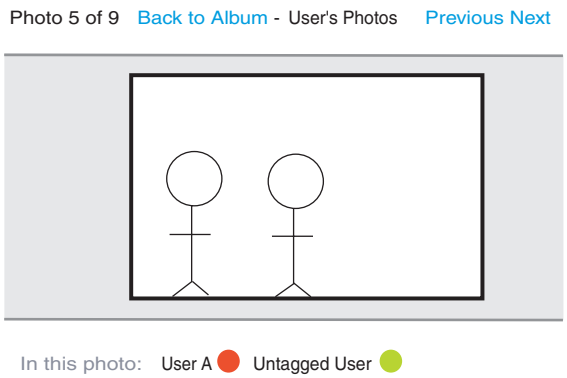

Figure 2: Mock-up of picture viewing screen in Facebook layout style. User A is name-tagged, so his color- coded preference is visible next to his name. The other user is not name-tagged, but his color-coded preference is nevertheless still visible. Note that on Facebook, when the mouse pointer scrolls over "User A" or "Untagged User," a box appears framing the person to whom the name-tag (or anonymous tag) refers.

While the descriptions themselves should be evaluated empirically for accuracy and contextual integrity, a preliminary group might look like this:

- **Green:** This picture can be disseminated throughout this OSN to any user.
- **Yellow:** This picture can be disseminated to anybody to whom I am linked on this OSN.
- **Orange:** This picture can be disseminated only to those to whom I explicitly provide access via this OSN's privacy settings.
- **Red:** This picture can be disseminated only by those who have asked me explicitly for re-posting permission.

- **Black:** This picture cannot, under any circumstances, be disseminated.[173]

Skeptics will likely have at least two pressing questions. First, how can we depend on OSNs to do this? In short, we cannot. But luckily, law provides a useful incentivizing force. There are many ways in which United States law can compel OSNs to adopt such a system. Perhaps most straightforwardly, the FTC can incentivize adoption via its adjudicatory authority. Subchapter I of the Federal Trade Commission Act provides that the FTC is "empowered and directed to prevent persons . . . [and] corporations . . . from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce."[174] If the FTC were to determine that failure to provide a preference expression system is an "unfair" act or practice, the Commission could issue a complaint to the offending OSN.[175] Even if the OSN were to successfully challenge the complaint, by flagging the system as something the FTC will look for when evaluating an OSN's privacy practices, such a tactical move would send a strong signal to other OSNs that they can minimize the risk of conflict with the FTC (and the bad press this sort of conflict entails) by providing the system.[176]

173. In light of the well-documented fact that users tend not to thoroughly read privacy policies, a color code might facilitate knowledge through experience for those who do not read the descriptions. In other words, over time, the colors will attain contextual meaning through continued use and recognition. Also, the colors are mapped (in part) onto the traffic light scheme with which most users will presumably be familiar.

174. 15 U.S.C. § 45 (2006).

175. *Id.* § 45(b).

176. In fact, the FTC has been relatively active in using its adjudicatory authority to improve industry privacy practice. *See Legal Resources*, BUREAU OF CONSUMER PROTECTION BUSINESS CENTER, http://www.ftc.gov/privacy/privacy initiatives/promises_enf.html (last visited Mar. 20, 2011) (listing FTC actions charging parties with deceptive or unfair practices under Case Highlights). It should be stressed, however, that the FTC is not unrestrained in its ability to condemn practices it deems as "unfair." According to the FTC Act, the Commission can find unlawful only those acts or practices that are "likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition." 15 U.S.C. § 45(n) (2006). One might reasonably doubt, however, whether the FTC would train its enforcement weaponry on such a narrow target. One might still expect the agency to exert some influence on industry practice via "nonenforcement regulatory tools." As Kenneth Bamberger and Deidre Mulligan demonstrate, such tools (e.g., publicity, best-practice guidance, the encouragement of certification regimes) can be powerful in shaping privacy policy. Kenneth A. Bamberger & Deidre K. Mulligan, *Privacy on the Books and on the Ground,* 63 STAN. L. REV. (forthcoming 2011).

A second approach would be to alter section 230 of the Communications Decency Act to offer a particularized safe harbor for OSNs providing tools enabling users to express privacy preferences for all materials they post. Currently, section 230(c)(2)(A) exempts OSNs from liability for subpar or ineffective efforts taken in "good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected."[177] Similarly, section 230(c)(2)(B) exempts OSNs from liability for "any action taken to enable or make available to information content providers or others the technical means to restrict access to material described [above.]"[178] A slight alteration of this safety net would allow plaintiffs to include OSNs in their lawsuits against tortious re-posters. Consider the following addition to section 230(c)(2):

(C) No provider of an Online Social Network shall be held liable on account of any reasonable action taken to enable or make available to users the technical means to express disclosure preferences with respect to all information posted to the Online Social Network.

(D) Nothing in (C) shall be interpreted to provide exemption from liability for providers of Online Social Networks whose actions to provide users the technical means to express disclosure preferences are either unreasonable or willfully incomprehensive.

Ideally, courts would read this modification to mean that when X sues Y for nonconsensual reposting, X can also sue the OSN provided that the privacy expression tools provided by the OSN are unreasonable or willfully incomprehensive. Ideally, the court would determine reasonableness by applying the sort of cost–benefit test familiar to all first-year torts students.[179] Thus, over time, OSNs would be incentivized to add only those privacy-protecting tools that are beneficial at the margin (i.e., efficient in light of the costs of implementing them).

The differences between the adjudicative regulatory approach and the safe-harbor approach are subtle. While the adjudicative regulatory approach avoids the slow gears of legislative decision-making, it also decouples the oversight process from the tort sys-

177. *See* 47 U.S.C. § 230(c)(2)(A) (2006).

178. 47 U.S.C. § 230(c)(2)(B) (2006).

179. United States v. Carrol Towing Co., 159 F.2d 169, 173 (2d. Cir. 1947) (the algebraic tort liability analysis known as the Hand Formula, articulated by Judge Learned Hand).

tem. By doing so, it takes significant wind out of plaintiffs' sails; whereas under the safe harbor regime, angry plaintiffs could simply join the negligent OSN to their lawsuit, under the adjudicative regulatory approach, they would have to complain to the FTC or wait for the FTC to act on its own. On the other hand, the adjudicative regulatory approach has the benefit of centralized and unambiguous decisionmaking, whereas the safe harbor approach subjects the law to the diffuse interpretation of the various courts.

Yet another related approach would borrow concepts from products liability law. As James Grimmelmann has recently suggested, defective design jurisprudence offers a useful model for compelling OSNs to behave in socially responsible ways.[180] For example, the Third Restatement of Torts provides that a product "is defective in design when the foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design by the seller . . . , and the omission of the alternative design renders the product not reasonably safe."[181] These principles could be used to find that the cost to an OSN of providing a preference expression system would be so minimal relative to the benefits to users that failure to institute such a system necessitates liability.

Even if proponents of this tool find it difficult to mobilize the legislative and administrative machinery to compel OSNs to provide better tools, they can likely provide some benefits via independent action. For example, Facebook's celebrated application programming interface makes it relatively easy for developers to create applications that operate within the Facebook environment. Drawing on Hartzog's privacy box concept, third-party developers could promote the color-coding system themselves via a free application that users could download.[182] Unlike the core solution, which ideally would be engineered by Facebook and embedded in the posting process, this approach would require users to seek out the tool and remind themselves and fellow users to use it. Thus, while a potential expedient, this independent option is a distant second best to an OSN-implemented approach.

Up to this point, we have been assuming that the photos posted on OSNs feature only the poster. This simplifies our task

180. James Grimmelmann, *Privacy as Product Safety*, 19 WIDENER L. REV. 793, 813 (2010).

181. RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 2(b) (1998).

182. I am currently in the process of developing such an application with the gracious support of the New York University Privacy Research Group. Details on the project can be found at www.postpref.com.

markedly, as the posting decision is made by the person who bears the risk of that decision. What happens when multiple people are in the posted picture? How would the proposed privacy tool account for the privacy externalities of a poster's decision?

One possibility is for the tool to take a cue from Facebook's tagging procedure. As mentioned earlier, Facebook provides the opportunity for users to name-tag photos (i.e., draw an invisible box around a face and link a name to the framed face). The proposed tool could piggyback on this tagging functionality. For example, all parties depicted in a photo could be given the opportunity to add disclosure preferences to the photo. The major difference between this sort of tagging and simple name-tagging would be that while anyone can name-tag anyone in a picture, only those people depicted in the picture would be able to add a disclosure preference to a picture in which they are depicted.

In the Facebook layout, when depicted parties express preferences and remain name-tagged, their color-coded preferences could be depicted at the bottom of the picture next to their names (fig. 2). In the event that these parties *do* untag themselves, the color-coded preferences could still be depicted at the bottom, however the parties' names could be deleted (fig. 2). To encourage active preference expression, the standard email sent to tagged users when someone name-tags them could explicitly remind these users to add their disclosure preferences to the picture. An email could also be sent to all persons depicted in a photo whenever the original poster updates his or her disclosure preferences for that photo.

A significant weakness of this system is that it would rely on the tagging behavior of OSN users; absent facial recognition technology, the system would be able to send notification emails only to users already name-tagged in the photo. Another weakness is that the system would have no way of contacting individuals who are depicted in posted photographs but who are not members of the OSN.

Weaknesses aside, this preference tool goes a long way toward reintroducing some context to context-naked OSN privacy settings. Understanding just how far this tool will take us, however, requires a consideration of how it can be expected to interact with privacy law. This is because the full potential of the preference tool I propose requires a one-two punch of code plus law. In the next section, I explain the necessity of this cooperative relationship and argue that the tool will play well with a reformed reasonableness analysis.

B. Reintroducing Context

To be successful, the preference tool needs to accomplish two objectives. First, it needs to reduce the probability that users will misunderstand the operative norms governing posters' posting decisions. Second, it needs to clarify the reasonableness analysis that will take place should a re-posting conflict make its way to court. On its own, the preference tool can address the first objective; the law will need to address the rest.

As Gelman suggests, "[S]imple neighborliness requires that we honor each other's privacy preferences."[183] In other words, Gelman predicts that "Internet users will respect the social force of a plea for privacy if they are faced with such a request at the time they access online content." Absent any enforcement mechanism, "simple social signals" can be relied on to "exert their own force across forums."[184] This optimism is tempting, but we should be wary of designing our policies to fit ideals instead of pragmatics. On what theoretical ground can we expect users to take the poster's preferences into account in deciding whether to re-post?

Again, contextual integrity comes to the rescue. Recall danah boyd's "tripping on the curb" example. Recall also that I argued that OSN technology caused a fundamental transformation of the transmission principles governing the visual interaction between the person who trips and those who see him fall. In physical space (that is to say, offline), a principle of reciprocity dominates—the tripping party is likely to take note of those who see him fall. When a photo of the fall is distributed online, this sense of reciprocity fades away because the tripper has no way of knowing who is viewing his embarrassing moment. This matters because reciprocity has important accountability effects. If Y knows that the tripper saw him witness the fall, Y will be much less likely to feel that she can disseminate the fact, or other representation, of the fall with impunity. We might call this contextual deterrence.

In a sense, the preference tool I propose will help bring the offline principle of reciprocity back into the online privacy fold. Experience with human nature encourages us to expect that a user faced with a photo bearing a red mark will think twice before reposting, *even if* there is no system of legal liability to add bite to the bark. Empirical evidence and economic analysis lead to similar conclusions. For example, Fehr, Fischbacher, and Gächter demonstrate that people "have a tendency to voluntarily cooperate, if treated

183. Gelman, *supra* note 110, at 1343.

184. *Id.*

fairly, and to punish noncooperators."[185] This "strong reciprocity" might have its roots in the struggles of ancient human groups to survive; groups with a disproportionately large number of strong reciprocators were probably "much better able to survive" the many threats that marked early human life.[186]

Even if we assume that the average OSN member will respect the norms expressed by posters, we have to confront the possibility that some will not. While many people respect privacy, some do not. Thus, while code can do much to make OSNs more context-friendly, law is necessary to complete the privacy circle. As Gelman suggests, "[I]f individuals were able to tag content with their preferences . . . one could envision the privacy torts evolving to take account of individual privacy expectations."[187] How exactly would the analysis play out?

To return to our simplified example, imagine that X has posted a picture to a three-person OSN consisting of X, Y, and Z. Imagine further that X has given Y viewing access to her photo and has used the proposed preference tool to assign a ranking of "red" to her photo. Ignoring this signal, Y re-posts the picture, effectively providing viewing access to Z—Y's OSN friend and someone with an ability to harm X—and anyone else Z permits. Assume that the picture includes some information that is useful to Z in his effort to harm X. Finally, Assume that Z takes this action and harms X. Should Y be legally accountable to X under the public disclosure tort?

Earlier I proposed that the presiding court should assess, given the information norms that obtained between Lee and those to whom he provided access, the probability that Lee's picture would have reached the public absent his mother's actions. I also argued that, absent some injection of contextual information at the time of the original posting, courts would be at a loss in determining the substance of the information norms that obtained. In providing evidence of the information norms supporting X's disclosure decision, the proposed tool fills the knowledge gap for the courts, providing them with the contextual information they need.

To illustrate, let us add a little more complexity to our hypothetical. Imagine now that A, B, C, and D join the OSN. Imagine also that X has shared her photo and her preferences with A, B, C, and D. In the language of contextual integrity, X has set herself as

185. Ernst Fehr, Urs Fischbacher & Simon Gächter, *Strong Reciprocity, Human Cooperation, and the Enforcement of Social Norms*, 13 HUMAN NATURE 1, 1 (2002).

186. *Id.* at 5.

187. Gelman, *supra* note 110, at 1344.

sender and Y, A, B, C, and D as receivers. Trampling on X's preferences, Y re-posts and thus alters the norms, setting herself as sender and the public—Z—as receiver. Absent Y's actions, the probability that X's picture would have reached Z is likely minimal; because Y, A, B, C, and D have access to X's clearly expressed preferences, we can assume that they would have respected these preferences and refrained from re-posting. Thus, Y should be held liable.

To illustrate further, assume that X's photo depicts X, G, and H, all of whom have expressed privacy preferences with respect to the posted photo. Let us also assume that X assigns a rating of "red," G assigns a rating of "red," and H assigns a rating of "green." As before, Y breaches the trust and re-posts the photo. As before, X (now, along with G) sues Y for public disclosure of private facts. What privacy rating should the court use? Assuming H doesn't care, the court can safely apply the "red" level. But what if H truly wants the picture disseminated to all the world? Is it not unjust (and, in fact, unconstitutional) to dampen H's freedom of expression?

Recall, however, that the remedy here is damages, not an injunction. With public disclosure suits, the oil has already spilled. In short, nobody is preventing H's image from spreading, because it already did. But what about chilling the sharing behavior of future posters? As Gelman has noted, X's "ability to protect [her] privacy may interfere with [Y's] ability to speak [her] life story."[188] In fact, the problem extends beyond the people in the picture. Even if Y is not in the picture, the picture might have some relevance or importance to Y that justifies her interest in taking part in the disclosure decision.

This is a valid concern. Yet I would argue that it is not so much a problem with the proposed approach to the reasonableness test as it is with the tort itself. Recall that the reasonableness analysis is focused only on the question of whether the plaintiff has a reasonable expectation of privacy in the disclosed material. Other elements of the public disclosure analysis—the legitimate concern test, for example—can be expected to help courts judge when the plaintiff's privacy interest is outweighed by the public's need to know. For example, imagine that X, G, and H are all social workers who help people with gambling addictions. Imagine further that the picture depicts X, G, and H at a party of a prominent casino owner. This potential conflict of interest might well justify Y's disclosure decision, X and G's privacy expectations notwithstanding.

188. *Id.* at 1332.

A final concern, though unrelated to free speech, runs to the possibility of a "race to the top." Insofar as users recognize the utility of the preference tool in deterring unwanted disclosure, they might just always choose the most restrictive setting. This would, of course, derail the tool's recontextualizing effect and hamper the legal analysis. It seems unlikely, however, that OSN users would take such an approach. OSN interchanges are all about socialization; users might reasonably worry that taking an extreme privacy attitude—one unrelated to specific contexts of disclosure—would mark them as an impediment to social interchange and detrimentally affect their social capital online. This logic also helps address the concern discussed above with regard to photos depicting multiple people. People will be hesitant to post pictures depicting someone who always chooses an unreasonably high rating. If this person truly cares about participating in the posting exchange, he or she will modify his or her posting behavior or risk exclusion from the socially valuable posting activity.

IV.
CONCLUSION

When Warren and Brandeis penned their classic article on privacy, the Kodak camera and the telephone were state-of-the-art technologies. Early in their discussion, Warren and Brandeis stress that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the housetops.'"[189] The privacy torts can be seen as emerging from a struggle between extant social norms and rapidly developing technologies that threatened them.

In our zeal to adopt fantastic (and useful) new devices, we often forget that these marvels of invention are not autonomous but rather are at our beck and call. In advocating against blind reliance on technological progress, Neil Postman stresses that "once a technology is admitted, it plays out its hand; it does what it is designed to do."[190] He argues that in designing and using technology, "[o]ur task is to understand what that design is." In other words, "when we admit a new technology to the culture, we must do so

189. Warren & Brandeis, *supra* note 89, at 195.

190. NEIL POSTMAN, TECHNOPOLY: THE SURRENDER OF CULTURE TO TECHNOLOGY 7 (1992).

with our eyes wide open."[191] Often, however, we cannot (or do not) foresee the full developmental trajectory of a given technology at the time we invent and implement it. Therefore, we are frequently engaged in a game of catch-up.

Yet it seems that many of the most influential digital hawkers have forsaken our eminently human duty to catch up. No less than Eric Shmidt, the CEO of Google, a company with access to enough information to write my biography, has matter-of-factly stated: "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[192] Similarly, Scott McNealy, the CEO of Sun Microsystems is on record as saying that "you have zero privacy."[193]

Such abdications are disappointing. But they are certainly not demoralizing. As the recent proliferation of blogs, academic papers, and books devoted to digital privacy demonstrates, digital privacy is not so private anymore. Consider Facebook's most recent privacy bungle. In April 2010, Facebook dramatically changed the way users list information on their profiles.[194] While historically, users were able to add information about their personal lives in plain text and limit access to that information to a select group of people, the update forced users to either broadcast that information to the entire Facebook network or refrain from posting it. This is because Facebook began to treat each bit of personal information as a "connection."[195] Under the connections model, user information (e.g., "I like football") shows up as a hyperlink on the user profile. At the time Facebook rolled out this new feature, anybody viewing the home page of the connection (be it "I like football" or "Northern New Jersey Violin Enthusiasts Club") was able to see the full list of users who list that connection in their profiles.

It doesn't take too much imagination to realize the potential chilling effects of this policy (just think about the gay teenager who wants to support gay rights but is not ready to come out publicly). This message wasn't lost on the world. Indeed, the privacy community (and major media institutions such as the New York Times)

191. *Id.*

192. *Google CEO on Privacy*, HUFFINGTON POST (Dec. 7, 2009, 3:43 PM), http://www.huffingtonpost.com/2009/12/07/google-ceo-on-privacy-if_n_383105.html.

193. Polly Sprenger, *Sun on Privacy: Get Over It*, WIRED (Jan. 26, 1999), http://www.wired.com/politics/law/news/1999/01/17538.

194. Kurt Opsahi, *Six Things You Need To Now About Facebook Connections*, ELECTRONIC FRONTIER FOUNDATION (May 4, 2010), http://www.eff.org/deeplinks/2010/05/things-you-need-know-about-facebook.

195. *Id.*

stepped up to bat in a big way to challenge Facebook's arguably irresponsible behavior. While the blogs ranted and the New York Times reported, the Electronic Privacy Information Center, along with fourteen privacy and consumer protection organizations, almost immediately filed a complaint with the FTC.[196] To fan the flames, Senators Charles E. Schumer, Michael F. Bennet, Mark Begich, and Al Franken wrote a letter to Mark Zuckerberg (Co-founder, CEO, and President of Facebook), in which they "express[ed] . . . concern regarding recent changes to the Facebook privacy policy . . . ."[197] By late May, Facebook had reined in the connections model; users can now employ privacy settings to control who can learn of their membership by viewing connection "home pages."[198]

As this slice of current events demonstrates, the privacy landscape changes fast and furiously. Perhaps our best defense against this changing landscape is conscientious innovation. Certainly, the time is ripe for developing creative and effective solutions to the novel privacy problems that today's phenomenally useful technologies produce. As this Note hopefully has demonstrated, it is by no means impossible to bring privacy law up to speed with technological reality. By combining our sophisticated judicial system with the intuition of technologists, incisive creativity of technological philosophers, and nearly limitless possibilities of code, we can help bring the color of context back to an increasingly dichromatic online canvas.

196. *New Facebook Privacy Complaint Filed with Trade Commission*, EPIC (May 5, 2010), http://epic.org/2010/05/new-facebook-privacy-complaint.html.

197. Letter from Charles E. Schumer, Michael F. Bennet, Mark Begich, and Al Franken, United States Senators, to Mark Zuckerberg, Co-founder, CEO, and President, Facebook (Apr. 27, 2010), *available at* http://www.politico.com/news/stories/0410/36406.html).

198. Scott M. Fulton III, *Facebook CEO: 'We are removing the connections privacy model,'* BETANEWS (May 26, 2010), http://www.betanews.com/article/Facebook-CEO-We-are-removing-the-connections-privacy-model/1274906695.