Saving Facebook

James Grimmelmann[*]

ABSTRACT: This Article provides the first comprehensive analysis of the law and policy of privacy on social network sites, using Facebook as its principal example. It explains how Facebook users socialize on the site, why they misunderstand the risks involved, and how their privacy suffers as a result. Facebook offers a socially compelling platform that also facilitates peer-to-peer privacy violations: users harming each others' privacy interests. These two facts are inextricably linked; people use Facebook with the goal of sharing information about themselves. Policymakers cannot make Facebook completely safe, but they can help people use it safely.

The Article makes this case by presenting a rich, factually grounded description of the social dynamics of privacy on Facebook. It then uses that description to evaluate a dozen possible policy interventions. Unhelpful interventions—such as mandatory data portability and bans on underage use—fail because they also fail to engage with key aspects of how and why people use social network sites. On the other hand, the potentially helpful interventions—such as a strengthened public-disclosure tort and a right to opt out completely—succeed because they do engage with these social dynamics.

I. INTRODUCTION 1139
   A. *DEFINITIONS* 1142
   B. *FACEBOOK* 1144

---

[*] Associate Professor of Law, New York Law School. Aislinn Black, Robert Blecker, Elise Boddie, Tai-Heng Cheng, Stephen Ellmann, Diane Fahey, Lauren Gelman, Doni Gweritzman, Chris Hoofnagle, H. Brian Holland, Molly Beutz Land, Jan Lewis, William McGeveran, Rebecca Roiphe, and Clay Shirky provided helpful comments. Earlier versions of this Article were presented at the Social Media and the Commodification of Community workshop at the University of Haifa in May 2008 and at a DIMACS/DyDAn Workshop on Internet Privacy in September 2008. All otherwise-undated websites in footnotes were last visited on March 17, 2009. The description of Facebook's activities is current as of March 17, 2009. Internet citations are formatted according to conventions suggested by the author, which may be found at http://james.grimmelmann.net/essays/CitationPrinciples.pdf.

II. THE SOCIAL DYNAMICS OF PRIVACY ON FACEBOOK....1149
A. MOTIVATIONS....1151
1. Identity....1152
2. Relationship....1154
3. Community....1157
B. RISK EVALUATION....1160
C. HARMS....1164
1. Disclosure....1164
2. Surveillance....1166
3. Instability....1168
4. Disagreement....1171
5. Spillovers....1174
6. Denigration....1175

III. WHAT WON'T WORK....1178
A. MARKET FORCES....1178
B. PRIVACY POLICIES....1181
C. TECHNICAL CONTROLS....1184
D. COMMERCIAL DATA COLLECTION RULES....1187
E. USE RESTRICTIONS....1190
F. DATA "OWNERSHIP"....1192

IV. WHAT WILL (SOMETIMES) WORK....1195
A. PUBLIC DISCLOSURE TORTS....1195
B. RIGHTS OF PUBLICITY....1197
C. RELIABLE OPT-OUT....1198
D. PREDICTABILITY....1200
E. NO CHAIN LETTERS....1202
F. USER-DRIVEN EDUCATION....1203

V. CONCLUSION....1205

I. INTRODUCTION

The first task of technology law is always to understand how people actually use the technology. Consider the phenomenon called "ghost riding the whip." The Facebook page of the "Ghost Riding the Whip Association" links to a video of two young men jumping out of a moving car and dancing around on it as it rolls on, now driverless. If this sounds horribly dangerous, that's because it is. At least two people have been killed ghost riding,[1] and the best-known of the hundreds of ghost-riding videos posted online shows a ghost rider being run over by his own car.[2]

Policymakers could respond to such obviously risky behavior in two ways. One way—the wrong way—would treat ghost riders as passive victims. Surely, sane people would never voluntarily dance around on the hood of a moving car. There must be something wrong with the car that induces them to ghost ride on it. Maybe cars should come with a "NEVER EXIT A MOVING CAR" sticker on the driver-side window. If drivers ignore the stickers, maybe any car with doors and windows that open should be declared unreasonably dangerous. And so on. The problem with this entire way of thinking is that it sees only the car, and not the driver who lets go of the wheel. Cars don't ghost ride the whip; people ghost ride the whip.

To protect drivers from the dangers of ghost riding, policymakers would be better off focusing on the ghost riders themselves. What motivates them? Why do they underestimate the risks? When they get hurt, what went wrong? Engaging with ghost riders' worldviews would suggest modest, incremental policies appropriate to the ways in which ghost riders use automotive technology. Sensible responses would include reducing ghost riding's allure, helping its practitioners appreciate the dangers, and tweaking car design to help drivers regain control quickly.[3] The key principle is to understand the social dynamics of technology use, and tailor policy interventions to fit.

This Article applies this principle to a different problem of risky technology use: privacy on Facebook. Think again about the Ghost Riding

---

1. *See* Garance Burke, *'Look Ma—No Hands!,'* STAR-LEDGER (Newark), Dec. 30, 2006, at 27. A Centers for Disease Control study of the related practice of car surfing—riding on the outside of a car, but one with a driver—found reports of fifty-eight deaths and an additional forty-one injuries over an eighteen-year period. *See Injuries Resulting from Car Surfing 1990–2008*, 57 MORBIDITY & MORTALITY WKLY. REP. 1121, 1121 (2008).

2. *Ghost Ride the Whip*, FUNNYORDIE, http://www.funnyordie.com/videos/428d3416c0.

3. For example, the videos and press accounts suggest that high-speed, showy ghost riding is much more dangerous than low-speed ghost riding in open, flat spaces. It's also evident that ghost riding is a cultural phenomenon, united by two pro-ghost-riding rap songs, and that the videos are the key form of showing off. Thus, rather than trying to stamp out all ghost riding, safety-conscious police should focus on high-profile ghost riders posting online videos of themselves doing particularly unsafe tricks with fast-moving cars. Such videos are greater direct risks and are more appealing to potential copycats.

the Whip Association. Anyone with a Facebook account, including police and potential employers, can easily identify the two ghost riders by name. Not only did these men misunderstand the physical risks of ghost riding, they also misunderstood the privacy risks of Facebook. They're not alone. Over a hundred million people have uploaded personally sensitive information to Facebook, and many of them have been badly burnt as a result. Jobs have been lost, reputations smeared, embarrassing secrets broadcast to the world.

It's temptingly easy to pin the blame for these problems entirely on Facebook. Easy—but wrong. Facebook isn't a privacy carjacker, forcing its victims into compromising situations. It's a carmaker, offering its users a flexible, valuable, socially compelling tool. Its users are the ones ghost riding the privacy whip, dancing around on the roof as they expose their personal information to the world.

Thus, if we seek laws and policies that mitigate the privacy risks of Facebook and other social network sites, we need to go through the same social and psychological analysis. What motivates Facebook users? Why do they underestimate the privacy risks? When their privacy is violated, what went wrong? Responses that don't engage with the answers to these questions can easily make matters worse.

Consider, for example, technical controls: switches that users can flip to keep certain details from being shared in certain ways. Facebook is Exhibit A for the surprising ineffectiveness of technical controls. It has severe privacy problems *and* an admirably comprehensive privacy-protection architecture. The problem is that it's extraordinarily hard—indeed, often impossible—to translate ambiguous and contested user norms of information-sharing into hard-edged software rules. As soon as the technical controls get in the way of socializing, users disable and misuse them. This story is typical; other seemingly attractive privacy "protections" miss essential social dynamics.

Thus, this Article provides the first careful and comprehensive analysis of the law and policy of privacy on social network sites, using Facebook as its principal example. The rest of Part I provides the necessary background. After clearing up the necessary terminology, it provides a brief history and technical overview of Facebook. Part II then presents a rich, factually grounded description of the social dynamics of privacy on Facebook. Part II.A explains how social network sites allow people to express themselves, form meaningful relationships, and see themselves as valued members of a community. Part II.B shows how these social motivations are closely bound up with the heuristics that people use to evaluate privacy risks, heuristics that often lead them to think that Facebook activities are more private than they actually are. Part II.C finishes by examining the privacy harms that result. The message of Part II is that most of Facebook's privacy problems are the result of neither incompetence nor malice; instead, they're natural consequences of the ways that people enthusiastically use Facebook.

Having described the social dynamics of privacy on Facebook, the Article applies that description in Parts III and IV, distinguishing helpful from unhelpful policy responses. Part III is negative; it shows how policy prescriptions can go badly wrong when they don't pay attention to these social dynamics:

- Leaving matters up to "the market" doesn't produce an optimal outcome; users' social and cognitive misunderstandings of the privacy risks of Facebook won't disappear anytime soon.

- "Better" privacy policies are irrelevant; users don't pay attention to them when making decisions about their behavior on Facebook.

- "Better" technical controls make matters worse; they cram subtle and complicated human judgments into ill-fitting digital boxes.

- Treating Facebook as a commercial data collector misconstrues the problem; users are voluntarily, even enthusiastically, asking the site to share their personal information widely.

- Trying to restrict access to Facebook is a Sisyphean task; it has passionate, engaged users who will fight back against restrictions.

- Giving users "ownership" over the information that they enter on Facebook is the worst idea of all; it empowers them to run roughshod over others' privacy.

Part IV, on the other hand, is positive; it shows how proposals that do engage with Facebook's social dynamics can sometimes do some good. Each of these proposals seeks to reduce the gap between what users expect to happen to their personal information and what actually happens to it:

- Not everything posted on Facebook is public. Users shouldn't automatically lose their rights of privacy in information solely because it's been put on Facebook somewhere.

- Users' good names are valuable. There's a commercial reputational interest in one's Facebook persona, and using that persona for marketing purposes without consent should be actionable.

- Opt-outs need to be meaningful. People who don't sign up for Facebook, or who sign up but then decide to quit, deserve to have their choices not to participate respected.

- Unpredictable changes are dangerous. Changes that pull the rug out from under users' expectations about privacy should be considered unfair trade practices.

- Strip-mining social networks is bad for the social environment. Bribing users to use a social network site—for example, by giving them rewards when more of their friends sign up—creates unhealthy chain-letter dynamics that subvert relationships.

- Education needs to reach the right audiences. Targeted efforts to explain a few key facts about social-network-site privacy in culturally appropriate ways could help head off some of the more common privacy goofs users make.

Finally, Part V concludes with a brief message of optimism.

A. *DEFINITIONS*

I'll refer to Facebook and its competitors as "social network sites." This phrase captures the idea that Facebook and its competitors are websites designed to be used by people connected in "a social network," a term that sociologists use to describe the structure of interactions within a group of people.[4] I'll rely on danah boyd[5] and Nicole Ellison's definition of "social network sites":

> [Social network sites 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 those made by others within the system.[6]

---

4. *See generally* LINTON C. FREEMAN, THE DEVELOPMENT OF SOCIAL NETWORK ANALYSIS (2004) (describing the history of "social network analysis" in social science). People sometimes refer to Facebook as a "social network," but that usage introduces an ambiguity whenever we want to distinguish between the map (Facebook) and the territory (the relationships among people).

5. I follow boyd's preferred orthography in writing her name without capital letters. *See* danah michele boyd, *What's in a Name?*, DANAH.ORG, http://www.danah.org/name.html.

6. danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, J. COMPUTER-MEDIATED COMM. 13(1), art. 11 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. boyd and Ellison use "social *network* site" rather than "social *networking* site" because "participants are not necessarily 'networking' or looking to meet new

This definition emphasizes the *explicit representation* of connections among users. I don't just write nice things about you on the site; I use the site's tools to create a standardized link from my profile to yours. Social network sites make the graph structure of social networks explicit; users are nodes and connections are links.[7] This design choice has profound implications for the social interactions that take place on such sites.

The definition's three prongs correspond to three important aspects of the social interactions that such sites enable. The first prong—profiles—emphasizes *identity*: users create profiles that represent them. The second prong—contacts—emphasizes *relationships*: users establish one-to-one connections with others. The third prong—traversing lists of contacts—emphasizes *community*: users occupy a specific place among their peers. (Loosely speaking, one could think of these aspects as corresponding to the first, second, and third persons: I, you, them.) I'll use this tripartite structure repeatedly when discussing what people do on social network sites and what privacy on them looks like.

I'll use the term "contact" to describe a user with whom one has an explicit link on a social network site; it's more neutral about the nature of the relationship than the terms used by many sites, such as "friend." The set of one's contacts on a social network site is well-defined; all other users are either contacts or not. On some sites, such as Facebook, being a contact is a symmetrical relationship; if I'm a contact of yours, you're a contact of mine. On other sites, such as LiveJournal, the relationship can be asymmetrical; I can add you as a contact without you adding me as one.[8] Some sites let users annotate their links so that they convey more information than the binary contact/not-a-contact distinction; for example, Orkut lets users indicate that they are "fans" of particular contacts.[9]

The term "social graph" is commonly used to refer to the entire network of users and explicit contact links on a social network site, or, by metonymy, to the idealized network of users and explicit contact links that would exist if the same site stored all significant human relationships.[10] When we speak of a user's "social network" in the context of a specific site, we usually mean something fuzzier and more subjective: the set of people with whom one interacts on the site, even if infrequently, and whether or

---

people; instead, they are primarily communicating with people who are already a part of their extended social network." *Id.* (emphasis added).

7. *See generally* ALBERT-LÁSZLÓ BARABÁSI, LINKED: THE NEW SCIENCE OF NETWORKS 16–18 (2002) (explaining the usefulness of graph theory in modeling real-world social networks).

8. Graph theorists would say that a social network site could have either *directed* or *undirected* links.

9. orkut Help, *"Icons": About Fans*, ORKUT.COM, http://www.google.com/support/orkut/bin/answer.py?hl=en&answer=11766.

10. *See, e.g.*, Brad Fitzpatrick, *Thoughts on the Social Graph*, BRADFITZ.COM, http://bradfitz.com/social-graph-problem/ (Aug. 17, 2007).

not they are listed as contacts. Facebook confuses matters by referring to a "network" of all users associated with a given institution—e.g., a user's "Barnett College Network" is the set of the user's contacts who have indicated that they are affiliated with Barnett College. Social network sites are only one kind of "social software," defined by Clay Shirky as "software that supports group communications."[11]

B. FACEBOOK

Social network sites date to the late 1990s. Some early sites have since closed,[12] but others, like LiveJournal, are still successful today.[13] Social network sites started to enter American mass popular consciousness with Friendster in 2002.[14] A series of technical problems and community-management missteps kept Friendster from fully exploiting its extensive press coverage.[15] Instead, MySpace (over 100 million users[16]) and Facebook (over 175 million users[17]) ate Friendster's lunch. There are many other social network sites, but I'll draw most of my examples from these four.[18]

Facebook was created by an ambitious Harvard student, and it shows.[19] The site, launched in February 2004, took its name (originally "TheFacebook.com") and inspiration from the books of student headshot photos and basic biographical data distributed to Harvard students to tell them about each other. Within a day of its creation, 1,200 students had signed up; within a month, half the undergraduate population had joined.[20] It rapidly expanded to provide "networks" for students at other colleges; by September 2005, Facebook claimed that eighty-five percent of all students at the 882 colleges it supported had Facebook profiles, sixty percent of whom

---

11. Clay Shirky, *Social Software and the Politics of Groups*, NETWORKS, ECON., & CULTURE MAILING LIST, http://www.shirky.com/writings/group_politics.html (Mar. 9, 2003). Other kinds of social software include blogs, wikis, and media-sharing sites, like Flickr and YouTube.

12. *See* boyd & Ellison, *supra* note 6.

13. *See Statistics*, LIVEJOURNAL, http://www.livejournal.com/stats.bml (claiming over 2.2 million active accounts).

14. danah boyd, *Friendster and Publicly Articulated Social Networks*, CONF. ON HUM. FACTORS & COMPUTER SYS. 2 (2004), http://www.danah.org/papers/CHI2004Friendster.pdf.

15. danah boyd, *Friendster Lost Steam. Is MySpace Just a Fad?*, DANAH.ORG, http://www.danah.org/papers/FriendsterMySpaceEssay.html (Mar. 21, 2006).

16. Catherine Holahan, *MySpace: My Portal?*, BUS. WK., June 12, 2008, http://www.businessweek.com/technology/content/jun2008/tc20080612_801233.htm.

17. *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics.

18. *See* DIGFOOT, http://www.digfoot.com/ (providing a directory of over 3700 social network sites).

19. John Markoff, *Who Found the Bright Idea?*, N.Y. TIMES, Sept. 1, 2007, at C1 (discussing competing claims to the "original college social networking system").

20. Sarah Phillips, *A Brief History of Facebook*, GUARDIAN.CO.UK, July 25, 2007, http://www.guardian.co.uk/technology/2007/jul/25/media.newmedia.

logged in daily.[21] Today, Facebook is open to anyone with an email address who is willing to claim to be thirteen or older.[22]

Facebook's roots as a college-based service are still visible in the key role it assigns to Networks. A "Network" is a collection of users with a school, workplace, or region in common.[23] Some of the privacy settings that Facebook offers allow users to restrict access to certain information to members of one of their Networks.[24] To gain access to a college or company network, you need an email address associated with the relevant institution.[25] For example, only people with an @barnett.edu address could access profiles in the (hypothetical) Barnett College Network. Backing up this rule, the terms of use repeatedly forbid signing up with false information.[26]

Facebook's pace of innovation is so blisteringly fast that it's not uncommon to log into the site and see that part of the interface has changed overnight to offer a new feature.[27] Each user's profile page has a "Wall" where other users can post messages.[28] There's also a private, email-like "Message" system,[29] and the "Poke" system, whose only message is "You were poked by ____."[30] Users can also send each other "Gifts" (64x64 pixel icons) for one dollar each.[31] There's a photo-sharing feature, imaginatively

---

21. Michael Arrington, *85% of College Students Use Facebook*, TECHCRUNCH, http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook/ (Sept. 7, 2005).

22. Carolyn Abram, *Welcome to Facebook, Everyone*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?blog_id=company&m=9&y=2006 (Sept. 26, 2006); *Terms of Use*, FACEBOOK, http://www.facebook.com/terms.php (Sept. 23, 2008).

23. *See Networks on Facebook*, FACEBOOK, http://www.new.facebook.com/networks/networks.php (listing the Networks that Facebook offers).

24. *See Facebook Principles*, FACEBOOK, http://www.facebook.com/policy.php?ref=pf ("Your profile information, as well as your name, email and photo, are displayed to people in the networks specified in your privacy settings . . . .").

25. *Networks: Joining or Leaving a Network*, FACEBOOK, http://www.facebook.com/help.php?page=799 (follow "How do I join a supported Facebook network?" hyperlink).

26. *Terms of Use*, *supra* note 22 ("[Y]ou agree to . . . provide accurate, current and complete information about you [and not to] misrepresent . . . your affiliation with any person or entity [and not to] create a false identity on the Service or the Site."). Facebook applies this policy rigorously, almost to the point of absurdity. For example, it banned an Australian rock critic because it didn't believe that she was really named Elmo Keep. Asher Moses, *Banned for Keeps on Facebook for Odd Name*, SYDNEY MORNING HERALD, Sept. 25, 2008, http://www.smh.com.au/news/technology/biztech/banned-for-keeps-on-facebook-for-odd-name/2008/09/25/1222217399252.html.

27. MySpace has also been an aggressive innovator. It's added, among other things, group pages, instant messaging, video-sharing, classified ads, and an application API. MYSPACE.COM, http://www.myspace.com/.

28. *Wall*, FACEBOOK, http://www.facebook.com/help.php?page=443.

29. *Messages and Inbox*, FACEBOOK, http://www.facebook.com/help.php?page=406.

30. *Pokes*, FACEBOOK, http://www.facebook.com/help.php?page=407.

31. *Gifts*, FACEBOOK, http://www.facebook.com/help.php?page=410. For an example of a gift icon, see http://static.ak.fbcdn.net/images/gifts/532.png. *See also* Steve Silberman, *The Mother of All Happy Macs Gives the Gift of Web 2.0*, WIRED, Nov. 7, 2007, http://www.wired.com/

named "Photos," with a clever tagging system: click on a face in a photo—even one posted by someone else—and you can enter the person's name.[32] If it's someone on Facebook, the name becomes a link to his or her profile.

All of these activities generate a rich stream of event notifications. In September 2006, Facebook made that stream visible to users.[33] Each user's homepage displayed a "News Feed"—a list of the most recent notifications from his or her contacts.[34] You'd see that Seth's relationship status changed, that Gwen gave Marcia a gift, that Fred wrote on Shari's Wall, and so on. The announcement of the change generated an uproar over the panoptic privacy implications. Facebook at first defended itself by saying that the information had always been available; users could have looked at the changed profiles directly.[35] Then it partially backed off, allowing users to exclude various items from showing up in others' News Feeds.[36]

Facebook's most technologically interesting feature is its "Platform," which developers can use to create "Applications" that plug seamlessly into the Facebook site.[37] The Platform provides developers an interface to issue instructions to Facebook and gather information from it,[38] along with a custom markup language so that the application's notifications and interface are shown to users with the Facebook look and feel.[39] There are now thousands of Applications, a few of which are runaway successes.[40] Some of the more notable Applications include:

---

print/gadgets/mac/magazine/15-11/ps_macicons (profiling the designer of Facebook Gift icons).

32. *Photos*, FACEBOOK, http://www.facebook.com/help.php?page=412.

33. Susan Kinzie & Yuki Noguchi, *In Online Social Club, Sharing Is the Point Until It Goes Too Far*, WASH. POST, Sept. 7, 2006, at A1.

34. *News Feed*, FACEBOOK, http://www.facebook.com/help.php?page=408.

35. *But see* danah boyd, *Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama*, APOPHENIA, http://www.danah.org/papers/FacebookAndPrivacy.html (Sept. 8, 2006) ("What happened with Facebook was not about a change in the bit state—it was about people feeling icky.")

36. Antone Gonsalves, *Facebook Founder Apologizes in Privacy Flap; Users Given More Control*, INFO. WK., Sept. 8, 2006, http://www.informationweek.com/news/internet/ebusiness/showArticle.jhtml?articleID=192700574.

37. *Build Social Applications on Facebook Platform*, FACEBOOK DEVELOPERS, http://developers.facebook.com/.

38. *API*, FACEBOOK DEVELOPERS WIKI, http://wiki.developers.facebook.com/index.php/API.

39. *FBML*, FACEBOOK DEVELOPERS WIKI, http://wiki.developers.facebook.com/index.php/FBML.

40. Tim O'Reilly, *Good News, Bad News About Facebook Application Market: Long Tail Rules*, O'REILLY RADAR, http://radar.oreilly.com/2007/10/good-news-bad-news-about-faceb.html (Oct. 5, 2007).

- Lexulous, a hugely popular (and possibly infringing[41]) implementation of Scrabble;[42]

- Zombies, in which each user controls a zombie that can bite other users' zombies;[43]

- Causes, which lets users display their social commitments, find other users who support the same causes, and donate money;[44] and

- Quiz Creator, which asks, "Ever wanted your own Facebook app? Too lazy to code? This app's for you! Use this app to create your very own quiz app by filling out a few easy forms!"[45]

Applications can be connected to almost every aspect of one's Facebook experience. For example, Causes writes to your profile page and News Feed, whereas Zombies builds a list of your contacts so that you can decide whom to bite. Facebook now sports an extensive set of options to let users decide what personal data Applications can see and what aspects of their Facebook presence Applications are allowed to spam with messages.[46]

In November 2007, Facebook unveiled Beacon, a system that allows third-party websites to send event notifications to Facebook. For example, Epicurious.com might send a message to Facebook that an Epicurious.com user has reviewed a recipe.[47] Through clever programming,[48] if the user is also logged into Facebook, the message will be associated with her and will

---

41. *See* Complaint at 1, Hasbro, Inc. v. RJ Softwares, No. 08 CIV 6567 (S.D.N.Y. July 24, 2008), http://www.scribd.com/doc/4083968/hasbro-v-scrabulous.

42. *See Lexulous*, FACEBOOK, http://www.facebook.com/applications/Scrabulous/30521 70175.

43. *Zombies*, FACEBOOK, http://www.facebook.com/applications/Zombies/2341504841.

44. *Causes*, FACEBOOK, http://www.facebook.com/applications/Causes/2318966938.

45. *Quiz Creator*, FACEBOOK, http://www.facebook.com/applications/Quiz_Creator/6016 992457.

46. *See Privacy*, FACEBOOK, http://www.facebook.com/help.php?page=419 (listing privacy options available to Facebook users).

47. Press Release, Facebook, Leading Websites Offer Facebook Beacon for Social Distribution (Nov. 6, 2007), http://www.facebook.com/press/releases.php?p=9166. One of Facebook's Beacon partners is Blockbuster; the process of sending notifications about video rentals through Beacon violates the Video Privacy Protection Act, 18 U.S.C. § 2710 (2000). *See* James Grimmelmann, *Facebook and the VPPA: Uh-Oh*, THE LABORATORIUM, http://laboratorium. net/archive/2007/12/10/facebook_and_the_vppa_uhoh (Dec. 10, 2007); *see also* Complaint at 3, Lane v. Facebook, No. 5:2008cv03845 (N.D. Cal. Aug. 12, 2008) (on file with the Iowa Law Review) (alleging that Beacon and Facebook violated several statutes, including the Video Privacy Protection Act).

48. *See* Jay Goldman, *Deconstructing Facebook Beacon JavaScript*, RADIANT CORE, http://www. radiantcore.com/blog/archives/23/11/2007/deconstructingfacebookbeaconjavascript (Nov. 23, 2007) (documenting the iframe/cookie-injction mechanism by which Beacon works).

show up in her News Feed.[49] (An additional Facebook program, "Social Ads," then offers the third-party affiliates the option of showing related ads to her contacts when they see the notification in her News Feed.[50]) Beacon launched with a clearly ineffective opt-out: a transient pop-up window treated inaction as consent, and there was no way to disable Beacon prospectively except on a site-by-site basis as each site tried to send notifications.[51] After dealing with yet another public outcry, Facebook implemented better opt-out procedures.[52] Facebook is currently in the process of launching "Facebook Connect," which allows other websites to embed Facebook features like profiles and friends lists.[53]

The most important distinction between Facebook and its most prominent competitor, MySpace, is that Facebook has fashioned itself around the institution of college.[54] There are plenty of college students on MySpace[55] and plenty of non-college students on Facebook,[56] but Facebook's cultural norms reflect the collegiate experience in a way that MySpace's don't.[57] The difference is also visible in their appearance. Facebook's user interface is tightly controlled; while users and Applications can add text and pictures to a profile, these elements can only appear in Facebook-approved locations and sizes. MySpace, on the other hand, allows users nearly limitless freedom to customize their profile page's design by entering raw HTML.[58] The result is that Facebook pages have the clean lines

49. *How Does Beacon Work*, FACEBOOK, http://www.facebook.com/beacon/faq.php.

50. *Facebook Ads*, FACEBOOK, http://www.facebook.com/help.php?page=409.

51. Ethan Zuckerman, *Facebook Changes the Norms for Web Purchasing and Privacy*, MY HEART'S IN ACCRA, http://www.ethanzuckerman.com/blog/2007/11/15/facebook-changes-the-norms-for-web-purchasing-and-privacy/ (Nov. 15, 2007).

52. Louise Story & Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES, Nov. 30, 2007, at C1; Mark Zuckerberg, *Thoughts on Beacon*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=7584397130 (Dec. 5, 2007).

53. *See Facebook Connect*, FACEBOOK DEVELOPERS, http://developers.facebook.com/connect.php. If you asked me to pick the next Facebook feature to cause a massive privacy implosion, I'd guess Connect, which incorporates the most dangerous features of both Platform (potentially untrustworthy third parties) and Beacon (context violations). The integration with other sites also risks confusing users by making it harder to understand who has control over their personal information and where it's going.

54. danah boyd, *Viewing American Class Divisions Through Facebook and MySpace*, DANAH.ORG, http://www.danah.org/papers/essays/ClassDivisions.html (June 24, 2007).

55. Eszter Hargittai, *Whose Space? Differences Among Users and Non-Users of Social Network Sites*, J. COMPUTER-MEDIATED COMM. 13(1), art. 14 (2007), http://jcmc.indiana.edu/vol13/issue1/hargittai.html.

56. *See* John Schwartz, *73 and Loaded with Friends on Facebook*, N.Y. TIMES, Oct. 14, 2007, § 9, at 1.

57. boyd, *supra* note 54.

58. *See* Dan Perkel, *Copy and Paste Literacy: Literacy Practices in the Production of a MySpace Profile* 5–8, http://people.ischool.berkeley.edu/~dperkel/media/dperkel_literacymyspace.pdf (2006).

of a modernized college dorm; MySpace pages are often hideous but self-expressive like a sticker-laden high-school locker.[59]

This Article will primarily discuss the social dynamics of social-network-site use among young people (roughly, those under thirty) in Anglophone countries. One reason for this limit is a paucity of sources in translation. Another reason is that there are substantial demographic variations in social-network-site usage, the causes and consequences of which are not well understood. A study of college students found that women are more likely to use social network sites than men are and that Hispanics were more likely to use MySpace and less likely to use Facebook than whites were.[60] Similarly, the United States-based Orkut never caught on big at home, but its popularity in Brazil has been a springboard to success in Latin America and Asia.[61] It may be possible to apply the lessons of this Article to other countries and cultures, but in keeping with this Article's thesis, such applications should be grounded in careful study of local patterns of social-network-site use.

II. THE SOCIAL DYNAMICS OF PRIVACY ON FACEBOOK

Facebook knows an immense amount about its users. A fully filled-out Facebook profile contains about forty pieces of recognizably personal information, including name; birthday; political and religious views; online and offline contact information; gender, sexual preference, and relationship status; favorite books, movies, and so on; educational and employment history; and, of course, picture. Facebook then offers multiple tools for users to search out and add potential contacts.[62] By the time you're done, Facebook has a reasonably comprehensive snapshot both of who you are and of whom you know.

The profiles and links are only the beginning. Consider again the features and Applications described above. Each of them serves as a conduit for information-sharing:

---

59. *See* Ze Frank, *Ugly, Designers, MySpace, Ugly, Ugly Song, Mushy Peas, Momma, Happy Birthday Becky*, THE SHOW, http://www.zefrank.com/theshow/archives/2006/07/071406.html (July 14, 2006) ("In MySpace, millions of people have opted out of pre-made templates that 'work' in exchange for ugly. Ugly when compared to pre-existing notions of taste is a bummer. But ugly as a representation of mass experimentation and learning is pretty damn cool."); boyd, *supra* note 15 (describing how MySpace's lack of "parsability" adds to its "subcultural capital").

60. Hargittai, *supra* note 55.

61. Olga Kharif, *Google's Orkut: A World of Ambition*, BUS. WK., Oct. 8, 2007, http://www.businessweek.com/technology/content/oct2007/tc2007107_530965.htm.

62. *See Friends*, FACEBOOK, http://www.facebook.com/help.php?page=441 (suggest contact to current contacts); *Find People You Know on Facebook*, FACEBOOK, http://www.facebook.com/findfriends.php (search for users); Florin Ratiu, *People You May Know*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=15610312130 (May 1, 2008) (get suggestions from Facebook).

- Wall posts can contain information about the poster (one contact who posted on my Wall mentioned an upcoming trip to Pisa), about the postee (another asked about my beard), or about both (a third mentioned a course we'd taken together in college).

- If I Poke you, it indicates that I'm online, and I'm thinking about you.

- The payment infrastructure required by Gifts provides stronger links between a profile and offline identities; choosing one Gift over another (e.g., a "Get Well" balloon rather than a lipstick kiss or a dreidel) has a meaning that at least one other person understands, as does the personalized message accompanying it.

- If I upload and tag a Photo of you, it documents what you look like and someplace that you've been. It also documents that I know you and permits a reasonable inference that I was the photographer.

- Each game of Lexulous you play gives some hints about your vocabulary. Playing a hundred games of Lexulous also says something different about your personality than having a Level 8 Zombie does.

- Your list of Causes tells others what principles are meaningful to you.

- Quiz Creator may not necessarily say much about the people who write quizzes, but the whole point of answering a quiz is to reveal things about your knowledge, beliefs, and preferences.

Put it all together, and your Facebook presence says quite a lot about you.[63] Now, it's true that there's not that much sensitive information in the fact that I have only a Level 1 Ensign Zombie (especially once I add that I play Zombies only for research purposes). But the law often treats many of

63. *See, e.g.*, Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, 28 BULL. SCI. TECH. & SOC. 20, 27–31 (2008) (finding that two-thirds of students surveyed indicated "romantic status and sexual orientation" on their profiles and half indicated their religion). *See generally* danah boyd & Jeffrey Heer, *Profiles as Conversation: Networked Identity Performance on Friendster*, *in* PROCEEDINGS OF THE HAWAI'I INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (2006), http://www.danah.org/papers/HICSS2006.pdf (discussing how people present their identities through profiles).

the other facts in a typical profile—including religious affiliation,[64] sexual orientation,[65] group memberships,[66] events attended,[67] and appearance[68]—as personal, and bars attempts to discover or disclose them.[69] Now multiply this depth of information by almost two hundred million users.

This flood of personal information presents us with a puzzle: Why do so many Facebook users entrust it with so much personal information? The answer is that people have *social* reasons to participate on *social* network sites, and these social motivations explain both why users value Facebook notwithstanding its well-known privacy risks and why they systematically underestimate those risks. Facebook provides users with a forum in which they can craft social identities, forge reciprocal relationships, and accumulate social capital. These are important, even primal, human desires, whose immediacy can trigger systematic biases in the mechanisms that people use to evaluate privacy risks.

A. MOTIVATIONS

People have used computers to socialize for a long time,[70] and new forms of social software take off when they offer users something socially compelling.[71] In this Section, I'll detail three ways in which Facebook scratches its users' social itches. Each drives users to release personal information; each depends on the personal information of other users.

---

64. *See, e.g.*, Soroka v. Dayton Hudson Corp., 1 Cal. Rptr. 2d 77, 86–89 (Ct. App. 1991) (preliminarily enjoining an employer from using a personality test that included religious questions).

65. *See* DoD Instruction No. 1304.26, § E2.2.8.1 (2007) ("Applicants for enlistment, appointment, or induction [into the U. S. military] shall not be asked or required to reveal their sexual orientation . . . .").

66. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–67 (protecting NAACP membership lists against compelled disclosure).

67. *See* Handschu v. Special Servs. Div., No. 71 Civ. 2203 (CSH), 2007 U.S. Dist. LEXIS 43176, at *2–4 (S.D.N.Y. June 13, 2007) (monitoring the New York Police Department's compliance with a consent decree and guidelines preventing certain forms of police photography and videotaping at protests).

68. *See* Times Picayune Publ'g Corp. v. U.S. Dep't of Justice, 37 F. Supp. 2d 472, 474 (1999) (preventing public disclosure of a mug shot).

69. *See, e.g.*, Andrew B. Serwin, Privacy 3.0—The Principle of Proportionality 27–30 (2008) (unpublished manuscript), http://works.bepress.com/cgi/viewcontent.cgi?article=1000&context=andrew_serwin (classifying such information in "Tier 1," the most sensitive of four categories of personal information and the one requiring the greatest legal protection).

70. *See generally* HOWARD RHEINGOLD, THE VIRTUAL COMMUNITY: HOMESTEADING ON THE ELECTRONIC FRONTIER (1993) (detailing the author's experiences participating in early online communities).

71. *See* MARTIN CAMPBELL-KELLY & WILLIAM ASPRAY, COMPUTER: A HISTORY OF THE INFORMATION MACHINE 294–96 (1996) (describing the rapid adoption of email in the 1970s); boyd, *supra* note 15 ("Social technologies succeed when they fit into the social lives and practices of those who engage with the technology.").

1. Identity

The first social factor is the easiest to see: a social network site lets you say who you are. Erving Goffman observed that daily social interactions are full of attempts, large and small, to convince others to accept your claims about yourself.[72] Online interactions are no different; you can use everything from your chat nickname to your home page to influence how other people think of you.[73]

Social network sites offer a gloriously direct tool for what Goffman calls "impression management": the profile page.[74] Just as your choice of clothing and hairstyle signals how you think of yourself (and want others to think of you), so does your choice of profile photo.[75] Many users choose to display the most flattering photographs of themselves that they can.[76] Each additional datum is a strategic revelation, one more daub of paint in your self-portrait. Facebook's profile fields aren't a list of the things most important to its users; they're a list of the things its users most want to say about themselves. The fact that half of the "Personal" fields on a Facebook profile involve favorite forms of media isn't an expression of consumerism; instead, it lets users communicate "prestige, differentiation, authenticity, and theatrical persona" using a common cultural language.[77]

These messages aren't universal; they're self-consciously coded for particular audiences. Since Friendster didn't allow users under eighteen, sixteen-year-olds would list their age as sixty-one, a code understood by other teens.[78] Burning Man attendees, on the other hand, listed their festival nicknames on their profiles, names that would mean nothing if you weren't also a "Burner."[79] The ultimate example of this phenomenon—a literally false, but still intelligible, profile—is the Fakester: a profile for a non-existent person[80] or an unauthorized profile claiming to be a celebrity.[81] While some

---

72. *See generally* ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959) (applying a "dramaturgical" perspective to daily social interactions).

73. *See* PATRICIA WALLACE: THE PSYCHOLOGY OF THE INTERNET 28–37 (1999) (examining the ways in which Internet users manage their online personas).

74. GOFFMAN, *supra* note 72 at 80.

75. *See 65 Ways to Post a Facebook Profile Picture*, BUZZ CANUCK, http://buzzcanuck.typepad.com/agentwildfire/2007/08/65-ways-to-post.html (Aug. 30, 2007).

76. *See* Kristy Ward, *The Psychology of Facebook*, THE CHARLATAN, http://www.charlatan.ca/index.php?option=com_content&task=view&id=20014&Itemid=151 (Mar. 20, 2008).

77. Hugo Liu, *Social Network Profiles as Taste Performances*, J. COMPUTER-MEDIATED COMM. 13(1), art. 13 (2007), http://jcmc.indiana.edu/vol13/issue1/liu.html.

78. boyd & Heer, *supra* note 63, § 3.1.

79. *Id.* § 2.1.

80. *See, e.g.*, *Beer Goggles Egads*, FRIENDSTER, http://profiles.friendster.com/8032093. *See generally* danah boyd, *None of This Is Real: Identity and Participation in Friendster*, *in* STRUCTURES OF PARTICIPATION IN DIGITAL CULTURE 132 (Joe Karaganis ed., 2007), http://www.danah.org/papers/NoneOfThisIsReal.pdf (describing the Fakester phenomenon).

Fakesters were creations of convenience (e.g. "Barnett College"), others were more expressively creative.[82]

Thus, social-network-site profiles are wholly social artifacts: controlled impressions for a specific audience, as much performative as informative.[83] Every letter and pixel of Barack Obama's Facebook profile was carefully crafted to send the precise messages that his campaign wanted to send.[84] I should add that profiles aren't just expressive of identity; they're also constitutive of it. You are the person you present yourself as, to your contacts, in the context of the site, using the site's lexicon of profile questions. Social software has facilitated identity play for a long time,[85] and the paper-doll aspect of a social-network-site profile encourages this dynamic.[86]

Identity construction isn't limited to one's profile; other communications also signal who you are. Joining a "Darfur Action Group" doesn't just encourage your contacts to save Darfur; it also tells them that you're the sort of person who cares about saving Darfur. Similarly, the comments other users leave on your profile become part of your own performance, albeit a part you can't fully control.[87] (Friendster called its profile comments "Testimonials," explicitly encouraging their use for reputation management.) Even your list of contacts makes statements about identity; on Facebook as in life, you're known by the company you keep.[88]

---

81. *See* Clifford J. Levy, *A New Leader's Mandate for Changing Little*, N.Y. TIMES, Apr. 18, 2008, at A12 (quoting the Russian president-elect as saying, "I found about 630 Dmitri Medvedevs" on Odnoklassniki, a Russian social network site)

82. boyd, *supra* note 80, at 148–49 (calling Fakesters "a public art form" and describing "positive feedback" as a consistent goal of Fakester creators). I personally like "Dave Sarfur" on Facebook.

83. *See* Alex Williams, *Here I Am Taking My Own Picture*, N.Y. TIMES, Feb. 19, 2006, § 9, at 1 (quoting experts describing "digital self-portraiture" on social network sites as "self-branding," "theatrical," and "role-playing").

84. *Barack Obama*, FACEBOOK, http://www.facebook.com/barackobama.

85. *See generally* SHERRY TURKLE, LIFE ON THE SCREEN: IDENTITY IN THE AGE OF THE INTERNET 178 (1995) (discussing the Internet's impact on how people present themselves).

86. *See* danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 129 (David Buckingham ed., 2008), http://www.mitpressjournals.org/doi/pdf/10.1162/dmal.9780262524834.119 ("A MySpace profile can be seen as a form of *digital body* where individuals must write themselves into being." (emphasis added)).

87. *See* danah boyd, *Friends, Friendsters, and Top 8: Writing Community into Being on Social Network Sites*, FIRST MONDAY, Dec. 2006, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336.

88. *See* Judith Donath & danah boyd, *Public Displays of Connection*, BT TECH., Oct. 4, 2004, at 71, 77–78.

2. Relationship

The second social factor is that a social network site lets you make new friends and deepen your connection to your current ones. Sharing personal information is a basic component of intimacy.[89] Communications technologies have been connecting people since long before the Internet,[90] and many authors have noted the strength of online relationships.[91]

Some social network sites see themselves as a way for users to meet new people. Friendster's "suggest a match" and "ask for an introduction" buttons leverage existing relationships to create new ones. Its "looking for" profile field is a dating-site touch that's been adopted by many other social network sites: whether you check off "friendship" or "dating" on Facebook, you're signaling an interest in new relationships. Other sites, like Classmates, see themselves as a way for friends who have fallen out of touch to reconnect.[92]

Still, as danah boyd persuasively argues, social network sites are most effective at continuing relationships established offline. In her words, "[T]he popularity of MySpace is deeply rooted in how the site supports sociality amongst preexisting friend groups."[93] Not only do the sites provide a new context for interaction, they can also help in the transmission of social cues that facilitate offline interactions. Friends can learn conversation-triggering things about each other that might have slipped through the cracks in a purely face-to-face age.[94]

If all that social network sites offered were the ability to send other users messages, they'd have little to recommend them over other electronic media, like e-mail and IM. Social network sites work for relationship building because they also provide semi-public, explicit ways to enact relationships. The act of adding someone as a contact is the most fundamental. It's a socially multivalent act, which can mean everything from "I am your friend" to "I'm a fan of yours" to "Please let me see your contacts-

89. *See* Lior Jacob Strahilevitz, *A Social Networks Theory of Privacy*, 72 U. CHI. L. REV. 919, 923–24 & nn.7–8 (2005) (explaining that sharing personal information with others helps form friendships and citing studies indicating that the exchange of personal information promotes friendship).

90. *See, e.g.*, TOM STANDAGE, THE VICTORIAN INTERNET 127–29, 133–39 (1998) (describing romances and weddings carried out via telegraph).

91. *See, e.g.*, JULIAN DIBBELL, MY TINY LIFE: CRIME AND PASSION IN A VIRTUAL WORLD 235–63 (1998) (describing the author's online romance); RHEINGOLD, *supra* note 70, at 20 (describing "heart-to-heart contact" online).

92. *See* Abby Ellin, *Yoo-Hoo, First Love, Remember Me?*, N.Y. TIMES, Feb. 6, 2005, § 9, at 16 (explaining how social network sites "expedite the process" of tracking down old flames).

93. boyd, *supra* note 86, at 126.

94. *See* Clive Thompson, *I'm So Totally, Digitally Close to You*, N.Y. TIMES, Sept. 5, 2008, § Magazine, at 42, http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html (discussing ways that Facebook and other social technologies allow users to maintain connections with increasingly large groups of friends).

only blog."[95] Facebook resolves a bit of this ambiguity with its "Friend Details," with which I can say that I know you from high school, or that we dated, or, amusingly, "I don't even know this person."[96] The act of adding someone as a contact also (by default) gives them access to your profile information, a form of minor intimacy that signals trust.[97]

These explicit contact links then provide a foundation for more robust interactions.[98] Facebook's Gifts are a straightforward performance of regard, and so are the Testimonials that Friendster's users give each other.[99] Everything from uploaded Photos to Event invitations to Zombie bites can be a way to interact with people; the interaction is psychologically valued.[100]

It's important to be sensitive to the social subtleties involved. Something as simple as a Poke can be socially rich,[101] whereas the only important message of a Wall post may be the implicit "You matter to me."[102] Some messages that appear to be sent to the world—like Status updates—may in fact be part of a conversation with specific other users.[103] Friendster users used Testimonials to carry out extended personal conversations, even though Friendster also had a private-messaging feature.[104] Facebook's "Wall-to-Wall" feature, which displays the back-and-forth of Wall posts between two users, explicitly embeds this semi-public conversational mode in the site's

---

95. *See* boyd, *supra* note 87 (listing thirteen reasons to add a user as a contact). On MySpace, things are even more free-form; having a band as a "friend" typically means only that you're a fan of the band, not that you're friends with its members.

96. Frances Wilson, *Do You Facebook?*, TELEGRAPH (London), Sept. 27, 2007, § 7, at 16, http://www.telegraph.co.uk/scienceandtechnology/technology/3354649/Do-you-Facebook.html.

97. *See* boyd, *supra* note 87; *see also* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 34–37 (2008) (discussing the intimacy theory of privacy).

98. Sometimes, they're even a prerequisite; for example, non-contacts can't leave comments on "friends-only" LiveJournals. *See* boredinsomniac, *Frequently Asked Question #120: How Do I Make All My Journal Entries Friends-Only, Private, or Public?*, LIVEJOURNAL, http://www.livejournal.com/support/faqbrowse.bml?faqid=120 (July 24, 2008).

99. *See Testimonials*, FRIENDSTER, http://www.friendster.com/info/testimonials.php ("Friendster makes me feel good because my friends write all these great testimonials about me.").

100. *See* Patti M. Valkenburg et al., *Friend Networking Sites and Their Relationship to Adolescents' Well-Being and Social Self-Esteem*, 9 CYBERPSYCHOLOGY & BEHAV. 584, 584 (2006) (finding that positive feedback on profiles increased users' self-esteem), *draft available at* http://www2.fmg.uva.nl/cam/pdfs/2006_friend_networking_sites.pdf.

101. *See* Dave McClure, *The Zen of Poke: A Facebook Story*, MASTER OF 500 HATS, http://500hats.typepad.com/500blogs/2007/10/the-zen-of-poke.html (Oct. 23, 2007) (listing eighteen possible meanings).

102. *See* danah boyd, *Socializing Digitally*, VODAFONE RECEIVER MAG., June 2007, at 4, http://www.danah.org/papers/VodafoneReceiver.pdf ("Friends are expected to comment as a sign of their affection.").

103. *See* boyd, *supra* note 86, at 124 ("By [writing conversational comments on each other's profiles], teens are taking social interactions between friends into the public sphere for others to witness.").

104. *See* boyd & Heer, *supra* note 63, § 3.

interface design. The norms of social network sites encourage both relationships and public affirmation of them.

These sites also piggyback on the deeply wired human impulse to reciprocate. People reciprocate because it helps them solve collective-action problems, because participation in a gift culture demands that gifts be returned or passed along, because it's disrespectful to spurn social advances, because there's a natural psychological instinct to mirror what one's conversational partner is doing, and because we learn how to conduct ourselves by imitating others. Facebook's design encourages reciprocal behavior by making the gesture-and-return cycle visible and salient. On your home page, the Status Updates box juxtaposes the question, "What's on Your Mind?" with recent answers to that question from your contacts.[105] Even seemingly undirected communications—such as filling out one's profile—implicitly invite conversation using the site's tools.[106]

The use of real names (rather than usernames) and especially of profile photos humanizes the interface, giving a stronger psychological impression of direct interaction. As we know from dealing with panhandlers, telemarketers, and spammers, the more personal the appeal, the harder it is to ignore. Friendster intensifies this personalization by using only first names in contact lists and messages, which emphasizes the intimate tone. The combined effect of these design decisions is to make the user feel like a *bad friend* if she doesn't sign up, write back, and expose personal information. After all, everyone else is doing it.

It's not a coincidence that social network sites activate relational impulses; they're engineered to. Friendster holds a patent on a "Method of inducing content uploads in a social network"—that is, on a way to convince users to upload more photos of themselves and other users.[107] At least four companies have jumped into the business of providing "analytics"—tools that help Application developers study how people are using their Applications and fine-tune them to draw more users.[108] There's even a class at Stanford in which students write Facebook Applications and receive grades based on the number of users that they attract.[109]

---

105. *Status*, FACEBOOK, http://www.facebook.com/help.php?page=706.

106. *See* boyd & Heer, *supra* note 63, § 1 (describing a profile as a "communicative body in conversation with" others).

107. U.S. Patent No. 7,117,254 (filed June 17, 2005).

108. *See* Justin Smith, *Facebook Gives Developers More Metrics—But Who Can You Turn to For Real Insight?*, INSIDE FACEBOOK, http://www.insidefacebook.com/2008/08/07/facebook-gives-developers-more-metrics-but-who-can-you-turn-to-for-real-insight/ (Aug. 7, 2008) (describing KISSMetrics, Sometrics, Kontagent Viral Analytics, and Developer Analytics).

109. *The Stanford Facebook Class*, STANFORD PERSUASIIVE TECH. LAB, http://credibilityserver.stanford.edu/captology/facebook/ (Oct. 28, 2007).

3. Community

The third social factor is that a social network site lets you establish your social position. The basic desire is simple and age-old: to be recognized as a valued member of one's various communities.[110] On social network sites, this desire to fit in and be noticed has several important consequences.

The most basic consequence of this desire is that people would enjoy using a social network site even if they had no reason to use it other than that their friends enjoy using it. If your friends are at the mall, you join them at the mall; if they're on Facebook, you join them on Facebook. As danah boyd puts it, "When I ask teenagers why they joined MySpace, the answer is simple: '*Cuz that's where my friends are.*'"[111] Call it a network externality,[112] call it a coordination game,[113] call it a comedy of the commons[114]—by whatever name, it means that real-life social networks rapidly tip towards mass social-network-site adoption as overlapping groups sign up because all their friends are signing up: Burning Man attendees on Friendster,[115] Los Angeles hipsters on MySpace,[116] Harvard students on Facebook.[117] Of course, signing up is pointless unless you supply enough personal information for your friends to find you.[118]

Another motivation for recreating a real-life social network on a social network site is to visualize it. By representing relationships as hyperlinks, the sites spatialize social networks, mapping the connections within them.[119] It thus becomes possible to see and to speak of an individual's location within networked space, described by Julie Cohen as "a nexus of social practice by embodied human beings."[120] Moving purposefully through informational

---

110. *See, e.g.*, ROBERT D. PUTNAM, BOWLING ALONE 274 (2000) (linking social capital, community membership, and sense of belonging).

111. boyd, *supra* note 86, at 126 (emphasis added).

112. *See* OZ SHY, ECONOMICS OF NETWORK INDUSTRIES 3 (2001) (explaining that the utility of a network product is "affected by the number of people using similar or comparable products").

113. *See* SAMUEL BOWLES, MICROECONOMICS 127–66 (2004) (giving game-theoretic treatment of situations in which players are better off if they take similar actions).

114. *See* Carol Rose, *The Comedy of the Commons: Custom, Commerce, and Inherently Public Property*, 53 U. CHI. L. REV. 711, 768 (1986) (describing social situations in which a "the more the merrier" dynamic prevails).

115. *See* boyd, *supra* note 87.

116. *Id.*

117. Phillips, *supra* note 20.

118. *See* boyd, *supra* note 86, at 127–30 (discussing profile creation and identity management on MySpace).

119. *See generally* DAVID GELERNTNER, MIRROR WORLDS 22–36 (1991) (describing the importance of navigable information spaces that "mirror" offline phenomena).

120. Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 236 (2007).

space can be pleasurable in itself;[121] the traversal function of a social network site offers the experience of navigating your own social geography.

This navigational pleasure also provides an inducement to extend your social horizon. Because many privacy settings are based on network distance, the more contacts you have, the more profiles are visible to you. If you add Seth as a contact, all of his contacts are now contacts-of-contacts of yours—and all of your contacts are now contacts-of-contacts of his. Adding connections fills out your social map, giving you a richer view of your social context.[122] It also makes you yourself more valuable as a contact, since by connecting to you, others can expand their own horizons.[123] Connectedness is social currency.

Moreover, social network sites enable users to negotiate a different kind of social "position": their status within communities. By reifying relationships and making them visible, social network sites enable new forms of competitive, conspicuous accumulation.[124] People compete, for example, to add more contacts. There's an entire niche of programs that will add more MySpace contacts for you.[125] A stand-up comedian racked up 182,000 Facebook contacts in 2005.[126] Facebook later instituted a 5000-contact limit, which led bloggers to protest angrily when they bumped up against it.[127] And it's not just contact counts: any number, badge, or ranking will be treated as a competitive game by someone.[128] Indeed, plenty of Facebook Applications *are* competitive games; it's no coincidence that Scrabulous, Zombies, and other games prominently display each user's scores. My personal favorite for blatant commodification of community is the "Friends

121. *See* JANET H. MURRAY, HAMLET ON THE HOLODECK 129–30 (1997).

122. *See* boyd, *supra* note 14, at 2.

123. *See* BARABÁSI, *supra* note 7, at 55–64 (describing the value of "hubs," i.e., highly connected nodes).

124. *See generally* THORSTEIN VEBLEN, THE THEORY OF THE LEISURE CLASS (Oxford Univ. Press 2007) (1899).

125. *See, e.g.*, ADDERDEMON, http://www.adderdemon.com/; ADDMYFRIENDS, http://www.addmyfriends.com/; FRIENDBLASTERPRO, http://www.addnewfriends.com/.

126. *See* Anne Wootton, *Quest for Facebook Friends Turns into $10K Hurricane Relief Effort*, BROWN DAILY HERALD (Providence), Sept. 9, 2005, http://media.www.browndailyherald.com/media/storage/paper472/news/2005/09/09/CampusWatch/Quest.For.Facebook.Friends.Turns.Into.10k.Hurricane.Relief.Effort-980480.shtml.

127. *See, e.g.*, Robert Scoble, *The You-Don't-Need-More-Friends Lobby*, SCOBLEIZER, http://scobleizer.com/2007/10/14/the-you-dont-need-more-friends-lobby/ (Oct. 14, 2007) (protesting angrily).

128. *See Reputation*, YAHOO! DEVELOPER NETWORK DESIGN PATTERN LIBRARY, http://developer.yahoo.com/ypatterns/parent.php?pattern=reputation (describing the use of patterns like "Leaderboard" and "Collectible Achievements" to harness the user community's competitive desires for good).

for Sale" Application, which has over 2,300,000 users putting price tags on each other.[129]

Similarly, the constant human desire to be part of desirable social groups drives social-network-site adoption and use. One study of college students found "a robust connection between Facebook usage and indicators of social capital, especially of the bridging type."[130] In addition to the direct value of the friendships themselves, you can signal your coolness by having cool friends.[131] Of course, in a familiar pattern, this signal itself becomes devalued if given off too obviously.[132] Some users call anyone else who they think has too many contacts a "slut" or a "whore."[133] Many of these dynamics are driven by the explicit representations of status demanded by the use of a software platform.[134] MySpace had a "Top 8" feature; only the other users on one's Top Friends list would appear on one's profile. danah boyd has documented the "tremendous politics" this feature generated, "not unlike the drama over best and bestest friends in middle school."[135] These "active[] signal[s]" of intimacy and respect use publicly revealed personal information to "work[] through status issues."[136]

* * *

Identity, relationship, and community are not unique to social network sites. They're basic elements of social interaction, offline and on. This urge to sociality is a highly motivating force—only sustenance and safety come before it on the Maslow hierarchy of human needs.[137] It's always been central to the human experience, and it always will be.

As this Section has shown, however, these *social* urges can't be satisfied under conditions of complete secrecy. Identity performance requires an audience; relationships are impossible without others; community *is* a

---

129. *Friends for Sale!*, FACEBOOK, http://www.facebook.com/apps/application.php?api_key=ac434b27ff9de7e3ae41944571c91e34.

130. Nicole Ellison et al., *The Benefits of Facebook "Friends": Social Capital and College Students' Use of Online Social Network Sites*, J. COMPUTER-MEDIATED COMM. 12(4), art. 1 (2007), http://jcmc.indiana.edu/vol12/issue4/ellison.html.

131. *See* boyd, *supra* note 87 (giving, as reason number seven to add a contact, "[t]heir Profile is cool so being Friends makes you look cool").

132. *See* Stephanie Tom Tong et al., *Too Much of a Good Thing? The Relationship Between Number of Friends and Interpersonal Impressions on Facebook*, 13 J. COMPUTER-MEDIATED COMM. 531, 542 (finding that viewers' ratings of a Facebook user's social attractiveness declined as the number of friends listed on the profile increased beyond 300).

133. boyd, *supra* note 87; boyd, *supra* note 80, at 22.

134. *See* James Grimmelmann, Note, *Regulation by Software*, 114 YALE L.J. 1719, 1740 (2005) (explaining that software necessarily applies "explicit ex ante rule[s]").

135. boyd, *supra* note 87.

136. *Id.*

137. *See* A.H. Maslow, *A Theory of Human Motivation*, 50 PSYCHOL. REV. 370, 372–86 (1943) (listing and discussing the basic human needs in order of importance).

public.[138] These factors intertwine; my comment on your Wall is a statement about who I am, an affirmation of our relationship, and a claim to a social position in proximity to you, all at once. Given how deeply these urges run, is it any wonder that social-network-site users are sometimes willing to give up a little privacy in exchange?

B. RISK EVALUATION

The social dynamics of social network sites do more than just give people a reason to use them notwithstanding the privacy risks. They also cause people to *misunderstand* those risks. People rely heavily on informal signals to help them envision their audience and their relationship to it. Facebook systematically delivers signals suggesting an intimate, confidential, and safe setting. Perhaps unsurprisingly, these signals are the same ones that make it such a natural place for socializing.

People don't think about privacy risks in the way that perfectly rational automata would. Instead, real people use all sorts of simplifying heuristics when they think about risk, some psychological (people fear the unfamiliar),[139] some social (people fear what their friends fear),[140] and some cultural (people fear things that threaten their shared worldviews).[141] As one recent review asserts, "culture is *cognitively* prior to facts" in risk evaluation.[142] What people "know" about how the world works drives their perception of risks.

When these risks are privacy risks, and when that evaluation takes place in the context of a social network site, these observations have particular force.[143] For one thing, there is absolutely no plausible way to assign probabilities to many of the possible outcomes. With sufficient data, we could in theory make reasoned decisions about the statistical trustworthiness of large commercial entities.[144] We can't reason in that way about the

138. *See* boyd, *supra* note 86, at 124–26 (describing social interactions among teens carried out in front of "networked publics").

139. *See* CASS SUNSTEIN, LAWS OF FEAR 35–63 (2005).

140. *See id.* at 89–106.

141. *See* MARY DOUGLAS & AARON WILDAVSKY, RISK AND CULTURE: AN ESSAY ON THE SELECTION OF TECHNICAL AND ENVIRONMENTAL DANGERS (1982).

142. Dan M. Kahan et al., *Fear of Democracy: A Cultural Evaluation of Sunstein on Risk*, 119 HARV. L. REV. 1071, 1083 (2006).

143. *See* Lilian Edwards & Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW, AND THE CORPORATION 19 (Andrea Matwyshyn ed., forthcoming 2009), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1148732 ("It is in human nature to want jam today—fun and frivolity—over jam tomorrow – safety and security in some murky future where relationships, job opportunities and promotions may be pursued.").

144. *See generally* Chris Jay Hoofnagle, Measuring Identity Theft (Version 2.0) (June 26, 2008) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1152082 (reporting comparative data on identity-theft-related fraud rates at financial institutions).

complex, situated, emotional–social dynamics of our contact networks. What is the probability that one of my contacts will republish some of my Wall posts on the Internet?[145] The best we can do is rely—and mostly subconsciously—on the proxies for privacy risks that seem to work well in the social settings that we're familiar with. These proxies don't always work so well on Facebook.

The water's fine; come on in. Most of the time, when in doubt, we do what everyone else is doing.[146] Quantitatively, fifty million Facebook users can't be wrong;[147] qualitatively, it must be that your Facebook-trusting friends know something you don't.[148] The problem with this heuristic is that it falsely assumes that other users know something about how safe Facebook is. Mass adoption is an echo chamber, not a careful pooling of information.[149] When our friends all jump off the Facebook privacy bridge, we do too. Those behind us figure we wouldn't have jumped unless it was safe, and the cycle repeats.

Safety in numbers. When we're nervous, we stick with the crowd because it feels safer than being exposed on our own.[150] They won't single *me* out; they can't possibly shoot *all* of us. On a social network site with over a hundred million users, what are the odds that the *New York Times* will write a front-page story about your personal indiscretions? Not high. This kind of reasoning, while perhaps valid for mobs[151] and financial instruments,[152] doesn't work for thinking about social-network-site privacy. Some kinds of

145. *See, e.g.*, Dan Gurewitch, *Epic Burn*, COLLEGEHUMOR, http://www.collegehumor.com/article:1759531 (July 24, 2008). The victim here was lucky; the re-poster blanked out his full name. *Id.*

146. ROBERT B. CIALDINI, INFLUENCE: THE PSYCHOLOGY OF PERSUASION 114–66 (1993) (explaining why it is sometimes, but not always, reasonable to go with the crowd and why most people usually do).

147. *See* JAMES SUROWIECKI, THE WISDOM OF CROWDS, at xi–xxi (2004) (summarizing arguments for the collective intelligence of large groups).

148. If your friends are concerned with privacy and you trust their judgment, Bayesian reasoning says that each time you observe one of them choosing to join a site, you should revise upwards your estimate of the probability that the site is in fact safe. *See generally* STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 426–29 (1995) (explaining Bayes' Theorem, which provides a mathematical rule for updating probability estimates in light of new knowledge).

149. *See* Sushil Bikhchandani et al., *A Theory of Fads, Fashion, Custom, and Cultural Change as Informational Cascades*, 100 J. POL. ECON. 992, 994 (1992).

150. Sometimes it is. *See* W.D. Hamilton, *Geometry for the Selfish Herd*, 31 J. THEORETICAL BIOLOGY 295, 295–311 (1971) (showing how herding behavior can result from self-interested decisions of animals fleeing a predator).

151. *See, e.g.*, W.A. Westley, *The Nature and Control of Hostile Crowds*, 23 CANADIAN J. ECON. & POL. SCI. 33, 38 (1957) (describing the police tactic of "pretend[ing] to know people in the crowd" to destroy crowd members' sense of anonymity and thus to restore order).

152. *See, e.g.*, Kenneth C. Kettering, *Securitization and Its Discontents: The Dynamics of Financial Product Development*, 29 CARDOZO L. REV. 1553, 1632–71 (2008) (assessing the process by which commonly used financial devices become "too big to fail").

privacy problems, such as the arrival of News Feeds, hit everyone on Facebook at once, whereas most individual risks (e.g., a stalker) don't depend on the overall size of the site.[153]

I think we're alone now. We don't say private things when the wrong people are listening in.[154] To know whether they might be, we rely on social[155] and architectural[156] heuristics to help us envision our potential audience.[157] Facebook's design sends mutually reinforcing signals that it's a private space, closed to unwanted outsiders. Seeing contacts' pictures and names makes it easy to visualize talking to them; unlike in a restaurant, potential eavesdroppers are literally invisible.[158]

Nobody in here but us chickens. People tend to assume (incorrectly) that a whole social network site is populated by people like them;[159] it's easy for college students to think that only college students use Facebook. This insularity also inhibits users' ability to remember that not everyone using the site shares their privacy norms.[160] The availability of technical controls (and the language of "control" in Facebook's policies and PR statements) further invites users to think in terms of boundedness, even though the actual network boundaries are highly porous. The powerful, if unspoken, message is that what you say on Facebook will reach your contacts and desired contacts but no one else.

You know me, old buddy, old pal. We don't say private things to people we don't know. Facebook is great at making us feel like we know lots of people. You see where this is going. The pictures, names, and other informal touches make each contact look like a well-known friend. That's socially satisfying, but primate brains only seem capable of maintaining between one

153. To be fair, since privacy norms depend on mass adoption, if everyone makes embarrassing revelations on Facebook, it may contribute to norms of forgiveness. The question of whether we're undergoing a great generational shift in privacy norms—and if so, to what—is a large and important question that I cannot possibly do justice to here.

154. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 508–12 (2007) (describing how courts in Fourth Amendment cases sometimes seek to understand societal expectations of observation).

155. *See* Strahilevitz, *supra* note 89, at 925–27 (discussing how social norms protect disclosures to good friends while anonymity protects disclosures to strangers).

156. *See* Lee Tien, *Architectural Regulation and the Evolution of Social Norms*, 7 YALE J.L. & TECH. 1, 13–15 (2004).

157. *See* boyd, *supra* note 86, at 127–34.

158. *See* DAVID BRIN, THE TRANSPARENT SOCIETY 14–15 (1999) ("An added factor that helps deter people from staring [in a restaurant] is *not wanting to be caught in the act.*").

159. *See* boyd, *supra* note 87; Seth Kugel, *Google's Orkut Captivates Brazilians*, INT'L HERALD TRIB., Apr. 10, 2006, § Finance, at 9, http://www.iht.com/articles/2006/04/09/business/orkut.php ("Almost as soon as Brazilians started taking over Orkut in 2004 . . . English-speaking users formed virulently anti-Brazilian communities like 'Too Many Brazilians on Orkut.'").

160. *See, e.g.*, Gabriel Sherman, *Testing Horace Mann*, N.Y. MAG., Mar. 30, 2007, http://nymag.com/news/features/45592/ (describing the argument over the propriety of a high-school teacher looking at student Facebook groups).

and two hundred close relationships at a time.[161] Everyone else *isn't* a close friend, and the socially thick sense of mutual personal obligation that keeps confidences confidential doesn't always operate as strongly as we expect.

I know how much this means to you. When we say things to people in person, we also tell them our expectations about how much to keep what we say private. We're rarely explicit about it; that's what leaning in, speaking quietly, and touching them on the arm are for. Electronic media are notorious for their ability to garble these nonverbal signals.[162] Especially in young media—such as Facebook—without well-established norms, people may disagree about expectations, leading to misunderstandings about confidentiality.[163]

Cut it out! Do you think I can't see what you're doing? When we trust people, it's often because of mutual surveillance;[164] we'll see if they betray us, and they know it, and we know that they know, and so on. This cooperative equilibrium breaks down easily in electronic media; people exit online communities all the time with spectacular betrayals and recriminations all around.[165] The same reasons there's a mismatch between our own actions on Facebook and our (insufficient) perceptions of being watched also mean there's a mismatch between others' actions and their (insufficient) perceptions of being watched.[166] And finally, the surveillance that most social network sites permit is better for learning personal information than it is for detecting misuse of that information.[167]

---

161. *See* R.I.M. Dunbar, *Neocortex Size as a Constraint on Group Size in Primates*, 22 J. HUM. EVOLUTION 469–93 (1992); Carl Bialik, *Sorry, You May Have Gone Over Your Limit of Network Friends*, WALL ST. J., Nov. 16, 2007, http://online.wsj.com/article/SB119518271549595364.html.

162. WALLACE, *supra* note 73, at 14–19 (describing emoticons as a compensation for the difficulty of conveying tone online).

163. *See* James Grimmelmann, *Accidental Privacy Spills*, 12 J. INTERNET L. 3, 5 (2008) (noting that once confidential information is introduced to online media such as e-mail, it can "spread like wildfire").

164. *Compare* BRIN, *supra* note 158, at 254–57 (promoting "mutually assured surveillance"), *with* Mark Andrejevic, *The Work of Watching One Another: Lateral Surveillance, Risk, and Governance*, 2 SURVEILLANCE & SOC. 479, 494 (2005) ("In an era in which everyone is to be considered potentially suspect, we are invited to become spies—for our own good.").

165. *See, e.g.*, KATIE HAFNER, THE WELL 85–101 (2001) (describing one member's destructive exit from an online community); *cf.* Luís Cabral & Ali Hortaçsu, *The Dynamics of Seller Reputation: Evidence from eBay* 24–31 (N.Y.U., Stern Sch. of Bus., Working Paper EC-06-32, 2006), http://archive.nyu.edu/handle/2451/26094 (documenting "opportunistic exit" by eBay sellers).

166. For a nice discussion of how people's behavior changes when they think that someone might be watching them, read the comments to Hamilton Nolan, *Who's Stalking You on Facebook*, GAWKER (May 13, 2008), http://gawker.com/390004/whos-stalking-you-on-facebook (describing a Facebook "feature" that supposedly provided a "list of the five people who search for your name most often"). The mere thought that searches might be visible to others makes some people freak out.

167. The previous example will serve just as well. Facebook immediately disabled the feature and claimed that it had nothing to do with who was searching for you. *See* Caroline

* * *

These misleading heuristics are all fueled by the relentless use of others' personal information. The more common self-revelation becomes on Facebook, the safer it feels—even when it isn't. If I upload a profile photo, that photo becomes a signal to you to trust me. The more personal your interactions with a few close friends, the less salient the presence of outsiders becomes. This is where the viral nature of Facebook participation is clearest and most frightening. By joining Facebook and adding you as a contact, I convince you to let down your guard. Once I've infected you, you'll help do the same for others.

None of this would happen if Facebook were not catalyzing genuine social interaction. Facebook very quickly gives a strong sense of relationship with other users; that sense is both a satisfying reason to use Facebook and a highly misleading heuristic for evaluating the privacy risks. Tipping dynamics mean that everyone cool is on Facebook; they also make us believe that everyone cool thinks Facebook is privacy-safe. And so on. Plenty of fake things happen on Facebook, but the social interaction is real.

C. HARMS

So far, we've seen that people's reasons for using social network sites and their evaluation of the privacy risks involved are driven by social factors. This Section will describe the similarly social dynamics of six common patterns of privacy violations on social network sites: disclosure, surveillance, instability, disagreement, spillovers, and denigration.

All six patterns are united by a common theme: their "peer-to-peer" nature. Users' privacy is harmed when *other users* learn sensitive personal information about them. Facebook enters the picture as a catalyst; it enables privacy violations more often than it perpetrates them. Because the patterns interlock and interrelate, this Section is not offered as a precise taxonomy of social-network-site privacy harms. Daniel Solove has already created a perfectly good taxonomy of privacy interests in general, so I'll simply refer to his categories as appropriate.[168]

1. Disclosure

One night in the summer of 2006, after a night out drinking, Marc Chiles, a student at the University of Illinois at Urbana-Champaign, was urinating in a bush when a police officer spotted him.[169] Chiles ran away, so

McCarthy, *Facebook Pulls 'Stalker List' Tool After Gawker Exposes It*, WEBWARE, May 13, 2008, http://news.cnet.com/8301-17939_109-9943285-2.html. That restored the status quo in which you could search for other people—thereby gathering information on them—but not learn whether anyone was gathering and distributing information on you and your contacts.

168. *See* SOLOVE, *supra* note 97, at 101–70; Daniel Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 480 (2006).

169. *See* Jodi S. Cohen, *Cop Snares College Pals in Own Web*, CHI. TRIB., Aug. 3, 2006, at C1.

the officer questioned another student, Adam Gartner, who was also present at the scene.[170] Gartner denied knowing the mystery urinator, but the officer logged on to Facebook, where he discovered that Chiles and Gartner were listed as friends.[171] The officer ticketed both of them.[172]

Gartner and Chiles may be more frat-boy than poster-boy, and we may be glad that they incriminated themselves on Facebook, but theirs is still a case about privacy. Specifically, they were victims of what Daniel Solove calls *disclosure*: a fact they'd rather have kept under wraps became more widely known.[173] Unwanted disclosure is everywhere on social network sites.

The best-known examples of unwanted disclosure on social network sites involve students acting their age and being called out for it by authority figures. One college student lost a shot at a summer internship when the company's president saw that his Facebook profile listed "smokin' blunts" as an interest.[174] Disclosure is hardly limited to students, though. Someone blackmailed Miss New Jersey 2007 by sending racy pictures from a private Facebook album to pageant officials.[175] Or consider Sandra Soroka, who posted a Facebook status update saying that she was "letting Will know it's officially over via Facebook status," only to see the story flood the Internet.[176] These people all thought (if only subconsciously) that their Facebook activities would be seen only by a trusted few; they were all wrong.

While people using any social medium often start with the implicit assumption that they're addressing only a peer group, social network sites add two things. First, there's a tighter psychic focus on "speaking" to your

---

170. *Id.*

171. *Id.*

172. *Id.*

173. *See* SOLOVE, *supra* note 97, at 140–46. Chiles was lucky that Gartner didn't upload and tag a photo of him actually doing the deed, as other college students have. *See* Jim Saksa, *Facebook—The Fall of Privacy*, DAILY PENNSYLVANIAN (Philadelphia), Mar. 31, 2008, http://media.www.dailypennsylvanian.com/media/storage/paper882/news/2008/03/31/Opinion/Jim-Saksa.Facebook.The.Fall.Of.Privacy-3292188.shtml ("On Facebook you can find pictures of me in a girl's shirt, urinating in public and drinking in a variety of settings."). That would have crossed the line into what Solove calls *exposure*: "exposing to others certain emotional and physical attributes about a person . . . that people view as deeply primordial." SOLOVE, *supra* note 97, at 146–49.

174. Alan Finder, *When a Risque Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, § 1, at 1.

175. *See* Austin Fenner, *N.J. Miss in a Fix over Her Pics*, N.Y. POST, July 5, 2007, at 5, http://www.nypost.com/seven/07062007/news/regionalnews/n_j__miss_in_a_fix_over_her_pics_regionalnews_austin_fenner__with_post_wire_services.htm ("A mysterious blackmailer has threatened to make public a series of personal web photographs of Miss New Jersey [from her Facebook page] . . . unless she surrenders the crown.")

176. *See* Jenna Wortham, *Is the Infamous Facebook Breakup Actually a Hoax?*, UNDERWIRE, http://blog.wired.com/underwire/2007/12/is-the-infamous.html (Dec. 6, 2007).

preexisting social network.[177] Second, there's a clearer expectation of boundedness; not everyone is "supposed" to be on the site.[178] Facebook's rules about who can and can't join, however, are leaky. Sometimes, people lie when they sign up for social-network-site accounts.[179] Sometimes, they don't need to. College faculty and administrators already have email addresses giving them access to their schools' Networks. Typically, so do alumni, which means that potential employers can ask alums to check on current students for them.[180]

College students have used privacy rhetoric to express their anger about disclosure on Facebook.[181] Their senses of identity and community are at stake. Their elders see them in ways they'd rather not be seen, which is a dignitary insult to their desired identity. Furthermore, their elders see them that way by sneaking onto Facebook, which disrupts the integrity of their chosen social groups.

2. Surveillance

There's also a privacy issue with Facebook investigations even if the investigator doesn't learn much. Solove calls this privacy harm *surveillance*: "awareness that one is being watched."[182] He connects it to "anxiety and discomfort . . . self-censorship and inhibition," even "social control."[183] In my framework, surveillance implicates the relationship interest; the spy has an asymmetrical, violative relationship with her subject. In the student examples, students believe that searches on Facebook break the rules of the student–administrator or student–employer relationship. Even Adam Gartner, whose lie to the police was exposed on Facebook, saw a relational surveillance problem. "I got bone-crushed," he said; "[i]t's a pretty shady way

177. As Lauren Gelman observes, many blog authors choose publicly accessible media "with the thought that someone they cannot identify a priori might find the information interesting or useful." (unpublished draft on file with author).

178. *See* Sherman, *supra* note 160 (summarizing student sentiment as, "[W]hy should students be disciplined for posting to sites that weren't intended to be public?").

179. *See, e.g.*, Indictment at 7–8, United States v. Drew, No. CR-08-582-GW-001 (C.D. Cal. Feb. 2008), http://blog.wired.com/27bstroke6/files/my_space_lori_drew_indictment.pdf. The indictment claims that the defendant created a false MySpace profile in violation of the site's terms of service and that doing so constituted a violation of the federal Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000). This theory is legally questionable. *See, e.g.*, Orin Kerr, *The MySpace Suicide Indictment—And Why It Should Be Dismissed*, VOLOKH CONSPIRACY, http://volokh.com/posts/1210889188.shtml (May 15, 2008) (questioning the legal basis for indictment).

180. *See, e.g.*, Andrew Grossman, *Is This How You Want Your Employer to See You for the First Time?*, MICH. DAILY (Ann Arbor), Apr. 17, 2006, http://www.michigandaily.com/content/how-you-want-your-employer-see-you-first-time.

181. *Id.* (calling employer use of Facebook "unethical").

182. SOLOVE, *supra* note 97, at 106–12. Note that surveillance in this sense, while a direct privacy harm, does lead users to be more cautious, which can have indirect privacy benefits.

183. *Id.* at 108.

they got us."[184] Chiles agreed, saying "It seems kind of unfair."[185] They've got a mental template for the student–police relationship, one with ethical limits; for a police officer to use Facebook in an investigation transgresses those limits. Of course, it isn't just college administrators conducting surveillance on Facebook, it's also police, lawyers,[186] and private investigators.[187]

One-sidedness seems to be a recurring theme of surveillance issues among users. Consider the following paraphrase of a self-confessed "Facebook stalker's"[188] code of ethics:

> With close friends, it is always OK to comment on their profiles; they expect it and might even be upset if you don't. With distant acquaintances, it is almost never OK. It's those in the middle that are tricky; it's OK to bring up their profiles only if there is a reasonable explanation for why you were looking at it in the first place.[189]

Note the social norms coded in these guidelines. The profiles themselves are widely visible. It's fine—indeed intended—for "close friends" to look at one's profile. It's also fine for more distant acquaintances to look at your profile, but there needs to be a social reason. People with no social connection to you *could* look at your profile but *shouldn't*; it's not your responsibility to fence them out.

---

184. *Id.*

185. *Id.*

186. *See* Vesna Jaksic, *Finding Treasures for Cases on Facebook*, NAT'L L.J., Oct. 15, 2007, http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=900005493439.

187. *See* Kevin D. Bousquet, *Facebook.com Vs Your Privacy—By a Private Investigator*, PRIVATE INVESTIGATION CTR., http://corpainvestigation.wordpress.com/2007/04/25/facebookcom-vs-your-privacy-by-a-private-investigator/ (Apr. 25, 2007).

188. "Stalking" means more than just looking at someone's Facebook profile. It's also an obsessive pattern of observing someone else, a pattern that can culminate in violence. Stalking moved online early, *see generally* DEP'T OF JUSTICE, CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY (1999), http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm, and many states now criminalize stalking with statutes specifically targeting online activities, *see* Naomi Harlin Goodno, *Cyberstalking, a New Crime: Evaluating the Effectiveness of Current State and Federal Laws*, 72 MO. L. REV. 125, 149 (2007). The appropriation of the term to describe certain uses of social network sites is a reminder of the high stakes. There are people with Facebook stalkers that they don't know about, some of whom will become criminal stalkers. I would add that older forms of stalking harassment are also migrating to social network sites. *See, e.g.*, People v. Fernino, 851 N.Y.S.2d 339 (Crim. Ct. 2008) (finding that a MySpace friend request could constitute a "contact" in violation of a protective order); Laura Clout, *Man Jailed over Facebook Message*, TELEGRAPH (London), Oct. 5, 2007, http://www.telegraph.co.uk/news/uknews/1565048/Man-jailed-over-Facebook-message.html (describing a similar case on Facebook).

189. Byron Dubow, *Confessions of 'Facebook Stalkers,'* USA TODAY, Mar. 8, 2007, http://www.usatoday.com/tech/webguide/internetlife/2007-03-07-facebook-stalking_N.htm.

Lauren Gelman describes this phenomenon in terms of "blurry-edged social networks"; your profile might be of legitimate social interest to many people, but you're not sure in advance exactly who. By making it broadly viewable, you can reach out to all of them; the social norm against snooping puts implicit limits on how far the information should spread.[190] But since snooping is generally invisible, that's an easy norm to violate.[191] Thus, it may be that the real *faux pas* isn't looking at someone's Facebook page, but letting them know that you did.

This observation explains the trend of the reactions to the News Feed rollout. I suspect that most Facebook users would have opted in to sharing with News Feed for the same reasons that they opted in to Facebook itself. But when News Feed launched, users were made vividly aware that they could now monitor each other, invisibly and in real time. Further, News Feed made it obviously trivial to assemble a rich portrait of a user by combining many individual data points. The *Chicago Tribune*'s HeadCandy blog made this point with a graphic that told the story of a relationship with nothing but News Feed entries, from "Kevin and Jennifer are in a relationship" through "Amy friended Kevin" and "Jennifer wrote on Amy's Wall: 'You tramp'" all the way to "Kevin is now listed as 'single.'"[192]

Thus, Facebook took an activity considered creepy—stalking—and made it psychologically salient for its users. There was no change in the actual accessibility of information, just a shift that focused users' attention on the panoptic prospect of constant, undetectable surveillance.[193] The immediate uproar was unsurprising, as danah boyd has explained.[194] However, as time passed, things settled into the same equilibrium as before. Precisely because the surveillance is invisible, you don't need to think about it, and the distinctive privacy harm of surveillance (as opposed to disclosure) recedes.

3. Instability

One of the most disruptive things that a social network site can do is to change the ground rules of how personal information flows—and social

190. Gelman, *supra* note 177.

191. *Cf., e.g.*, Nara Schoenberg, *Don't Go into Date Blind; Singles Google Before Canoodling*, CHI. TRIB., Apr. 2, 2001, Tempo, at 3 (describing the practice of using Google to research potential romantic partners).

192. Jonathon Berlin, *A Modern Day Romance (Using Facebook's News Feed Feature as a Narrative Device)*, HEADCANDY, http://featuresblogs.chicagotribune.com/headcandy/2008/06/a-modern-day-ro.html (June 25, 2008); *cf.* Sarah Schmelling, *Hamlet (Facebook News Feed Edition)*, MCSWEENEY'S, July 30, 2008, http://mcsweeneys.net/2008/7/30schmelling.html (retelling *Hamlet* in the form of News Feed updates).

193. This surveillance is not panoptic in the Foucaldian sense; it doesn't enforce discipline through internalization. It's panoptic in the more limited, more literal Benthamite sense; you never know whether you're being watched or not.

194. boyd, *supra* note 35.

network sites do it a lot. Friendster and Facebook originally kept profiles wholly internal. Now both sites put "limited profiles" on the public Internet, where search engines can find them.[195] There are opt-outs, but the opt-outs don't address the more fundamental problem: these limited profiles went live after people had uploaded personal information to sites that weren't on the publicly searchable Web.[196] If you—like most people—formed your privacy expectations around the way the site originally worked, they ceased being valid when the site changed.

In Solove's taxonomy, this is a problem of *secondary use*: "the use of data for purposes unrelated to the purposes for which the data was originally collected without the data subject's consent."[197] Helen Nissenbaum's theory of privacy as contextual integrity also pinpoints the problem: once a site has established a social "context" with specific informational "norms of flow," it transgresses those norms by changing the structure of informational flow.[198] Nissenbaum's theory provides an alternate explanation of the privacy problem with News Feed. The information wasn't exposed to the wrong people, wasn't particularly sensitive, and wasn't sent to a more public place.[199] Instead, Facebook changed how profile-update information flowed from users to their contacts. Pull (you visit my profile to check on me) and push (my activities are sent to you automatically) are socially different, so switching between them implicates privacy values.

Social network sites disrupt flow norms in privacy-damaging ways all the time. Friendster launched a "Who's viewed me?" feature in 2005; with it, users could find out which other users had looked at their profiles.[200] We've seen that the inability to know who's watching you on a social network site can lead to a mistaken sense of privacy, so it's possible to defend "Who's viewed me?" as a privacy-promoting step.[201] Perhaps it is, once we reach

195. *See Frequently Asked Questions: What Is My Public (Limited) Profile?*, FRIENDSTER (Jan. 11, 2007), http://friendster.custhelp.com/cgi-bin/friendster.cfg/php/enduser/std_adp.php?p_faqid=192 (discussing the information included in a public profile); *Search*, FACEBOOK, http://www.new.facebook.com/help.php?page=428.

196. *See* danah boyd, *Facebook's "Opt-Out" Precedent*, APOPHENIA, http://www.zephoria.org/thoughts/archives/2007/12/11/facebooks_optou.html (Dec. 11, 2007).

197. SOLOVE, *supra* note 97, at 129–33.

198. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 136–38 (2004).

199. *See id.* at 133–36 (rejecting the principles of government action, sensitivity, and location as insufficient to describe privacy violations).

200. Tara Wheatland, *Friendster's Sneak Attack on Your Anonymity*, BIPLOG (Sept. 29, 2005), http://www.boalt.org/biplog/archive/000631.html. The feature can be disabled; a user willing to give up the ability to see who's viewed his or her page can view other pages anonymously. *Frequently Asked Questions: Who's Viewed Me?*, FRIENDSTER (Feb. 15, 2007), http://friendster.custhelp.com/cgi-bin/friendster.cfg/php/enduser/std_adp.php?p_faqid=212. As Wheatland notes, however, Friendster deployed the feature without announcement, and opting out didn't retroactively efface users' nose prints. Wheatland, *supra*.

201. *See* Lior Strahilevitz, *Friendster and Symmetrical Privacy*, UNIV. CHI. LAW SCH. FACULTY BLOG (Oct. 6, 2005), http://uchicagolaw.typepad.com/faculty/2005/10/friendster_and_.html.

equilibrium, but the unpleasant privacy surprises involved in the transition are themselves a serious problem.[202] They disrupt established relationships and redefine the scope of relevant communities out from under users' feet.

Facebook's Beacon provides another good example of a contextual integrity violation, this time involving an information flow *into* a social network site. E-commerce shoppers don't expect their purchase information to be dispersed to third parties.[203] They especially don't expect it to be imported into social network sites. Pushing purchase data into Facebook thus transgressed the flow norms of two different contexts. Beacon also interfered with certain socially sanctioned forms of secret-keeping: one blogger complained that Facebook ruined his son's birthday by spoiling the surprise when it pushed a video-game purchase out into his Facebook feed where his son could see it.[204]

Finally, it's worth noting that there are both unintentional instability problems—i.e., bugs—and malicious ones—i.e., security breaches. Facebook has had to scramble to fix privacy leaks caused by mistakes in how it handled searches[205] and in how it keeps photos private,[206] and it banned the "Secret

---

See generally BRIN, *supra* note 159. While the principle of "symmetrical privacy" or "mutually assured surveillance" may work in other settings, the "Who's viewed me?" feature probably doesn't actually implement it. Not only does the opt-out mean that anyone willing to give up one kind of surveillance (knowing who's viewed their profile) can engage in another (viewing others' profiles anonymously), users can circumvent even this modest restriction. I have an alternate account on Friendster in addition to my named account. *See Ben*, FRIENDSTER, http://profiles.friendster.com/1327678 (showing me with a paper bag over my head). If I leave my main account in the "Who's viewed me?" system but opt-out with my alternate account, then whenever I want to browse profiles anonymously, I can do so through my alternate account. Meanwhile, my main account can track anyone who's viewing it.

202. *See* Wheatland, *supra* note 201 ("This freaks me out.").

203. *See* JOSEPH TUROW, ANNENBERG PUB. POLICY CTR. OF THE UNIV. OF PA., AMERICANS AND ONLINE PRIVACY: THE SYSTEM IS BROKEN 3–4 (2003), http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/36-page-turow-version-9.pdf [hereinafter TUROW, AMERICANS AND ONLINE PRIVACY]; JOSEPH TUROW ET AL., ANNENBERG PUB. POLICY CTR. OF THE UNIV. OF PA., OPEN TO EXPLOITATION: AMERICA'S SHOPPERS ONLINE AND OFFLINE (2005), http://repository.upenn.edu/cgi/viewcontent.cgi?article=1035&context=asc_papers [hereinafter TUROW ET AL., OPEN TO EXPLOITATION]. Perhaps online shoppers ought to expect their purchase information to be dispersed, given how widely purchase information is shared, online and off. But they don't. *See generally* Chris Jay Hoofnagle & Jennifer King, Research Report: What Californians Understand About Privacy Offline (May 15, 2008) (unpublished manuscript), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1133075 (finding that large fractions of Californians overestimated the legal limits on data sharing by merchants.

204. Mike Monteiro, *Facebook, You Owe Me One Christmas Present*, OFF HOOF (Nov. 20, 2007), http://weblog.muledesign.com/2007/11/facebook_you_owe_me_one_christ.php.

205. *See* Alessandro Acquisti & Ralph Gross, Information Revelation and Privacy in Online Social Networks (The Facebook Case) § 3.5, at 7 (2005) (unpublished manuscript), http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf; Ryan Singel, *Private Facebook Pages Are Not So Private*, WIRED (Oct. 9, 2007) http://www.wired.com/print/software/webservices/news/2007/06/facebookprivacysearch (describing Facebook's move to close a hole that leaked identities of users "who thought they marked their information as private, but didn't also change their search settings").

Crush" Application after security researchers discovered that it tricked users into downloading and installing adware on their computers.[207] Samy Kamkar took advantage of MySpace's profile customization options to write a computer worm that spread from page to page, adding the phrase "but most of all, Samy is my hero."[208] It infected over a million MySpace pages.[209] These may sound like garden-variety computer-security issues, but they're also fueled by social-network-site dynamics. The Samy worm, for example, took advantage of MySpace's identity-promoting profile customization and spread so rapidly because MySpace users formed a highly connected social network.[210]

4. Disagreement

The *New York Times* recently ran an article on the phenomenon of "untagging" on Facebook:

> De-tagging—removing your name from a Facebook photo—has become an image-saving step in the college party cycle. "The event happens, pictures are up within 12 hours, and within another 12 hours people are de-tagging," says Chris Pund, a senior at Radford University in Virginia. . . . "If I'm holding something I shouldn't be holding, I'll untag," says Robyn Backer, a junior at Virginia Wesleyan College. She recalls how her high school principal saw online photos of partying students and suspended the athletes who were holding beer bottles but not those with red plastic cups. "And if I'm making a particularly ugly face, I'll untag myself. Anything really embarrassing, I'll untag."[211]

The remarkable thing about the untagging ritual is that it would be completely unnecessary if there weren't a corresponding tagging ritual. Robyn Backer doesn't want a photo of her holding a beer bottle tagged with her name on Facebook, but the friend who tagged it does.[212] Backer's friend

206. Michael Liedtke, *Security Lapse Exposes Facebook Photos*, MSNBC, Mar. 24, 2008, http://www.msnbc.msn.com/id/23785561/.

207. *See* Matt Hines, *First Serious Facebook Hack?*, PC WORLD, Jan. 3, 2008, http://www.pcworld.com/article/140994/first_serious_facebook_hack.html.

208. Nate Mook, *Cross-Site Scripting Worm Hits MySpace*, BETANEWS, Oct. 13, 2005, http://www.betanews.com/article/CrossSite_Scripting_Worm_Hits_MySpace/1129232391.

209. *Id.*

210. *See id.* (describing how the worm spread with exponential speed by infecting the account of any user viewing an afflicted profile).

211. Lisa Guernsey, *Picture Your Name Here*, N.Y. TIMES, July 27, 2008, Education Life Supplement, at 6.

212. *Cf.* Associated Press, *Unrepentant on Facebook? Expect Jail Time*, CNN.COM, July 18, 2008, http://freedom-school.com/reading-room/unrepentant-on-facebook-expect-jail-time.pdf (describing increasing use by prosecutors of drunk-driving defendants' Facebook party photos to show lack of remorse).

is holding a piece of information that affects her privacy—*this is a photo of Robyn*—but doesn't respect her preferences about that information. That's a relationship problem. Disagreement and privacy problems go hand-in-hand on social network sites.

A photo tag can involve not just two, but three parties: the photographer, the tagger, and the subject. Facebook lets the subject untag the photo, but not demand that it be taken down or made private.[213] Note also that a photo of you that isn't tagged may not be visible to you, and that Facebook also lets users tag photos with the names of nonusers.[214] I'd add, of course, that any given photo can have multiple people in it, and can be tagged by multiple people. These complexities illustrate an important point: it's not easy to uniquely associate each piece of information on a social network site with one person. Whoever has control over the information can use it in ways that others with legitimate interests in it don't like.[215]

This problem is amplified because social network sites require explicit representation of social facts. Offline, I can think of you as "my friend Bob from work" and loosely associate with that hook my various memories of a stressful preparation for an important presentation, a water-balloon fight at the company barbeque, and the way you covered for me when I was sick. All of these thoughts are implicit. I don't need to articulate precisely our relationship or what goes into it; you're just Bob, and I can make decisions about how much to trust you or what to invite you to in an ad-hoc, situational manner, on the basis of all sorts of fuzzy facts and intuitions. But Facebook reifies these social facts into explicit links: we're contacts, or we're not. Everything is explicit and up front—at the cost of flattening our entire relationship into a single bit.[216] Some sites have tried to deal with this information loss by increasing the precision of connections.[217] Flickr, for example, lets users limit access to their photos to contacts they've tagged as "friends" or "family."[218] But this way lies madness; our social lives are

213. *Photos*, FACEBOOK, http://www.new.facebook.com/help.php?page=412.

214. Just because you don't know about a tagged photo doesn't mean that other people can't link it back to you if they want. Researchers at CMU were able to do just that with Friendster profile pictures using off-the-shelf face-recognition software. *See* Acquisti & Gross, *supra* note 205, § 4.2.2.

215. *See* Emma Justice, *Facebook Suicide: The End of a Virtual Life*, TIMES (London), Sept. 15, 2007, http://women.timesonline.co.uk/tol/life_and_style/women/body_and_soul/article2452928.ece (describing a user caught between her jealous boyfriend and an ex-boyfriend who "had posted up old pictures of us together which I had no power to remove").

216. *Cf.* Grimmelmann, *supra* note 134, at 1738–41 (explaining inefficiencies caused by software's insistence on making decisions explicit).

217. *See* Clay Shirky, *YASNSes Get Detailed: Two Pictures*, MANY2MANY (Mar. 9, 2004), http://many.corante.com/archives/2004/03/09/yasnses_get_detailed_two_pictures.php (discussing how Friendster allows users to characterize their friends on a linear scale of friendship).

218. *See Help, FAQ: Sharing*, FLICKR, http://www.flickr.com/help/sharing/. There's something strange about the question, "Is this photo okay for everyone in your family and no one else?" We don't have to answer categorical, hard-edged questions about privacy and

infinitely richer than any controlled vocabulary can comprehend.[219] Consider the RELATIONSHIP project, which aims to provide a "vocabulary for describing relationships between people" using thirty-three terms such as "apprenticeTo," "antagonistOf," "knowsByReputation," "lostContactWith," and "wouldLikeToKnow."[220] Clay Shirky shows what's wrong with the entire enterprise by pointing out that RELATIONSHIP's authors left out "closePersonalFriendOf," "usedToSleepWith," "friendYouDontLike," and every other phrase we could use to describe our real, lived relationships.[221] We shouldn't expect Facebook's formal descriptors to be precise approximations of the social phenomena they represent.[222]

Nor should we expect people to agree about them. You think you're my friend; I disagree. We may be able to work together in real life without needing to confront the basic fact that you like me but not vice versa. But if you Facebook-add me and say, "We dated," what am I supposed to do? Uncheck that box and check "I don't even know this person"? Divergences are made manifest, sometimes to mutual chagrin.[223]

danah boyd has brilliantly documented one example of the social fallout from this fact. MySpace users can choose which "Top Friends" (originally eight, though now up to forty) would show up on their profile page.[224] The feature therefore "requires participants to actively signal their relationship with others" in a context where there's only room for a few people inside the velvet rope.[225] The result is visible, often painful "drama," particularly among younger users who are negotiating similar status issues in

---

relationships in offline social life. Our brains aren't good at it. *Cf.* Heather Richter Lipford et al., *Understanding Privacy Settings in Facebook with an Audience View*, USABILITY PSYCHOL. & SECURITY (2008), http://www.usenix.org/event/upsec08/tech/full_papers/lipford/lipford_html/ (arguing that Facebook could improve users' ability to understand privacy settings by allowing them to view their profiles through others' eyes).

219. *See* Clay Shirky, *RELATIONSHIP: Two Worldviews*, MANY2MANY (Mar. 22, 2004), http://many.corante.com/archives/2004/03/22/relationship_two_worldviews.php ("Human social calculations are in particular a kind of thing that cannot be made formal or explicit without changing them so fundamentally that the model no longer points to the things it is modeled on.").

220. Ian Davis & Eric Vitiello Jr., *RELATIONSHIP: A Vocabulary for Describing Relationships Between People*, VOCAB.ORG (Aug. 10, 2005), http://vocab.org/relationship/.

221. Clay Shirky, *RELATIONSHIP: A Vocabulary for Describing Relationships Between People*, MANY2MANY (Mar. 16, 2004), http://many.corante.com/archives/2004/03/16/relationship_a_vocabulary_for_describing_relationships_between_people.php.

222. *Cf.* danah boyd, *Autistic Social Software*, *in* THE BEST SOFTWARE WRITING I, at 35, 39–41 (Joel Spolsky ed., 2005) (comparing flattened computer representations of social life to an autistic worldview).

223. *See* boyd, *supra* note 80, at 19 ("Expressing social judgments publicly is akin to airing dirty laundry and it is often socially inappropriate to do so. Friend requests on Friendster require people to make social judgments about inclusion and exclusion and—more to the point—to reveal those decisions.").

224. boyd, *supra* note 87.

225. *Id.*

their school peer groups.[226] The fallout from telling a friend she's not a "Top 8" friend is a relationship issue; people joining a social network to connect with friends sometimes find instead that they've been snubbed.

The most tragic example of disagreement is that of Wayne Forrester, who stabbed his estranged wife to death after she changed her Facebook relationship status to "single."[227] Note that it wasn't their separation that he cited as the inciting incident; he'd moved out four days before. Instead, it was the status update—the public assertion about a private relationship—that triggered his derangement.

5. Spillovers

What people do on social network sites has privacy consequences for others. We've already seen how users can upload information—embarrassing photos, for example—about each other. Recall as well that adding contacts is a way to expand your horizon in the social network. That point works in reverse. If Hamlet and Gertrude are contacts, then when Gertrude accepts Claudius's contact request, she may compromise Hamlet's privacy from Claudius. Relying on network structure to limit profile visibility often means relying on the discretion of your contacts and their contacts. But as Clay Shirky observes, "'[F]riend of a friend of a friend' is pronounced 'stranger.'"[228]

I can also leak information about you implicitly. If you attend Barnett College, many of your Facebook contacts probably attend Barnett College too. Even if you don't list a trait on your profile, it may be possible to infer it statistically by looking at the values listed by others in the social network.[229] Researchers using a simple algorithm on LiveJournal were able to predict users' ages and nationalities with good confidence in many cases simply by observing the ages and nationalities of their contacts.[230] How many openly gay friends must you have on a social network before you're outed by implication? The identity privacy interests here are clear, but there are also community ones. Katherine Strandburg has written about the related problem of "relational surveillance," in which the network structure itself is used to infer sensitive information about relationships and group

226. *Id.*

227. *Man Killed Wife in Facebook Row*, BBC NEWS, Oct. 17, 2008, http://news.bbc.co.uk/2/hi/uk_news/england/london/7676285.stm.

228. Shirky, *supra* note 217.

229. *See* Jianming He & Wesley W. Chu, *Protecting Private Information in Online Social Networks*, *in* INTELLIGENCE AND SECURITY INFORMATICS 249, 260–61 (H. Chen & C.C. Yang eds., 2008), http://www.cobase.cs.ucla.edu/tech-docs/jmhek/privacy_protection.pdf (using Bayesian inference to predict user interests on Epinions.com).

230. Ian MacKinnon & Robert H. Warren, *Age and Geographic Inferences of the LiveJournal Social Network*, *in* STATISTICAL NETWORK ANALYSIS: MODELS, ISSUES, AND NEW DIRECTIONS 176, 177–78 (Edoardo Airoldi et al. eds., 2006), http://nlg.cs.cmu.edu/icml_sna/paper2_final.pdf.

activities.[231] The NSA call database is the most famous example of such analysis, but in an aside Strandburg perceptively notes that commercial profilers are likely to start looking at patterns of association on social network sites.[232]

There's an important underlying dynamic that makes these spillover problems more likely. A social network site in motion tends to grow. We've seen the various reasons that people add contacts. One of them is disproportionately important: it's hard to say no to a contact request.[233] Because of explicit representation, there's no way to finesse requests from people you'd rather not invite; rather than embarrass both them and yourself with a visible rejection, it's easier just to click on "Confirm."[234] The same goes for removing contacts; "I don't like you as much as I used to" is a hard message to send, so we don't. And so the networks grow.[235]

This leads not only to large, dense social networks, but also to ones in which the social meaning of being a contact is ambiguous. Facebook "friends" include not only people we'd call "friends" offline, but also those we'd call "acquaintances" (to say nothing of the Fakesters).[236] Contact links are a mixture of what sociologists would call "strong ties" and "weak ties."[237] Weak ties are essential for networking (whether it be finding a job or a spouse);[238] social network sites usefully amplify our limited ability to manage weak ties. The price we pay for that networking, however, is that we must delegate some of our privacy decisions to people with whom we don't have close relationships. Those are precisely the people who are less likely to understand or respect our individual privacy preferences.

6. Denigration

Since a Facebook user's identity is social—it inheres in the impressions she gives and gives off to others[239]—she runs the risk that someone else will mutilate it. If so, then the dignitary side of her privacy interest has been

231. Katherine J. Strandburg, *Freedom of Association in a Networked World: First Amendment Regulation of Relational Surveillance*, 49 B.C. L. REV. 741 *passim* (2008).

232. *Id.* at 765.

233. *See* boyd, *supra* note 87 ("[T]here are significant social costs to rejecting someone.").

234. *See* boyd, *supra* note 80, at 19 (describing the social pressures associated with friend requests).

235. The cycle is self-reinforcing. The more weak-tie contact requests you accept, the worse the insult of implying that someone fails to meet your already-debased standards.

236. *See* boyd, *supra* note 80.

237. *See generally* Mark S. Granovetter, *The Strength of Weak Ties*, 78 AM. J. SOC. 1360 (1973).

238. *See id.* at 1371 ("American blue-collar workers find out about new jobs more through personal contacts than by any other method."); *see also* MALCOLM GLADWELL, THE TIPPING POINT: HOW LITTLE THINGS CAN MAKE A BIG DIFFERENCE 30–88 (2000).

239. *See* GOFFMAN, *supra* note 72, at 2.

harmed.[240] Two of Solove's categories are relevant here. There's *distortion*—"being inaccurately characterized"[241]—and there's *appropriation*—"the use of one's identity or personality for the purposes and goals of another."[242] Both protect "control of the way one presents oneself to society."[243] A comedy sketch broadcast on the BBC, "Facebook in Reality," dramatizes an unwanted Wall post as a "friend" spray-painting crude graffiti on the protagonist's house.[244] As we've seen, your contacts can also blacken your good name by using it to tag embarrassing photos, which Facebook will helpfully link to from your profile. If your contacts are feeling cruel, they could tag photos of someone else as you. Any parts of a profile page that are filled by data supplied by other users could be filled with garbage, explicit pornography, or worse.[245]

You don't even have to be a Facebook user to be a victim of denigration on Facebook. An acquaintance of Matthew Firsht created a fake Facebook profile which falsely said that Firsht was looking for "whatever I can get," that he owed large sums of money, and that he was a member of the "Gay in the Wood . . . Borehamwood" group.[246] This may sound like a classic defamation case, and legally, it was (the defendant argued that someone else had created the false profile). There's still, however, a social-network-site angle to the harm. The use of Facebook amplified the defamation by increasing its credibility: readers would be more likely to assume that Firsht's profile page was, like the typical Facebook profile, actually written by its putative author.[247] Similarly, the social dynamics of the site can both encourage

240. *See* Robert C. Post, *Three Concepts of Privacy*, 89 GEO. L.J. 2087, 2092–96 (2001) (discussing the nexus between dignity and privacy); James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1161–64 (discussing one's privacy as part of one's dignity and liberty).

241. SOLOVE, *supra* note 96, at 158–61.

242. *Id.* at 154–58.

243. *Id.*

244. Idiots of Ants, *Facebook in Reality* (BBC television broadcast), http://www.youtube.com/watch?v=nrlSkU0TFLs.

245. *See* Clay Shirky, *Operation Fuck with the LJ Christians*, MANY2MANY (Apr. 8, 2004), http://many.corante.com/archives/2004/04/08/operation_fuck_with_the_lj_christians.php (describing a LiveJournal prank to fill Christian communities with an image reading, "Hey, Assholes, stop trying to cram your religion down my throat, mm-kay").

246. *See* Jonathan Richards, *'Fake Facebook Profile' Victim Awarded £22,000*, TIMES (London), July 24, 2008, http://technology.timesonline.co.uk/tol/news/tech_and_web/article4389538.ece.

247. *Cf.* Mark A. Lemley, *Rights of Attribution and Integrity in Online Communications*, 1995 J. ONLINE L. art. 2, ¶¶ 30–39, http://web.wm.edu/law/publications/jol/95_96/lemley.html?svr=law (discussing possible privacy torts for impersonation); *see also Jail for Facebook Spoof Moroccan*, BBC NEWS, Feb. 23, 2008, http://news.bbc.co.uk/2/hi/africa/7258950.stm (reporting on a three-year jail sentence for an engineer who created a false Facebook profile of a Moroccan prince).

groups to egg each other on into anti-social behavior[248] and encourage the rapid spread of false information.[249] Even what your contacts do with their own profiles reflects on you; they're *your* contacts after all.

Finally, consider Facebook's Beacon. Not everything I buy or do online reflects me as I'd like to be seen; perhaps I bought that copy of "Bio-Dome" for my Pauly Shore obsessed six-year-old nephew.[250] That's a distortion to the extent that associating it with me impugns my judgment and my honor. Even if I bought this "movie" for myself, I can still have a reputational interest in keeping that fact confidential. Social-network-site profiles are carefully calibrated to present the persona users want to present. If I've gone to some effort to list only French New Wave cinema, "Bio-Dome" hits me where it hurts: in my identity. William McGeveran persuasively argues that Beacon also has an appropriation problem.[251] Putting an advertisement for "Bio-Dome" in my News Feed hijacks my persona—my reputation and credibility with my contacts—for its commercial endorsement value.[252]

* * *

The story of social network sites is the story of what danah boyd calls "social convergence."[253] Our social roles are contextual and audience-specific, but when multiple audiences are present simultaneously, it may not be possible to keep up both performances at once.[254] The stories we've just seen are stories of convergence; Facebook performances leak outwards, while facts inconsistent with our Facebook performances leak inwards. The paradox of Facebook is that the same mechanisms that help it create new

248. *See, e.g.*, Benjamin Ryan, *The Case of the Facebook Four*, NOW LEB., Jan. 23, 2008, http://www.nowlebanon.com/NewsArticleDetails.aspx?ID=27719 (reporting on the arrest of four Lebanese men for "making crude and harassing remarks on a Facebook group dedicated to a female student" and on each others' Walls).

249. *See, e.g.*, Charles Mandel, *Dalhousie Halts Defamatory Facebook Group*, GAZETTE (Montreal), Aug. 24, 2007, http://www.canada.com/montrealgazette/news/story.html?id=c8f236f0-bab2-4be1-913f-e8ecc9316ab8 (describing Dalhousie University's response to the 15,000-member Facebook Group named "Stop Dogs and Puppies from being murdered at Dalhousie University").

250. *See Bio-Dome*, METACRITIC, http://www.metacritic.com/video/titles/biodome (giving "Bio-Dome" a one on a scale of zero to one hundred—the lowest all-time score on Metacritic's average of critics' movie ratings—a rating Metacritic describes as "extreme dislike or disgust").

251. William McGeveran, *Disclosure, Endorsement, and Identity in Social Marketing*, 2009 U. ILL. L. REV. (forthcoming).

252. In addition to the identity interests encompassed by appropriation and distortion, Beacon may also improperly piggyback on users' relationships with their contacts. Channels created for social purposes are misused for commercial ones; Beacon tricks the unintentional endorser into betraying her friend's expectations of loyalty within the relationship. That's a relationship-based harm. Solove might call it *breach of confidence*. *See* SOLOVE, *supra* note 97, at 136–40.

253. danah boyd, *Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence*, 14 CONVERGENCE 13, 19–20 (2008), http://www.danah.org/papers/FacebookPrivacyTrainwreck.pdf.

254. *See* GOFFMAN, *supra* note 72 at 137–40.

social contexts also help it juxtapose them. It offers social differentiation but delivers convergence—which its users experience as a violation of privacy.

III. WHAT WON'T WORK

People who use social network sites get deeply upset about many of the privacy-violating things that happen to them there. If we can avert some of those harms without causing worse ones in the process, we ought to. Sometimes law will be the best tool for the job; at other times changes to software will be better. In other cases, keeping our hands off and letting the market or social norms do the job will do more good.[255] (Of course, we can't and shouldn't worry about preventing every privacy harm that results from Facebook use; just as the law ignores most insults offline, it should ignore most insults on Facebook.)

The problem for policymakers is that many seemingly plausible "fixes" for Facebook actually make things worse. This Part will show how interventions that don't think about Facebook's social dynamics can go catastrophically wrong. When an intervention interferes with users' perceptions of their social environment, they become disoriented and may act in even riskier ways. Worse, when an intervention keeps users from doing what they want to, they fight back.

A. MARKET FORCES

One possible response to privacy concerns is the default: do nothing. On this point of view, while privacy harms are costly, so too is privacy-protecting regulation. If left to their own devices, businesses will naturally sort out an optimal level of privacy protection by offering consumers as much privacy as they actually value.[256] If the government intervenes, it may artificially distort markets in favor of some technologies and against others,[257] while depriving consumers of the benefits of personalized online experiences.[258] This is a powerful argument, but it depends critically on the assumption that market forces will converge on giving users the level of privacy they truly desire.

We have good reason to believe that this assumption is false for social network sites. The problem is that there's a consistent difference between

255. *See* LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE 85–99 (1999).

256. *See generally* PAUL H. RUBIN & THOMAS M. LENERD, PRIVACY AND THE COMMERCIAL USE OF PERSONAL INFORMATION (2002) (finding no failures in the market for personal information and recommending against government intervention).

257. *See, e.g.*, Randal C. Picker, *Competition and Privacy in Web 2.0 and the Cloud* 8–10 (Univ. Chi. L. & Econ., Olin Working Paper No. 414, 2008), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1151985 (discussing how limiting competition can create market power for some firms).

258. *See, e.g.*, Eric Goldman, *A Coasean Analysis of Marketing*, 2006 WIS. L. REV. 1151, 1213–18.

how much privacy users expect when they sign up for a social network site and how much they get.[259] That's a market failure; if users overestimate how much privacy they'll get, they won't negotiate for enough, and companies will rationally respond by undersupplying it. In order to have a well-functioning market for social network sites there would need to be a feedback loop; instead, there's a gap.

The social causes of this gap should be familiar by now. Social-network-site users don't think rationally about the privacy risks involved due to all sorts of deeply wired cognitive biases. Social network sites change their architecture in ways that defeat earlier privacy expectations. Sometimes—as when Facebook allows photo tagging of nonusers—the people who've suffered a privacy loss aren't in a position to negotiate effectively.[260]

Later regret about initial openness is an especially serious problem for the most active social-network-site users: young people.[261] People are time-inconsistent; they care more about privacy as they age.[262] Teens in particular are notorious risk-takers; they do dangerous things, like smoke and drive recklessly, that they later regret, even when given accurate information about the risks.[263] Even if people generally develop more accurate expectations about how social network sites work and the privacy risks involved, hundreds of thousands of children come online each year: people who by definition don't have much experience in what to expect in terms of online privacy. It's quite plausible that these hundreds of thousands of new users form accurate expectations about the privacy risks only by being burned. That wouldn't be good.

Jonathan Zittrain's work on generative technologies also suggests why the social dynamics of social network sites do not tend towards equilibrium.

---

259. *See* Edwards & Brown, *supra* note 143, at 18–20.

260. The intuitive reason why Facebook can't internalize the tagged nonuser's privacy preferences is that if Facebook knows her name and what she looks like but nothing else about her, it's not in a position to find out how much she'd pay not to be tagged. The more subtle reason is that there's a structural difference between a Facebook user choosing the terms of her participation and a nonuser potentially being tagged by any social network site. The former situation is bilateral; if the user and Facebook reach a satisfactory agreement, that's the end of the matter. The latter situation is multilateral; even if the nonuser pays Facebook to go away, MySpace and Bebo and every other site could still tag her. The transaction costs are prohibitive unless the nonuser has a property-style in rem exclusionary right at the outset.

261. *See* AMANDA LENHART ET AL., PEW INTERNET & AM. LIFE PROJECT, TEENS AND SOCIAL MEDIA 13 (2007), http://www.pewinternet.org/~/media//Files/Reports/2007/PIP_Teens_Social_Media_Final.pdf.pdf (finding that fifty-five percent of online teens had a social network profile compared with twenty percent of older users).

262. *See, e.g.*, Emily Gould, *Exposed*, N.Y. TIMES, May 25, 2008, § Magazine, http://www.nytimes.com/2008/05/25/magazine/25internet-t.html (describing how a writer who chronicled her romantic life on her blogs gradually came to regret it).

263. *See* Susan Hanley Duncan, *MySpace Is Also Their Space: Ideas for Keeping Children Safe from Sexual Predators on Social-Networking Sites*, 96 KY. L.J. 527, 554–57 (2008) (explaining that teens may make decisions that develop into "addictions and unhealthy patterns of behavior later in life").

Social network sites are socially generative platforms: their users can socially reconfigure them in new, unexpected, and valuable ways.[264] But Zittrain also shows how generative technologies can be victims of their own success.[265] When sites are small, the social flexibility that makes them compelling also helps users predict and enforce privacy norms. But popularity leads to heavy stress on its early, informal social norms as new users flood in.[266] Early privacy expectations fall apart. danah boyd's description of MySpace's growth shows the dynamic:

> Most people believe that *security through obscurity* will serve as a functional barrier online. For the most part, this is a reasonable assumption. Unless someone is of particular note or interest, why would anyone search for them? Unfortunately for teens, there are two groups who have a great deal of interest in them: those who hold power over them—parents, teachers, local government officials, etc.—and those who wish to prey on them—marketers and predators. Before News Corporation purchased MySpace, most adults had never heard of the site; afterwards, they flocked there either to track teenagers that they knew or to market goods (or promises) to any teen who would listen. This shift ruptured both the imagined community and the actual audience they had to face on a regular basis.[267]

Indeed, given the enthusiasm with which the young have embraced semi-public online media, we as a society will have some serious issues in getting to the steady state needed for the market-equilibrium theory of privacy choices to hold. The divergence in privacy norms between heavily wired teens and their parents (to say nothing of their grandparents) is striking; the personal information *already* online would suffice to ruin the political careers of millions of young people if they were judged by the standards we apply to adult politicians.[268] That overhang of personal

---

264. This is the story danah boyd tells about Fakesters on Friendster. boyd, *supra* note 80, at 22–29. It's also the story that T.L. Taylor tells about EverQuest, T.L. TAYLOR, PLAY BETWEEN WORLDS 136–50 (2006), that Katie Hafner tells about the Well, HAFNER, *supra* note 165, at 25–37, and that Howard Rheingold tells about USENET and BBSes, RHEINGOLD, *supra* note 70, at 110–44.

265. *See* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 67–100 (2008), http://futureoftheinternet.org/static/ZittrainTheFutureoftheInternet.pdf (discussing generative patterns); Jonathan L. Zittrain, *The Generative Internet*, 119 HARV. L. REV. 1974, 1980–96 (2006) (defining "generative" technologies).

266. *See, e.g.*, WENDY M. GROSSMAN, NET.WARS 4–41 (1998) (describing stresses on USENET culture caused by an influx of spammers and AOL users).

267. boyd, *supra* note 86, at 133 (emphasis added).

268. Emily Nussbaum, *Say Everything*, N.Y. MAG., Feb. 12, 2007, at 24 http://nymag.com/news/features/27341 ("More young people are putting more personal information out in public than any older person ever would—and yet they seem mysteriously healthy and normal, save for an entirely different definition of privacy.").

information isn't going away; either society will significantly adjust its privacy norms or a lot of people are going to have some lifelong regrets about their youthful Internet indiscretions.[269] Either way, the precondition for market forces to work effectively—stable privacy preferences—fails. The market prescription leaves matters in the hands of instability-producing social dynamics.

B. PRIVACY POLICIES

Some privacy scholars, companies, and regulators support an informed-choice model of online privacy.[270] On this view, government shouldn't regulate any specific privacy standards; instead, it should make sure that companies clearly tell consumers what will be done with their personal information.[271] Armed with good information, consumers will make good choices. The traditional focus of this approach is the privacy policy; if a site's privacy policy is clear and honest, its users will know what they're getting into and will approve of the consequences.[272]

An examination of Facebook's privacy policy shows that the informed-choice model is completely unrealistic. Everything the model knows is wrong; there's no room in it for the social dynamics of how people actually make privacy-affecting decisions. Facebook's beautifully drafted privacy policy ought to be Exhibit A for informed choice: it bears a TRUSTe seal[273] and contains reassuring statements such as "We share your information with third parties only in limited circumstances" and "Facebook takes appropriate precautions to protect our users' information."[274] Nonetheless, Facebook users don't read it, don't understand it, don't rely on it and certainly aren't protected by it. It's a beautiful irrelevancy. In the first place, most people don't read privacy policies, and even those users who do read them generally don't understand them. Facebook users are no exception. A 2001 poll found that only three percent of the people surveyed claimed to read

269. Anupam Chander, *Youthful Indiscretion in an Internet Age*, *in* PRIVACY AND FREE SPEECH ON THE INTERNET (Martha Nussbaum & Saul Levmore eds., forthcoming 2010) (on file with the Iowa Law Review).

270. *See, e.g.*, Corey A. Ciocchetti, *E-Commerce and Information Privacy: Privacy Policies as Personal Information Protectors*, 44 AM. BUS. L.J. 55, 110–26 (2007) (proposing federal legislation to mandate effective informed choice).

271. Note the absence of substantive regulations from industry policy statements such as SOFTWARE & INFO. INDUS. ASS'N, SIAA FAIR INFORMATION PRACTICE PRINCIPLES (2001), http://www.siia.net/govt/docs/pub/priv_brief_fairinfo.pdf.

272. The approach is typified in, for example, FED. TRADE COMM'N, FAIR INFORMATION PRACTICE PRINCIPLES (2007), http://www.ftc.gov/reports/privacy3/fairinfo.shtm.

273. Facebook remains in good standing with TRUSTe. *Validated Privacy Statement for www.facebook.com*, TRUSTE, http://www.truste.org/ivalidate.php?url=www.facebook.com&sealid=101.

274. *Facebook Principles*, FACEBOOK, http://www.facebook.com/policy.php.

privacy policies carefully "most of the time,"[275] and a 2007 poll found that thirty-one percent claimed to do so.[276] Studies have also found that although the consumers surveyed claimed to care about privacy and to look to see whether sites had privacy policies, large majorities of them were badly misinformed about what those policies actually said.[277] A 2006 survey of Facebook users found that seventy-seven percent had never read its privacy policy and that large majorities had mistaken beliefs about how Facebook collected and shared personal information.[278] Even the twenty-three percent who claimed to have read the policy were no more likely to understand what it allowed.[279] It's hard to fault them; if all Americans actually read the privacy policies of all the sites they visited, they'd be using up $365 billion worth of their time.[280] Between the lawyerly caution, the weasel words, the commingling of many standard terms with the occasional surprising one, the legally mandated warnings and disclaimers, and the legalese, most privacy policies have a painfully low signal-to-noise ratio.

If its users did read Facebook's privacy policy closely—and even more counterfactually, if they understood it—they'd know that it doesn't restrict Facebook's activities in any genuinely significant ways. Here's the paragraph that disclaims any responsibility for actual privacy in no uncertain terms:

> You post User Content (as defined in the Facebook Terms of Use) on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. We cannot control the actions of other Users with whom you may choose to share your pages and information. Therefore, we *cannot and do not guarantee that User Content you post on the Site will not be viewed by unauthorized persons*. We are not responsible for circumvention of any privacy settings or security measures contained on the Site. You

275. HARRIS INTERACTIVE, INC., PRIVACY LEADERSHIP INITIATIVE, PRIVACY NOTICES RESEARCH FINAL RESULTS 2 (2002), http://www.bbbonline.org/UnderstandingPrivacy/library/datasum.pdf (telephone poll conducted Nov. 9–14, 2001).

276. *Zogby Poll: Most Americans Worry About Identity Theft*, ZOGBY INT'L, Apr. 3, 2007, http://www.zogby.com/NEWS/readnews.cfm?ID=1275 (online survey conducted Mar. 23–26, 2007).

277. TUROW, AMERICANS AND ONLINE PRIVACY, *supra* note 203, at 18; TUROW ET AL., OPEN TO EXPLOITATION, *supra* note 203, at 17–19. The percentage of adults using the Internet at home who incorrectly believed that the mere existence of a privacy policy meant that the site offering it would not share personal information with third parties was fifty-seven percent in 2003, TUROW, AMERICANS AND ONLINE PRIVACY, *supra* note 203, at 3, and fifty-nine percent in 2005, TUROW ET AL., OPEN TO EXPLOITATION, *supra* note 203, at 20.

278. Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, *in* PRIVACY ENHANCING TECHNOLOGIES: SIXTH INTERNATIONAL WORKSHOP 36, 54 (George Danezis & Philippe Golle eds., 2006), http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf.

279. *Id.*

280. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: J. OF L. & POL'Y FOR INFO. SOC'Y (forthcoming).

> understand and acknowledge that, even after removal, copies of User Content may remain viewable in cached and archived pages or if other Users have copied or stored your User Content.[281]

Facebook also warns users that it may retain data on them even after they delete their accounts, that it may surveil them even when they're not using Facebook, that it uses their information for marketing purposes (including targeted ads), that it retains discretion over whether and when to share their information with third parties, and that sometimes Facebook even deliberately gives out accounts to let outsiders see what's going on inside.[282] The bottom line, as Facebook repeats near the end of the policy, is that any personal information users upload "may become publicly available."[283]

Moreover, to the extent that it has any binding effect at all, Facebook's privacy policy binds only Facebook. There are plenty of other actors, including other users, Application developers, and law enforcement agents, who can use Facebook's data to invade privacy. In 2005 two MIT students were able to download over 70,000 profiles—over seventy percent of the profiles from the four schools in their study—using an automated script.[284] In late June 2008, Facebook suspended Top Friends, its third-most popular Application (with over a million users[285]), for privacy violations.[286] Of course, Facebook's privacy policy explicitly warns readers that Facebook has no control over other users, Application developers, or the legal system.[287] (Indeed, if some accounts in the blogosphere are to be believed, Facebook has trouble controlling its own employees, who treat access to profile and user-activity information as a "job perk."[288])

We can put one last nail in the coffin of the informed-choice theory: Facebook's reputation on privacy matters is terrible. When people use "Facebook" and "privacy" in the same sentence, the word in between is never

---

281. *Facebook Principles*, *supra* note 274 (emphasis added).

282. *Id.*

283. *Id.*

284. Harvey Jones & José Hiram Soltren, Facebook: Threats to Privacy 13 (Dec. 14, 2005) (unpublished class paper), http://www.swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf.

285. *Top Friends*, FACEBOOK, http://apps.facebook.com/apps/application.php?id=2425101550.

286. Justin Smith, *Breaking: Top Friends Vanishes from Facebook Platform*, INSIDE FACEBOOK (June 26, 2008), http://www.insidefacebook.com/2008/06/26/breaking-top-friends-vanishes-from-facebook-platform/.

287. *Facebook Principles*, *supra* note 274.

288. Nick Douglas, *Facebook Employees Know What Profiles You Look At*, VALLEYWAG (Oct. 27, 2007), http://valleywag.com/tech/scoop/facebook-employees-know-what-profiles-you-look-at-315901.php. *See generally* Owen Thomas, *Why Facebook Employees Are Profiling Users*, VALLEYWAG, http://valleywag.com/tech/your-privacy-is-an-illusion/why-facebook-employees-are-profiling-users-316469.php (Oct. 29, 2007) (collecting posts on Facebook employee misbehavior).

"protects."[289] Facebook's privacy missteps haven't just drawn the attention of bloggers, journalists, scholars, watchdog groups,[290] and regulators[291]; they've also sparked mass outrage among Facebook users. An anti-Beacon group attracted over 70,000 members[292] and an anti-News Feed group over 700,000. [293] Facebook's pattern—launch a problematic feature, offer a ham-handed response to initial complaints, and ultimately make a partial retreat—hasn't given it much privacy credibility.[294] In short, consumers don't, can't, couldn't, and shouldn't rely on Facebook's privacy policy to protect their personal information as they use the site.[295]

C. TECHNICAL CONTROLS

Some scholars think that one of the better ways to protect privacy on Facebook is to give users better technical controls on who can see their personal information.[296] But, as danah boyd's ethnography of teenage MySpace users illustrates, social factors undermine technical controls:

> By choosing to make their profile *private*, teens are able to select who can see their content. This prevents unwanted parents from lurking, but it also means that peers cannot engage with them without inviting them to be Friends. To handle this, teens are often

289. I'm not exaggerating. Searches on Google, Yahoo, MSN, and Lexis (News, All (English, Full Text)) produced zero results for the phrase "Facebook protects privacy."

290. *See, e.g.*, Letter from Philippa Lawson, Dir., Canadian Internet Policy & Pub. Interest Clinic, to Comm'r Stoddart, Privacy Comm'n of Can. (May 30, 2008), http://www.cippic.ca/uploads/CIPPICFacebookComplaint_29May08.pdf [hereinafter PIPEDA Facebook Complaint] (detailing complaints against Facebook under the Personal Information and Protection and Electronic Documents Act by Lawson on behalf of law students); *Facebook Privacy*, ELEC. PRIVACY INFO. CTR., http://epic.org/privacy/facebook/default.html (collecting news and resources).

291. Chris Vallance, *Facebook Faces Privacy Questions*, BBC NEWS, Jan. 18, 2008, http://news.bbc.co.uk/2/hi/technology/7196803.stm (describing an investigation of Facebook by the U.K. Information Commissioner's Office).

292. *Petition: Facebook, Stop Invading My Privacy!*, FACEBOOK, http://www.facebook.com/group.php?gid=5930262681 (72,314 members on Facebook as of Mar. 17, 2009)

293. Story & Stone, *supra* note 52.

294. *See* danah boyd, *Will Facebook Learn from Its Mistake?*, APOPHENIA, http://www.zephoria.org/thoughts/archives/2006/09/07/will_facebook_l.html (Sept. 7, 2006) (describing the pattern).

295. *See generally* JOSEPH TUROW ET AL., THE FEDERAL TRADE COMMISSION AND CONSUMER PRIVACY IN THE COMING DECADE (2006), http://www.ftc.gov/bcp/workshops/techade/pdfs/Turow-and-Hoofnagle1.pdf (criticizing the informed-choice model and calling for substantive regulation).

296. *See* DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 200–03 (2007) (discussing problems with current controls on who can see personal information); Edwards & Brown, *supra* note 143, at 17–23; *see also* Jonathan Zittrain, *What the Publisher Can Teach the Patient: Intellectual Property and Privacy in an Era of Trusted Privication*, 52 STAN. L. REV. 1201, 1226–40 (discussing use of technical measures to provide detailed control over private medical information).

> promiscuous with who they are willing to add as Friends on the site.[297]

The fact is, there's a deep, probably irreconcilable tension between the desire for reliable control over one's information and the desire for unplanned social interaction.[298] It's deeply alien to the human mind to manage privacy using rigid *ex ante* rules. We think about privacy in terms of social rules and social roles, not in terms of access-control lists and file permissions.[299] Thus, when given the choice, users almost always spurn or misuse technical controls, turning instead to social norms of appropriateness and to informal assessments of practical obscurity.

Facebook's experience provides strong evidence of the limited usefulness of technical controls. One of Facebook's two "core principles" is that users "should have control over [their] personal information,"[300] and it implements this principle by offering users a staggeringly comprehensive set of privacy options presented in a clean, attractive interface.[301] Chris Kelly, its Chief Privacy Officer, called its controls "extensive and precise" in testimony to Congress, and emphasized that Facebook's goal was "to give users . . . effective control over their information" through its "privacy architecture."[302] He's not blowing smoke; Facebook has the most comprehensive privacy-management interface I've ever seen. Facebook users have greater technical control over the visibility of their personal information than do users of any of its major competitors.

Not that it matters. Surveys show that many users either don't care about or don't understand how Facebook's software-based privacy settings work. One study by the U.K. Office of Communications found that almost half of social-network-site users left their privacy settings on the default.[303] Another study by a security vendor found that a similar fraction of Facebook users were willing to add a plastic frog as a contact, thereby leaking personal

---

297. boyd, *supra* note 86, at 132 (emphasis added).

298. *See* Gelman, *supra* note 177.

299. *See* Nissenbaum, *supra* note 198, at 155.

300. *Facebook Principles*, *supra* note 274.

301. *See* Naomi Gleit, *More Privacy Options*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=11519877130 (Mar. 19, 2008) (describing Facebook's new privacy interface and options).

302. *Privacy Implications of Online Advertising: Hearing Before the S. Comm. on Commerce, Science, & Transportation*, 110th Cong. 2 (2008) (statement of Chris Kelly, Chief Privacy Officer of Facebook), http://www.insidefacebook.com/wp-content/uploads/2008/07/chriskellyfacebookonlineprivacytestimony.pdf.

303. OFFICE OF COMMC'NS, SOCIAL NETWORKING: A QUANTITATIVE AND QUALITATIVE RESEARCH REPORT INTO ATTITUDES, BEHAVIOURS, AND USE 8 (2008), http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/report.pdf.

information to it.[304] A study of college students found that between twenty and thirty percent didn't know how Facebook's privacy controls worked, how to change them, or even whether they themselves ever had.[305] Indeed, more detailed technical controls can be worse for privacy than less detailed ones. Computer users are often confused by complex interfaces[306] and can easily be talked into overriding security measures designed to protect them.[307] Complexity also requires more maintenance, and Facebook has already gotten into trouble by changing privacy controls with which users were familiar.

The deeper problems are social. There are no ideal technical controls for the use of information in social software. The very idea is an oxymoron; "social" and "technical" are incompatible adjectives here. Adding "FriendYouDontLike" to a controlled vocabulary will not make it socially complete; there's still "FriendYouDidntUsedToLike." As long as there are social nuances that aren't captured in the rules of the network (i.e., always), the network will be unable to prevent them from sparking privacy blowups. Marc Chiles and Adam Gartner would have liked a technical control that would have allowed them to say that they're friends, unless it's the police asking, in which case they're not friends. Facebook could add such a control, but that way lies madness. Increased granularity can also make problems of disagreement worse. Maybe Chiles would have been willing to acknowledge the friendship to members of the "College Administrators" group, but Gartner wouldn't have. If Facebook adds that option, the two of them have something new to argue about—or worse, to be unpleasantly surprised by when one realizes that the other's privacy settings have just gotten him busted.

Another reason that comprehensive technical controls are ineffective can be found in Facebook's other "core principle": that its users should "have access to the information others want to share."[308] If you're already sharing your information with Alice, checking the box that says "Don't show to Bob" will stop Facebook from showing it Bob, but it won't stop Alice from showing it to him. Miss New Jersey, Amy Polumbo, wanted her friends to have access to photos of her dressed up as a salacious Alice in Wonderland;

304. *Sophos Facebook ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves*, SOPHOS (Aug. 14, 2007), http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html.

305. Acquisti & Gross, *supra* note 278, at 16.

306. *See* Roger Dingledine & Nick Mathewson, *Anonymity Loves Company: Usability and the Network Effect*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE 547, 552 (Lorrie Faith Cranor & Simson Garfinkel eds., 2005) ("Extra options often delegate security decisions to those least able to understand what they imply.").

307. *See* BRUCE SCHNEIER, SECRETS AND LIES 266–69 (2000) ("Social engineering [i.e. convincing a computer user to trust you through non-technical means] bypasses cryptography, computer security, network security, and everything else technological.").

308. *Facebook Principles*, *supra* note 274.

if one of them couldn't be trusted, that was the friend's fault, and all the technical controls in the world wouldn't have helped Polumbo. If we've learned anything at all from the digital-rights-management wars, it's that technical controls are rarely effective against a person genuinely determined to redistribute information they've been given access to.[309]

There's also another way of looking at "information others want to share." If I want to share information about myself—and since I'm using a social network site, it's all but certain that I do—anything that makes it harder for me to share is a bug, not a feature. Users will disable any feature that protects their privacy too much.[310] The defaults problem nicely illustrates this point. Lillian Edwards and Ian Brown flirt with the idea that default "privacy settings be set at the most privacy-friendly setting when a profile is first set up," only to recognize that "this is not a desirable start state for social networking."[311] If Facebook profiles started off hidden by default, the next thing each user would do after creating it would be to turn off the invisibility. Social needs induce users to jump over technological hurdles.

D. COMMERCIAL DATA COLLECTION RULES

H. Brian Holland has observed that while users share individually and for social reasons, Facebook's role as a platform gives it access to everyone's data.[312] Large concentrations of personal data in the hands of a single entity raise serious and well-known privacy concerns. One concern is that the government may misuse the data for illegitimate investigations.[313] Another is that the entity itself may misuse the data, whether for marketing or by turning it over to third parties. There are plenty of other contexts in which it

309. *See* Cory Doctorow, European Affairs Coordinator, Elec. Frontier Found., DRM Talk for Hewlett-Packard Research (Sept. 28, 2005), http://craphound.com/hpdrm.txt (applying lessons to conclude that "privacy DRM" cannot work).

310. *See* Bruce Tognazzini, *Design for Usability*, *in* SECURITY AND USABILITY: DESIGNING SECURE SYSTEMS THAT PEOPLE CAN USE, *supra* note 306, at 31, 32 ("Unless you stand over them with a loaded gun, users will disable, evade, or avoid any security system that proves to be too burdensome or bothersome.").

311. Edwards & Brown, *supra* note 143, at 22; *see also* Jay P. Kesan & Rajiv C. Shah, *Setting Software Defaults: Perspectives from Law, Computer Science and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 589–97 (2006) (emphasizing the power of defaults).

312. H. Brian Holland, Visiting Assoc. Professor, Penn. State Univ. Dickinson Sch. of Law, Presentation at the Computers, Freedom and Privacy Conference, New Haven, Conn. (May 21, 2008) (video of a similar presentation of the same material is available at http://www.ethicsandtechnology.eu/index.php/news/comments/privacy_in_social_network_sites_videos_and_slides/).

313. *See* Matthew J. Hodge, Comment, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and MySpace.com*, 31 S. ILL. U. L.J. 95, 106–07 (2006) (discussing whether users have a reasonable expectation of privacy in data revealed to social network sites).

makes sense to ask whether platform operators have too much power over their users.[314]

These are important concerns, but they're orthogonal to the privacy issues detailed above. Even if the government left Facebook completely alone, and Facebook showed no advertisements to its users, and no other company ever had access to Facebook's data, most of the problems we've seen would remain. Amy Polumbo's would-be blackmailer wasn't a government agent or a data miner, just someone in her social network with a little ill will towards her. That's typical of the problems we've seen in this Article: we worry about what our parents, friends, exes, and employers will see, just as much as we worry about what malevolent strangers will see.

In other words, these are peer-produced privacy violations. Yochai Benkler describes peer production as a mode of "information production that is not based on exclusive proprietary claims, not aimed toward sales in a market for either motivation or information, and not organized around property and contract claims to form firms or market exchanges."[315] That's a fair description of Facebook culture: users voluntarily sharing information with each other for diverse reasons, both personal and social. They don't use intellectual property to control Wall posts, they don't buy and sell their social capital (except in jest[316]), and they don't organize themselves hierarchically. Facebook has the essential features of an information commons.

As we've seen, however, when it comes to private information, a genuine commons is the last thing we want. The same sharing-friendly platform, diversely social motivations, and enormous userbase that make Facebook compelling and valuable also make it a privacy nightmare. The privacy violations are bottom-up; they emerge spontaneously from the

---

314. *See, e.g.*, Frank Pasquale, *Internet Nondiscrimination Principles: Commercial Ethics for Carriers and Search Engines*, 2008 U. CHI. LEGAL F. 263 (2008) (claiming that arguments for imposing limits on the exercise of power by network providers also justify imposing limits on the exercise of power by search engines).

315. YOCHAI BENKLER, THE WEALTH OF NETWORKS: HOW SOCIAL PRODUCTION TRANSFORMS MARKETS AND FREEDOM 105 (2006). *See generally* Yochai Benkler, *Siren Songs and Amish Children: Autonomy, Information, and Law*, 76 N.Y.U. L. REV. 23 (2001) (deploying the concept of peer production); Yochai Benkler, *Coase's Penguin, or, Linux and* The Nature of the Firm, 112 YALE L.J. 369 (2002) (discussing peer production at length and in detail).

316. *See, e.g.*, Brian Morrissey, *BK Offers Facebook 'Sacrifice,'* ADWEEK (Jan. 8, 2009), http://www.adweek.com/aw/content_display/news/digital/e3i9953839003c11ce8bbf5f762069ef9ba. The article notes that:

> [Burger King's Whopper Sacrifice Facebook Application] rewards people with a coupon for BK's signature burger when they cull 10 friends. Each time a friend is excommunicated, the application sends a notification to the banished party via Facebook's news feed explaining that the user's love for the unlucky soul is less than his or her zeal for the Whopper.

Id.

natural interactions of users with different tastes, goals, and expectations. The dark side of a peer-to-peer individual-empowering ecology is that it empowers individuals to spread information about each other.

These are not concerns about powerful entities looking down on the network from above; they're concerns about individuals looking at each other from ground level. Even if Facebook were perfectly ethical and completely discreet, users would still create false profiles, snoop on each other, and struggle over the bounds of the private. For this reason, while reports dealing with privacy and other platforms often propose strong restrictions on data collection and transfer, the focus of reports on social-network-site privacy is appropriately elsewhere. [317]

Consider the complaint filed against Facebook under Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA") by a student clinic at the University of Ottawa.[318] While the clinic certainly knows how to draft hard-hitting complaints that object to data collection or transfers to third parties,[319] its Facebook complaint focuses instead on improving Facebook's disclosure of its practices to its users and on enabling users who wish to quit Facebook to remove their information from it.[320] European reports from the International Working Group on Data Protection in Telecommunications ("IWGDPT")[321] and the European

317. *See, e.g.*, Letter from Peter Schaar, Chairman, Article 29 Data Protection Working Party, to Peter Fleischer, Privacy Counsel, Google (May 16, 2007), http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_google_16_05_07_en.pdf (expressing concern over the length of time that Google retains query logs); Complaint at 10–11, *In re* Google, Inc. & DoubleClick, Inc., FTC File No. 071-0170 (Apr. 20, 2007), http://epic.org/privacy/ftc/google/epic_complaint.pdf (requesting an injunction to prevent data transfers between Google and DoubleClick as part of proposed merger).

318. PIPEDA Facebook Complaint, *supra* note 290. PIPEDA fits squarely within the usual framework for thinking about the privacy obligations owed by platform operators to users: a collection of principles known as the Fair Information Practices. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973). Although the FTC and state attorneys general sometimes target companies that egregiously misrepresent their privacy practices to users, they're not part of U.S. statutory law. *See* Ciocchetti, *supra* note 270, at 72–98 (describing the current U.S. privacy-practices enforcement framework). Internationally, they've been more popular: for example, the European Union's Data Protection Directive seeks to protect individuals from nonconsensual data collection. Council Directive 95/46/EC art. 1, 1995 O.J. (L 281) 31, 38.

319. *See, e.g.*, Letter from Philippa Lawson, Dir., Can. Internet Policy & Pub. Interest Clinic, to Comm'r Stoddart, Privacy Comm'n of Can. 3–7 (Nov. 17, 2005), http://www.cippic.ca/documents/privacy/Ticketmaster-OPCCletter.pdf (objecting under PIPEDA to unconsented marketing and transfer of customer information to Ticketmaster affiliates).

320. *See* PIPEDA Facebook Complaint, *supra* note 290, at 11–32.

321. INT'L WORKING GROUP ON DATA PROT. IN TELECOMM., REPORT AND GUIDANCE ON PRIVACY IN SOCIAL NETWORK SERVICES (2008), http://www.datenschutz-berlin.de/attachments/461/WP_social_network_services.pdf [hereinafter IWGDPT REPORT].

Network and Information Security Agency ("ENISA")[322] similarly focus on improving communications with users rather than on stronger restrictions on data collection and transfer.

The reason that these privacy advocates are reluctant to apply restrictions on data transfer too rigorously is that if they did, it could kill off social network sites completely, baby and bathwater together. As the IWGDPT report acknowledges, "[M]ost of the personal information published in social network services is being published at the initiative of users and based on their consent."[323] Social network sites that couldn't collect or distribute personal information couldn't function—and users would be frustrated, rather than relieved. Commercial data-collection rules are inappropriate because they treat the problem as commercial, not social.

E. USE RESTRICTIONS

Our next bad idea comes out of the moral panic over online sexual predators.[324] Social network sites, like chat rooms before them, are seen as a place where "predators" find children and lure them into abusive sexual relationships.[325] While recent studies show that these fears are substantially overblown,[326] some children do in fact meet their abusers through social network sites.[327]

Unfortunately, some legislators and attorneys general think that the solution is to severely limit access to social network sites. The Deleting Online Predators Act of 2006 ("DOPA") passed in the House during the 109th Congress but died in the Senate in committee.[328] The Act would have required libraries and schools to install Internet filters on computers to

322. EUR. NETWORK & INFO. SEC. AGENCY, SECURITY ISSUES AND RECOMMENDATIONS FOR ONLINE SOCIAL NETWORKS (2007), http://www.enisa.europa.eu/doc/pdf/deliverables/enisa_pp_social_networks.pdf.

323. IWGDPT REPORT, *supra* note 321, at 1.

324. *See* Patricia Sanchez Abril, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 73–78 (2007) (attributing the fears of sexual predators on social network sites to a generation gap).

325. *See, e.g.*, Julie Rawe, *How Safe Is MySpace?*, TIME, July 3, 2006, at 34.

326. *See* Janis Wolak et al., *Online "Predators" and Their Victims: Myths, Realities, and Implications for Prevention and Treatment*, 63 AM. PSYCHOLOGIST 111 *passim* (2008) (summarizing the conclusions of multiple surveys). The authors concluded that most victims know they are dealing with adults, *id.* at 112, that most victims go to face-to-face encounters expecting sexual activity, *id.* at 113, that Internet-initiated contacts were responsible for about seven percent of statutory rapes, *id.* at 115, that putting personal information online was not a predictor of receiving sexual solicitations, *id.* at 117, that social-network-site usage was not associated with increased risk, *id.*, and that claims of increased sexual offenses due to the Internet "remain speculations as yet unsupported by research findings," *id.* at 120.

327. *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413, 416 (5th Cir. 2008) (dismissing claims against MySpace arising out of a sexual assault committed by a nineteen-year-old who first contacted his fourteen-year-old victim via her MySpace profile).

328. H.R. 5319, 109th Cong. (2006). Versions were reintroduced in the Senate and House in the 110th Congress and died. S. 49, 110th Cong. (2007); H.R. 1120, 110th Cong. (2007).

block access to "commercial social networking website[s]."[329] Under the list of factors that the Federal Communications Commission would have been required to use in defining that term, essentially all social network sites would have been covered.[330]

Other proposals go even farther. DOPA would have only applied to libraries receiving federal E-Rate funding and would have allowed librarians to enable social-network-site access upon patron request. An Illinois bill would have dropped both of those limits.[331] Bills in Georgia[332] and North Carolina,[333] along with a broad coalition of state attorneys general, would have threatened social network sites with legal action for not preventing minors from signing up.[334] (For now, the states' agreements with both MySpace[335] and Facebook[336] stop short of keeping kids off the sites.[337])

The first problem with trying to keep people (especially teens) off of social network sites is that it doesn't work. Friendster originally didn't allow users under eighteen to sign up, but that didn't stop users under eighteen

---

329. H.R. 1120, § 3(a).

330. *Id.* § 3(c). Commentators have observed that the definition—and similar ones offered in similar state bills—could encompass not just MySpace but also Wikipedia and many other websites with social network features. *See, e.g.*, Adam Thierer, *Would Your Favorite Website Be Banned By DOPA?*, TECH. LIBERATION FRONT (Mar. 10, 2007), http://techliberation.com/2007/03/10/would-your-favorite-website-be-banned-by-dopa/ (listing websites that DOPA would affect, including USAToday.com, CBS Sportsline, and many others).

331. S.B. 1682, 95th Gen. Assem. (Ill. 2007).

332. S.B. 59, 149th Gen. Assem., Reg. Sess. (Ga. 2007).

333. S.B. 132, 2007 Gen. Assem., Reg. Sess. (N.C. 2007). The bill did eventually pass but was amended to eliminate provisions that created liability for allowing minors to sign up for social network sites.

334. *See* Jennifer Medina, *States Ponder Laws to Keep Web Predators from Children*, N.Y. TIMES, May 6, 2007, § 1, at 37 (reporting that many states are pushing through legislation aimed at protecting children by imposing age verification requirements).

335. Press Release, Roy Cooper, N.C. Attorney Gen., AG Cooper Announces Landmark Agreement to Protect Kids Online (Jan. 14, 2008), http://www.ncdoj.com/DocumentStreamerClient?directory=PressReleases/&file=AG%20Cooper%20MySpace%20agreement.pdf.

336. Joint Statement on Key Principles of Social Networking Sites Safety (May 8, 2008), http://www.nj.gov/oag/newsreleases08/Facebook-Joint-Statement.pdf.

337. The "voluntary" steps that MySpace has agreed to take in trying to keep convicted sex offenders off the site are themselves worrisome from a privacy point of view. The site checks its membership rolls against a database of known sex offenders and deletes their accounts. *See* Story & Stone, *supra* note 52. It also gave their names and addresses to the attorneys general. *Id.* These broad restrictions—as enforced by MySpace with minimal due process protections for the individuals whose profiles are removed—are part and parcel of the increasingly comprehensive surveillance now being directed at sex offenders. *See* Patricia A. Powers, Note, *Making a Spectacle of Panopticism: A Theoretical Evaluation of Sex Offender Registration and Notification*, 38 NEW ENG. L. REV. 1049, 1057–58 (2004). They also sweep up many people who are not significant threats to anyone's safety online. *See* Kevin Poulsen, *Banned MySpace Sex Offender: Why Me?*, THREAT LEVEL, http://blog.wired.com/27bstroke6/2007/05/banned_myspace_.html (May 21, 2007) (discussing a registered sex offender's troubles in obtaining a MySpace account even though he claimed to have been clean for nine years with no intent of committing another sex crime).

from signing up by lying about their ages.[338] That shouldn't be surprising. People *want* to use socially compelling technologies, so they'll look for ways to circumvent any obstacles thrown up to stop them. State attorneys general consistently call for social network sites to use age verification technologies, but age verification is no silver bullet either. In its opinion striking down the Communications Decency Act of 1996, the Supreme Court held that there was "no effective way to determine the identity or the age of a user" on the Internet.[339] There still isn't.[340]

The impossibility of keeping teens off social network sites points to a deeper reason why it's a bad idea to try. In danah boyd's words, "[O]nline access provides a whole new social realm for youth."[341] She traces a set of overlapping trends that have pushed teens into age-segregated spaces while simultaneously subjecting them to pervasive adult surveillance and depriving them of agency in roles other than as consumers.[342] For them, social online media provide an essential "networked public": a space in which they can define themselves, explore social roles, and engage publicly.[343] These are compelling social benefits for social-network-site users of all ages.[344] We shouldn't deprive ourselves of these profoundly social technologies.[345]

F. DATA "OWNERSHIP"

Some people think that the biggest problems with social network sites are closure and lock-in.[346] When users can't easily carry their digital identities with them from one site to another, it's much harder for new entrants to compete with an entrenched incumbent.[347] When that happens, users suffer. As Edwards and Brown put it, "Users will put up with a bad deal

338. boyd & Heer, *supra* note 62, § 3.1.

339. Reno v. ACLU, 521 U.S. 844, 855 (1997), *quoting* ACLU v. Reno, 929 F. Supp. 824, 845 (E.D. Pa. 1996).

340. *See* ADAM THIERER, PROGRESS & FREEDOM FOUND., PROGRESS ON POINT RELEASE 14.5, SOCIAL NETWORKING AND AGE VERIFICATION: MANY HARD QUESTIONS; NO EASY SOLUTIONS 3 (2007), http://www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf ("Perfect age verification is a quixotic objective").

341. boyd, *supra* note 86, at 136.

342. *Id.* at 137–38.

343. *Id.*

344. *See generally* MIZUKO ITO ET AL., MACARTHUR FOUND., LIVING AND LEARNING WITH NEW MEDIA: SUMMARY OF FINDINGS FROM THE DIGITAL YOUTH PROJECT (2008), http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf.

345. *See* Anita Ramasastry, *Why the Delete Online Predators Act Won't Delete Predatory Behavior*, FINDLAW, Aug. 7, 2006, http://writ.news.findlaw.com/ramasastry/20060807.html (arguing that DOPA would increase the digital divide).

346. *See, e.g.*, Michael Geist, *Getting Social Network Sites to Socialize*, TORONTO STAR, Aug. 13, 2007 (calling for social-network-site interoperability); Jason Kottke, *Facebook Is the New AOL*, KOTTKE.ORG (June 29, 2007), http://kottke.org/07/06/facebook-is-the-new-aol (calling Facebook a "walled garden").

347. *See* Picker, *supra* note 257, at 15–16.

rather than make the effort of replicating all their personal data and 'friends' connections elsewhere."[348] Some see this "bad deal" as a form of exploitative unpaid labor;[349] others think that the lack of market discipline means that social network sites don't pay enough attention to privacy.[350] Users themselves want a seamless online experience; reentering information from scratch is a big hassle.[351]

These are serious concerns, but far too many people have fallen into the trap of thinking that we should respond by giving users "ownership" over "their" information on a social network site.[352] The ownership frame thinks that the problem is that because Facebook currently "owns" all user data, it can squelch user attempts to leave.[353] Thus, goes the argument, users should "own" their personal information—retaining the rights to export the information, delete it from Facebook, and feed it into one of Facebook's competitors. Unfortunately, while user data ownership might help with the competitive lock-in problem, the privacy consequences would be disastrous. Think of it this way: If you and I are contacts, is that fact your personal information or mine? Giving me the "ownership" to take what I know about you with me to another site violates your privacy.

Consider the story of Plaxo's screen-scraper.[354] Plaxo, a contacts manager with strong social network features, encouraged Facebook users to change horses midstream by providing a tool for users to import their piece of the social graph from Facebook into Plaxo. The tool worked by loading Facebook profiles and extracting the relevant information from them directly. Blogger Robert Scoble tried it out and promptly had his account banned for violating Facebook's terms of service.[355]

---

348. Edwards & Brown, *supra* note 143, at 23.

349. *See* Trebor Scholz, *What the MySpace Generation Should Know About Working for Free*, COLLECTIVATE.NET, Apr. 3, 2007, http://www.collectivate.net/journalisms/2007/4/3/what-the-myspace-generation-should-know-about-working-for-free.html.

350. *See* Ruben Rodrigues, *You've Been Poked: Privacy in the Era of Facebook*, SCITECH LAW., Summer 2008, at 18–19.

351. *See* Erica Naone, *Who Owns Your Friends?*, TECH. REV., July–Aug. 2008, https://www.technologyreview.com/Infotech/20920/ ("huge burden").

352. *See, e.g.*, John Battelle, *It's Time for Services on the Web to Compete on More Than Data*, SEARCHBLOG, http://battellemedia.com/archives/004189.php (Jan. 4, 2008) ("Imagine a world where my identity and my social graph is truly *mine*, and is represented in a machine readable manner."). Many people use ownership rhetoric uncritically, even though the nature of the property allegedly to be "owned" is unclear. *E.g.*, Josh Quittner, *Who Owns Your Address Book?*, FORTUNE, Feb. 12, 2008, http://money.cnn.com/2008/02/11/technology/quittner_address.fortune/index.htm ("My contacts should belong to me.") Does that mean that Quittner's contacts also own him?

353. *See* Joseph Smarr et al., *A Bill of Rights for Users of the Social Web*, OPEN SOCIAL WEB, http://opensocialweb.org/2007/09/05/bill-of-rights/ (Sept. 5, 2007) (listing "ownership" as one of three "fundamental rights").

354. *See* Naone, *supra* note 351.

355. Specifically, the Plaxo tool gathered email addresses, which Facebook users can put on their profile pages, but which aren't exposed through Facebook's public API. *See* Michael

Facebook's decision makes sense from a privacy perspective.[356] If you agreed to be Scoble's contact on Facebook, you had Facebook's privacy rules in mind. You may have tweaked your Facebook account settings to limit access, relied on Facebook's enforcement of community norms, and presented yourself in ways that make sense in the social context of Facebook. You probably didn't have in mind being Scoble's contact on Plaxo. If he can unilaterally export his piece of the social graph from Facebook to Plaxo, he can override your graph-based privacy settings, end-run Facebook's social norms, and rip your identity out of the context you crafted it for. In other words, Robert Scoble's screen scraper is an insult to thousands of people's contextual privacy expectations.

Thus, while data portability may reduce vertical power imbalances between users and social network sites, it creates horizontal privacy trouble. Everyone who has access to "portable" information on social network site *A* is now empowered to move that information to social network site *B*. In the process, they can strip the information of whatever legal, technical, or social constraints applied to it in social network site *A*. Perhaps social network site *B* has similar restrictions, but it need not. Unless we're prepared to dictate the feature set that every social network site must have, mandatory data-portability rules create a privacy race to the bottom for any information subject to them.

For this reason, we should also be extremely cautious about technical infrastructures for social network portability, like Google's OpenSocial,[357] and APIs from MySpace[358] and Facebook.[359] Personal information is only as secure as the least secure link in the chain through which such information passes. One study found that ninety percent of Facebook Applications requested access to more personal information than they needed.[360] A bug in data portability between MySpace and Yahoo! exposed Paris Hilton's and Lindsay Lohan's "private" MySpace pages to anyone with a Yahoo! account, complete with plenty of photos.[361] As social-network-site data becomes more

---

Arrington, *Plaxo Flubs It*, TECHCRUNCH (Jan. 3, 2008), http://www.techcrunch.com/2008/01/03/plaxo-flubs-it/.

356. Juan Carlos Perez, *Facebook Privacy Chief: Data Portability Dangers Overlooked*, INFOWORLD (Feb. 8, 2008), http://www.infoworld.com/article/08/02/08/Facebook-privacy-chief-Data-portability-dangers-overlooked_1.html.

357. *OpenSocial*, GOOGLE CODE, http://code.google.com/apis/opensocial/.

358. *Data Availability*, MYSPACE DEVELOPER PLATFORM, http://developer.myspace.com/community/myspace/dataavailability.aspx.

359. *Facebook Connect*, FACEBOOK DEVELOPERS, http://developers.facebook.com/connect.php.

360. Adrienne Felt & David Evans, *Privacy Protection for Social Networking APIs* § 4.1, http://www.cs.virginia.edu/felt/privacybyproxy.pdf.

361. *See* Owen Thomas, *Paris Hilton, Lindsay Lohan Private Pics Exposed by Yahoo Hack*, VALLEYWAG (June 3, 2008), http://valleywag.com/5012543/paris-hilton-lindsay-lohan-private-pics-exposed-by-yahoo-hack.

portable, it also becomes less secure—and thus less private. The supposedly privacy-promoting solution so badly misunderstands the social nature of relationships on social network sites that it destroys the privacy it means to save.

* * *

The strategies detailed in this Part fail because they don't engage with Facebook's social dynamics. People have compelling social reasons to use Facebook, and those same social factors lead them to badly misunderstand the privacy risks involved. "Solutions" that treat Facebook as a rogue actor that must be restrained from sharing personal information miss the point that people use Facebook *because* it lets them share personal information.

IV. WHAT WILL (SOMETIMES) WORK

Recognizing that Facebook's users are highly engaged but often confused about privacy risks suggests turning the problem around. Instead of focusing on Facebook—trying to dictate when, how, and with whom it shares personal information—we should focus on the users. It's their decisions to upload information about themselves that set the trouble in motion. The smaller we can make the gap between the privacy they expect and the privacy they get, the fewer bad calls they'll make.

This prescription is not a panacea. Some people walk knowingly into likely privacy trouble. Others make bad decisions that are probably beyond the law's power to alter (teens, I'm looking at you). There will always be a need to keep companies from making privacy promises and then deliberately breaking them. Even more importantly, the many cases of interpersonal conflict we've seen can't be fixed simply by setting expectations appropriately. People have different desires—that's the point—and someone's hopes are bound to be dashed.

Still, there are ways that law can incrementally promote privacy on social network sites, and we ought not to let the fact that they're not complete solutions stop us from improving matters where we reasonably can. Some of these suggestions are jobs for law; they ask regulators to restrain social network sites and their users from behaving in privacy-harming ways. Others are pragmatic, ethical advice for social-network-site operators; they can often implement reforms more effectively than law's heavy hand could. They have in common the fact that they take social dynamics seriously.

A. PUBLIC DISCLOSURE TORTS

For legal purposes, there's often a sharp dichotomy between "secret" and "public" information. Courts sometimes seem to believe that once a personal fact is known by even a few people, there's no longer a privacy interest in it. Scholars have sharply criticized this dichotomy, arguing that in everyday life, we rely on social norms and architectural constraints to reveal

information to certain groups while keeping it from others.[362] Lauren Gelman persuasively argues that publicly *accessible* information is often not actually *public*, because it's practically obscure and social norms keep it that way.[363] (She gives the example of a blog by a breast-cancer survivor; she's speaking to a community of other women who've had breast cancer, even if the blog is visible to anyone.[364])

Facebook provides a great illustration of why the secret/public dichotomy is misleading. If I hide my profile from everyone except a close group of contacts, and one of them puts everything from it on a public web page seen by thousands of people, including a stalker I'd been trying to avoid, my faithless contact is the one who made the information "public," not me. The same would be true if Facebook were to make all profiles completely public tomorrow. They weren't secret—they were on Facebook, after all—but they were still often effectively private.

Lior Strahilevitz's social-networks theory of privacy provides a better middle ground.[365] He draws on the sociological and mathematical study of networks to show that some information is likely to spread widely throughout a social network and other information is not. He invites courts to look at the actual structure of real social networks and the structure of information flow in them to decide whether information would have become widely known, even if a particular defendant hadn't made it so.[366]

Social network sites—where the social network itself is made visible—are a particularly appropriate place for the kind of analysis Strahilevitz recommends. Because six of his proposed factors require examining features of the network itself—e.g. "prevalence of ties and supernodes"—they're substantially easier to evaluate on Facebook than offline.[367] Courts should therefore sometimes have the facts that they need to conclude that a piece of information, while "on Facebook," remained private enough to support a public-disclosure-of-private-facts lawsuit along the lines Strahilevitz suggests.

In particular, while the privacy settings chosen by the original user shouldn't be conclusive, they're good evidence of how the plaintiff thought about the information at issue, and of how broadly it was known and knowable before the defendant spread it around. Where the defendant was a contact and learned the information through Facebook, we might also consider reviving the tort of breach of confidence, as Neil Richards and

362. *See* Nissenbaum, *supra* note 199, at 136–38 (discussing contextual integrity); *see also* DANIEL SOLOVE, THE DIGITAL PERSON 42–44 (2004) (attacking the "secrecy paradigm").

363. Gelman, *supra* note 177.

364. *Id.*

365. Strahilevitz, *supra* note 89, at 921.

366. *Id.* at 973–80.

367. *Id.* at 970–71.

Daniel Solove propose.[368] These torts are not appropriate in all situations—*de minimis non curat lex*—but they're a good legal arrow to have in our quiver for protecting online privacy.

The same idea should apply, but with a difference balance, when it comes to defining reasonable expectations of privacy for Fourth Amendment purposes.[369] The police officer who logged into Facebook and saw that Marc Chiles and Adam Gartner were friends was like an undercover investigator pretending to be a student in the back row of a classroom, and it's eminently reasonable to let the police use information that they gain this way. Similarly, under the third-party doctrine, a Facebook user who makes a fact known only to a small group of contacts has no Fourth Amendment grounds for complaint if one of those contacts reveals the fact to the police.[370] On the other hand, when users make privacy choices using Facebook's technical controls, they're expressing expectations about who will and won't see their information, and society should treat those expectations as reasonable for Fourth Amendment purposes. Thus, when the police get the information by demanding it from Facebook the company (rather than by logging in as users or having someone log in for them), they should be required to present a search warrant. Drawing the line there appropriately recognizes the social construction of users' expectations of privacy.

B. RIGHTS OF PUBLICITY

William McGeveran's point that Beacon and Social Ads appropriate the commercial value of users' identities for marketing purposes bears repeating.[371] We're used to thinking of the right of publicity as a tool used by celebrities to monetize their fame. Beacon and Social Ads do the same thing on a smaller scale; by sticking purchase-triggered ads in News Feeds with users' names and pictures, Facebook turns its users into shills. In one respect, it's a brilliant innovation. If, as David Weinberger asserts, on the Internet everyone is famous to fifteen people,[372] Facebook has found a way to tap into the commercial value of this "Long Tail" of micro-celebrity.

Just as with traditional celebrity endorsements, Facebook should be required to obtain the knowing consent of its users before it can use their personae for advertising. That's not onerous. Users can meaningfully opt into Social Ads on a notification-by-notification basis; it would also be

368. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 156–58 (2007).

369. *See generally* Kerr, *supra* note 154 (discussing the "reasonable expectation" test in Fourth Amendment jurisprudence).

370. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 564–66 (2009) (describing and defending the third-party doctrine).

371. McGeveran, *supra* note 251.

372. DAVID WEINBERGER, SMALL PIECES LOOSELY JOINED 103–04 (2002).

reasonable to let them opt in on a source-by-source basis (e.g., "It's okay to show an ad with my name and picture to my friends whenever I add a Favorite Book available at Amazon"). But consent to the program in general is meaningless; users can't reasonably be asked to predict what new sites and services might become Facebook partners. Even worse is the way that Facebook launched Beacon: on an opt-out basis—with an ineffective opt-out at that. These facts ought to support suits under state right-of-publicity laws.

A related concern is that people invest a lot of time and effort in their Facebook personae; to lose one's profile can be a harsh blow.[373] Facebook has been bad about deleting profiles without warning or explanation.[374] When Brandon Blatcher and his wife asked why their accounts had been deleted, they received the fearsome reply, "Unfortunately, we will not be able to reactivate this account for any reason. This decision is final."[375] Facebook's stated reason for kicking them off—it thought that they'd signed up under false names—is reasonable enough, but its application of that principle to the Blatchers leaves a lot to be desired. Facebook has an ethical obligation to institute better due process safeguards: at the very least, notice and an opportunity to be heard.[376] By allowing users to better direct how their profiles are used commercially, Facebook would further users' interest in shaping their social identities.

C. RELIABLE OPT-OUT

Many expectations about what will happen on a social network site are ambiguous and confused. People who haven't completely thought through the logical consequences of their privacy preferences—and that's pretty much all of us—can be surprised when some of those preferences turn out to be inconsistent. But there is one class of expectations that is reliable enough that the law should draw a simple, bright-line rule to enforce them.

People who have chosen not to be on Facebook at all have made a clear statement of their privacy preferences and deserve to have that choice

373. *See* Baratunde Thurson, *Facebook Follies (Or the Dangers of Investing in Someone Else's Platform)*, GOODCRIMETHINK, http://baratunde.com/blog/archives/2007/08/facebook_follies_or_the_dangers_of_investing_in_someone_elses_platform.html (Aug. 28, 2007) (describing how a comedian who regularly invited fans to follow him on Facebook lost his ability to contact them).

374. *See, e.g.*, Daniel Solove, *Facebook Banishment and Due Process*, CONCURRING OPINIONS, http://www.concurringopinions.com/archives/2008/03/facebook_banish.html (Mar. 3, 2008) (describing the plight of one Facebook user who inexplicably had his profile deleted).

375. *See* Brandon Blatcher, *What the Hell Facebook?*, ASK METAFILTER, http://ask.metafilter.com/99021/What-the-hell-Facebook (Aug. 12, 2008). As the thread recounts, despite the take-no-prisoners tone of this "final" decision, a Facebook protest led to their accounts being reinstated. *Id.*

376. *Cf.* Frank Pasquale, *Rankings, Reductionism, and Responsibility*, 54 CLEV. ST. L. REV. 115, 135–38 (2006) (discussing due process protections for people affected by search-engine-ranking decisions).

honored. Facebook's past missteps illustrate why. Until February 2008, it was nearly impossible to delete one's Facebook account; the data associated with it would remain on Facebook's servers even after a user "deactivated" the account.[377] Facebook figured that some users who left would want to come back and reopen their old accounts, a rationale that doesn't justify trapping those users who really do want to leave for good.[378] Facebook told one blogger that to close his account, he'd need to delete each contact, Wall post, and so on by hand—all 2500 of them.[379] Facebook relented and added a "delete" option,[380] but even that was plagued by bugs at first: some "deleted" profiles were still visible, including contact lists and Applications.[381] Facebook may also have violated this principle by gathering information on people even before they've signed up. For a while in July 2008, Facebook had a drop-down option to show users their "Friends without Facebook profiles."[382] Theories vary as to where Facebook gathered the names, but the most plausible explanation seems to be that it took the names of non-Facebook users from tagged photos. Data suction like this—Facebook can also gather names from current users' address books and instant messenger buddy lists[383]—is worrisome, because non-users have never seen Facebook's privacy policies and have had no reasonable chance to opt out.

By way of contrast, Facebook now gets it mostly right when a user tags a photo of a non-user. It prompts the user to supply the non-user's email address. The email that the non-user then receives from Facebook informing them of the tag offers not just the chance to untag the photo, but also to opt out of future contact from Facebook.[384]

---

377. *See* Maria Aspan, *How Sticky Is Membership on Facebook? Just Try Breaking Free*, N.Y. TIMES, Feb. 11, 2008, at C1.

378. *See* PIPEDA Facebook Complaint, *supra* note 290, at 25–27 (arguing that the lack of a delete option violated PIPEDA).

379. Steven Mansour, *2504 Steps to Closing Your Facebook Account*, STEVENMANSOUR.COM, http://www.stevenmansour.com/writings/2007/jul/23/2342/2504_steps_to_closing_your_facebook_account (July 24, 2007) (describing the author's efforts to close his Facebook account).

380. *See* Maria Aspan, *Quitting Facebook Gets Easier*, N.Y TIMES, Feb. 13, 2008, at C1.

381. *See* Maria Aspan, *After Stumbling, Facebook Finds a Working Eraser*, N.Y. TIMES, Feb. 18, 2008, at C5.

382. *See* Nick O'Neill, *Facebook Starts Recommending Friends Not on Site*, ALLFACEBOOK, http://www.allfacebook.com/2008/07/facebook-starts-recommending-friends-not-on-site/ (July 26, 2008).

383. *Friends*, FACEBOOK, http://www.new.facebook.com/help.php?page=441.

384. This is not to say that the opt-out option is always successful in practice. Facebook's description of the feature would seem to imply that the subject can't untag the photo without signing up for Facebook. In my (admittedly brief) tests, I found that I couldn't even see the photo without signing up for Facebook. Also, query whether this opt-out is prompted by Facebook's CAN-SPAM obligations. *See* 15 U.S.C. § 7704(a)(3)–(5) (Supp. 2004) (requiring commercial e-mails to contain opt-out provisions for consumers).

The correct general rule extends this principle in two ways. First, Facebook should proactively offer this sort of an opt-out to any non-user as soon as it acquires enough information about them to be able to contact them (e.g., an email address or IM screen name);[385] it should also purge from its servers any other information linked with the email address whose owner has opted out. Deliberately staying off of Facebook has an unambiguous social meaning, and Facebook should respect the request.

Lillian Edwards and Ralph Brown's idea of more privacy-preserving default settings also has value in specific clear cases where users are likely to want heightened privacy. I've been told[386] about two different people who ended long-term relationships and wanted to change their Facebook relationship status without notifying the world. Both of them spent a long time poring through Facebook's privacy settings so that it would stay strictly confidential when they made the switch. In both cases, the "*X* changed her relationship status to single" announcement was broadcast to their entire networks. There's no need here to have a larger argument about the usability of Facebook's privacy interface, not when a simpler rule would suffice. Facebook shouldn't send announcements about the *ends* of relationships unless the users explicitly click on a "post this to my News Feed" button. Breakups should be opt-in, not opt-out. Similarly, Facebook currently treats joining a geographical network as permission to share your profile with anyone else in the network. That's a dangerous default: photos of Bono from U2 frolicking with two nineteen-year-olds in bikinis were effectively made public when one of the girls joined the New York network, which has over a million members.[387]

D. PREDICTABILITY

In the Introduction, I made fun of the idea that cars should be declared unreasonably dangerous because people injure themselves ghost riding the whip. But in a more limited way, this idea does have some value. Suppose that the Powell Motors Canyonero unpredictably lurches from side to side about forty seconds after the driver takes his or her foot off the gas pedal. This is a bad product feature by any measure, but it turns ghost riding from a dangerous sport into a positively suicidal one. Since manufacturers are generally strictly (and non-waivably) liable for injuries proximately caused by a defectively designed product, it might make sense to hold Powell Motors

385. *Cf.* PIPEDA Facebook Complaint, supra note 290, at 28–29. CIPPIC argues that Facebook should need permission to obtain non-users' consent when pictures of them are uploaded; the "as soon as contact is possible" principle provides a necessary qualification to that argument.

386. In confidence, for reasons that will become apparent.

387. *See Bono's Bikini Party Photos Exposed by Facebook Privacy Flaw*, SOPHOS, http://www.sophos.com/pressoffice/news/articles/2008/10/bono.html (Oct. 29, 2008).

liable for ghost riding accidents caused by Canyonero lurches.[388] A well-designed product doesn't change what it's doing in unpredictable and dangerous ways.

Facebook, however, changes in unpredictable and privacy-threatening ways with disconcerting frequency. News Feed is the most famous example, an overnight change that instantly made highly salient what had previously been practically obscure. As danah boyd explains, Facebook users were like partygoers who felt "protected by the acoustics" of the loud music at a party.[389] A reasonable voice for talking to a friend over loud music becomes an unreasonable scream when the music stops—and everyone can hear the end of your sentence. Facebook users have since embraced their News Feeds, but the transition was a privacy lurch.

What should the law do about lurches? Users' "consent" to the new patterns of data flow is questionable. There's a strong argument that lurches of this sort constitute a new "use" or "purpose" under privacy schemes like the European Data Protection Directive[390] or the Canadian PIPEDA,[391] for which fresh consent would be required. It's harder to make such an argument under U.S. law, since the lack of a comprehensive information-privacy statute means that Facebook needs no permission in the first place to collect personal information.

An explicit consumer-protection approach is promising. On this way of looking at things, the initial design of the system is a representation to users that information they supply will be used in certain ways; by changing the service in a fundamental, privacy-breaching way, the site also breaches that implicit representation. The FTC action against Sony/BMG for distributing CDs that surreptitiously installed spyware on consumers' computers provides a useful model.[392] There too, consumers were confronted with a product that threatened their privacy by failing to conform to their legitimate expectations about how it would work.[393]

Similar reasoning ought to apply to the rollout of a service like Beacon. There's not much wrong with Beacon as long as everyone involved knows it's there and can turn it off if they want. But Beacon was completely unforeseeable from a user standpoint. There was no precedent for two unrelated websites to realize that they had a user in common and start

388. *See, e.g.*, RESTATEMENT (THIRD) OF TORTS: PRODUCTS LIABILITY § 1 (basic liability); *Id.* § 2 (design defects and foreseeable harm); *Id.* § 10 (failure to warn); *Id.* § 15 (causation); *Id.* § 18 (non-waivability).

389. boyd, *supra* note 35.

390. *See* Edwards & Brown, *supra* note 143, at 14–16.

391. *See* PIPEDA Facebook Complaint, *supra* note 290, at 24.

392. *In re* Sony BMG Music Entm't, No. C-4195, 2007 FTC LEXIS 83 (June 29, 2007).

393. *See generally* Deirdre K. Mulligan & Aaron K. Perzanowski, *The Magnificence of the Disaster: Reconstructing the Sony BMG Rootkit Incident*, 22 BERKELEY TECH. L.J. 1157, 1158–77 (2007).

funneling information from one to a highly visible place on the other. That unannounced design change made both Facebook and its partner sites unreasonably dangerous services.

That Facebook could have done better with News Feed and Beacon is demonstrated by its own actions in rolling out public profiles. It made an announcement several weeks before opening the profiles up to search engines, giving users an opportunity to uncheck the appropriate box. [394] Even so, such a large cultural shift—danah boyd observes that "Facebook differentiated itself by being private" and walled off from the Internet at large[395]—should have been opt-in, rather than opt-out. Moreover, Facebook didn't give its users advance warning about the public profile pages, only about their exposure to search engines, and one blogger has produced evidence suggesting that Facebook may well have made the announcement at least several weeks *after* enabling the public profiles.[396]

Consumer-protection rules are not a cure-all. There's a subtle but crucial difference between a user's "consent" to Beacon and her "consent" to let her employer see photos of her in a drunken stupor. We can save the former from her folly by declaring the consent fictitious and rewriting a contract, but we can't save the latter by meddling with the contract.[397] Facebook would have been perfectly happy to take the photos down if she asked, but she didn't. This is not a case about misleading the consumer. Social lurches, on the other hand, are inherently misleading.

E. NO CHAIN LETTERS

We've seen that social network sites spread virally through real social networks. Once they have spread, they themselves provide a fertile environment for memes and add-ons to spread rapidly through the social network of users. There's an obvious network effect at work; the more users a given site or Application has, the more engaging it is.

There's also an obvious conflict of interest here. For example, Hubert would like Hermes to join him in using HyperPoke, even if Hermes himself wouldn't enjoy it. Under most circumstances, the network effect and the conflict of interest are inseparable; they're both irreducibly social, and the best we can do is to leave it up to Hubert and Hermes to negotiate any

394. Phillip Fung, *Public Search Listings on Facebook*, FACEBOOK BLOG, http://blog.facebook.com/blog.php?post=2963412130 (Sept. 5, 2007).

395. danah boyd, *SNS Visibility Norms (A Response to Scoble)*, APOPHENIA, http://www.zephoria.org/thoughts/archives/2007/09/09/sns_visibility.html (Sept. 9, 2007).

396. Danny Sullivan, *4 Questions and Answers You Should Know About Facebook's Public Search Listings*, SEARCH ENGINE LAND, http://searchengineland.com/070911-103851.php (Sept. 11, 2007).

397. *Cf.* Edwards & Brown, *supra* note 143, at 19 (discussing "online consumer contracts" that courts have declared void or voidable for unconscionability).

tension between themselves. Most of the actual operations of viral word-of-mouth marketing are necessarily beyond regulation, and should be.

Matters may be different, however, when Hubert has an interest in Hermes's participation that goes beyond the pleasure of his company. If Hubert is being *paid* to convince Hermes to sign up, he has an incentive to treat Hermes as an object, rather than as a friend. HyperPoke is subverting the relationship; that's bad for Hermes and for their friendship.[398] There's a particular danger that a social-network-site feature could be "social" in the same way that a multi-level marketing scheme or a chain letter is: by bribing or threatening current users to use every social trick in their book to bring in new ones.[399]

Fortunately, in its role overseeing the Applications it allows to run, Facebook now wisely prohibits "incentivized invites."[400] Before the policy went into effect, Application developers would sometimes reward users for inviting others (e.g., you can use HyperPoke as soon as you join, but your character can't be more than a Level 1 Nudger until you've invited ten other users). Now, an Application may not "[r]equire that users invite, notify, or otherwise communicate with one or more friends to gain access to any feature, information, or portion of the application . . . ."[401]

This is a useful general principle: it's presumptively illegitimate to bribe users to take advantage of their social networks. True, there's a fine line between these "artificial" incentives and the "natural" incentives of inherently social Applications, but Facebook is doing the right thing by banning viral incentives that have no legitimate connection to the Application's actual functionality. Regulators should watch out for the deliberate exploitation of social dynamics and, where appropriate, prohibit such practices.

F. USER-DRIVEN EDUCATION

Education about the privacy risks of Facebook can also help. Although people are always going to make mistakes at the margin and have privacy-affecting disputes with each other, there are some basic facts about how social network sites work that people don't always appreciate. Education can

398. *Cf.* Ellen P. Goodman, *Stealth Marketing and Editorial Integrity*, 85 TEX. L. REV. 83 (2006) (arguing for mandatory sponsorship disclosure of "stealth marketing").

399. *See generally* Sergio Pareja, *Sales Gone Wild: Will the FTC's Business Opportunity Rule Put an End to Pyramid Marketing Schemes?*, 39 MCGEORGE L. REV. 83 (2008) (describing the history and limits of the FTC's efforts to curb abusive business opportunity schemes).

400. *See* Karl Bunyan, *Incentivized Invites No Longer Allowed on the Facebook Platform*, INSIDE FACEBOOK, http://www.insidefacebook.com/2008/08/13/incentivized-invites-no-longer-allowed-by-facebook/ (Aug. 13, 2008).

401. *Platform Policy* § 2.6, FACEBOOK DEVELOPERS WIKI, http://wiki.developers.facebook.com/index.php?title=Platform_Policy&oldid=14244 (July 21, 2008).

help them learn these essentials the easy way, rather than from painful experience.[402]

That education, however, needs to be rooted in the communities it targets. When outsiders try to lecture on the dangers of Facebook, they often end up talking past the groups that they're trying to reach. Education via privacy policy, we've seen, is wholly ineffective. So, too, are dry statements of fact by distant authority figures. Even worse is the "education" that a Cheyenne police officer offered to an assembly of high-school students. He pulled up one student's MySpace page and claimed that he'd shared her information with an imprisoned sexual predator. She ran from the room in tears as the police officer told the students that the predator would now be masturbating to her picture.[403] This wasn't education about privacy violations, this *was* a privacy violation.

An inspirational model of culturally appropriate education comes from the work of anthropologist Dwight Conquergood in the Ban Vinai refugee camp in the mid-1980s.[404] Western doctors in the camp had difficulty explaining the health risks of rabies and poor refuse disposal to Hmong refugees. The Hmong were suspicious of the doctors, whose cultural practices—drawing blood, asking intrusive questions, and demanding that patients undress—clashed with Hmong cultural practices.

Instead of trying to disabuse the Hmong of their cultural assumptions, Conquergood embraced them. He held parades in which allegorical figures drawing on elements of Hmong folklore and costume—such as Mother Clean, a gigantic grinning puppet—explained disease-prevention essentials through song, dance, and proverbs.[405] Conquergood succeeded where the doctors had failed; after a rabies-prevention parade, thousands of refugees brought in dogs for vaccination. Conquergood attributed much of the parades' appeal to the way the Hmong actors improvised and rewrote the messages to make them culturally appropriate.[406]

Cultural appropriateness is particularly important for younger users. On the unfortunate but probably justified assumption that society will not

402. *Compare* Tim O'Reilly, *Social Graph Visibility Akin to Pain Reflex*, O'REILLY RADAR, http://radar.oreilly.com/2008/02/social-graph-visibility-akin-t.html (Feb. 2, 2008) ("It's a lot like the evolutionary value of pain. Search creates feedback loops that allow us to learn from and modify our behavior."), *with* danah boyd, *Just Because We Can, Doesn't Mean We Should*, APOPHENIA, http://www.zephoria.org/thoughts/archives/2008/02/04/just_because_we.html (Feb. 4, 2008) ("I'm not jumping up and down at the idea of being in the camp who dies because the healthy think that infecting society with viruses to see who survives is a good idea.").

403. *See* Hallie Woods & David Persons, *MySpace Lecture Generates Outrage*, FORT COLLINS COLORADOAN, Aug. 21, 2008, at 1A.

404. *See* ANNE FADIMAN, THE SPIRIT CATCHES YOU AND YOU FALL DOWN 32–38 (1998) (describing Conquergood's work).

405. *See* Dwight Conquergood, *Health Theatre in a Hmong Refugee Camp: Performance, Communication, and Culture*, 32 DRAMA REV. 174, 174–203 (1988).

406. *Id.* at 182–84, 203.

become more tolerant of youthful indiscretions any time soon, teens and college students would be better off with a better understanding of the ways that persistent postings can return to haunt them later. Teens are sophisticated (if not always successful) at negotiating boundaries of obscurity with respect to *present* surveillance from their elders; the challenge is to help them be similarly sophisticated in dealing with *future* surveillance.[407] A critical theme of boyd's work, however, is that social network sites are hugely popular with young users because they fit so effectively into the social patterns of teenage and young-adult life.[408] Warnings about the dangers of MySpace will wash right over them unless those warnings resonate with lived experience.

One possible Mother Clean in American society may be student-run college newspapers. The pages of college newspapers have been peppered with editorials and articles explaining how embarrassing photos and profiles are fodder for employers.[409] Indeed, college newspapers were generally on the scene earlier than the mainstream media: the October 2005 expulsion of a Fisher College student for creating a Facebook group targeting a campus security officer was shortly followed by articles about Facebook and privacy in at least a dozen college newspapers.[410] Reaching out to student-newspaper editors may be an effective way of getting appropriate warnings heard by the people who need to hear them.

It could also help in educating regulators themselves. Conquergood explained that the Ban Vinai health workers needed to learn just as much from their patients as vice-versa, stating "The ideal is for the two cultures, refugees' and relief workers', to enter into a productive and mutually invigorating dialog . . . ."[411] For regulators, studying the social dynamics of Facebook is the essential first step in that dialog.

V. CONCLUSION

In his recent book *Here Comes Everybody*, Clay Shirky, the great theorist of online social media, had this to say about blog audiences:

> [W]hy would anyone put such drivel out in public?
>
> It's simple. They're not talking to you.
>
> We misread these seemingly inane posts because we're so unused to seeing written material in public that isn't intended for us. The people posting messages to one another in small groups are doing

407. boyd, *supra* note 86, at 131–34.

408. *See generally id.*

409. *See, e.g.*, Jilian Gundling, *Facebook: The Facetime That Can Lose You a Job*, DARTMOUTH, http://thedartmouth.com/2007/11/02/arts/jobsandfacebook/ (Nov. 2, 2007).

410. *See* Jones & Soltren, *supra* note 284, at 30 (describing the incident at Fisher College and the "explosion" of cautionary articles that followed).

411. Conquergood, *supra* note 405, at 202.

> a different kind of communicating than people posting messages for hundreds or thousands of people to read.[412]

This short passage captures everything that makes it hard to set sensible policy for new social media. Their norms are surprising. Their messages are heavily context-dependent. Their users think socially, not logically. It's easy for outsiders to misunderstand what's really going on.

This may sound like a pessimistic message, but it isn't. The deeper point of *Here Comes Everybody* is that new online media and the social networks that coalesce around them are comprehensible, that there is an underlying social logic to how they work. Policymakers who are willing to take the time to understand those social dynamics will find their efforts rewarded.

This Article has confirmed the essential truth of Shirky's lesson by applying it to Facebook and other social network sites. We've seen that the same three social imperatives—identity, relationships, and community—recur again and again on these sites. Users want and need to socialize, and they act in privacy-risking ways because of it. We cannot and should not beat these social urges out of people; we cannot and should not stop people from acting on them. We can and should help them understand the consequences of their socializing, make available safer ways to do it, and protect them from sociality hijackers. There are better and worse ways to do these things, and this Article has attempted to start a conversation about what those ways are.

Ultimately, this is a story about *people doing things together*, which really means it's a story about *people*. New technologies matter when they change the dynamics of how people do things together; the challenge for technology law is always to adapt itself to these changing dynamics. Laws are made for people, and we lose sight of that fact at our peril. Social networking, like ghost riding the whip, can be a dangerous activity; if we wish to address that danger, our inquiry must start with the people engaged in it. This is their story, the story of people taking a technology and making it their own. As Shirky wrote over a decade ago, "[t]he human condition infects everything it touches."[413]

412. CLAY SHIRKY, HERE COMES EVERYBODY 85 (2008).

413. CLAY SHIRKY, VOICES FROM THE NET, at xi (1995).