LOSING FACE:

AN ENVIRONMENTAL ANALYSIS OF PRIVACY ON FACEBOOK

Chris Peterson—Draft—January 2010

This Article contributes to the ongoing conversation about privacy on social network sites. Adopting Facebook as its primary example, it reviews behavioral data and case studies of privacy problems in an attempt to understand user experiences. The Article fills a crucial gap in the literature by conducting the first extensive analysis of the informational and decisional environment of Facebook. Privacy and the environment are inextricably linked: the practice of the former depends upon the dynamics and heuristics of the latter.

The Article argues that there is an environmental element to the Facebook privacy problem. Data flow differently on Facebook than in the physical world, and the architectural heuristics of privacy are absent or misleading. This counterintuitive informational environment waylays privacy practices, opens a gulf between expectation and outcome, causes a crisis in self-presentation, and facilitates what Professor Helen Nissenbaum calls a loss of contextual integrity.

The Article explores possible interventions. It explains how regulatory solutions and market forces are themselves hindered by the the deficient privacy environment of Facebook and can't solve all of its problems. This Article recommends renovating the design of Facebook to privilege privacy practices and proposes specific interventions drawn from the computer science and behavioral economics literature. It concludes with a message of cautious optimism for the emerging coalition of engineers, academics, and practitioners who care about privacy on networked publics.

TABLE OF CONTENTS

INTRODUCTION

A. EVERYBODY AND THEIR GRANDMOTHER

On April 12, 2009, a college student named Rachel broadcast a distress signal out into the electronic ether. "my grandmother just friend requested me," her Facebook status read.[1] "no. Facebook, you have gone too far!"[2]

It's not intuitively obvious why such a simple request should bother Rachel so much. After all, Rachel and her grandmother are very close. She trusts her grandmother. She confides in her grandmother. She tells her grandmother "private" things. She is certainly closer to her grandmother than to many of her Facebook "Friends." So what's the big deal?

Rachel explains:

> Facebook started off as basically an online directory of COLLEGE STUDENTS. I couldn't wait until I had my college email so that I could set up an account of my own, since no other emails would give you access to the site. Now, that was great. One could [meet] classmates online or stay in touch with high school mates [but it] has become a place, no longer for college students, but for anyone. [About] five days ago, the worst possible facebook scenario occurred, so bizarre that it hadn't even crossed my mind as possible. MY GRANDMOTHER!? How did she get onto facebook?. . . As my mouse hovered between the accept and decline button, images flashed through my mind of sweet Grandma [seeing] me drinking from an ice luge, tossing ping pong balls into solo cups full of beer, and countless pictures of drunken laughter, eyes half closed. Disgraceful, I know, but these are good memories to me. To her, the picture of my perfectly angelic self, studying hard away at school, would be shattered forever. [3]

Rachel isn't the only person facing privacy problems on Facebook. Some members of the popular social networking site have been shamed,[4] expelled,[5] fired,[6] and even arrested[7] because of content posted by them or their "Friends" to the site. Many more have, like Rachel, experienced less dramatic but nevertheless uncomfortable social tensions.

The most obvious and interesting question to ask here is *why*. Why do these privacy problems occur? Why do members of Facebook regularly share such sensitive information with so many people? Why do they routinely underestimate the breadth of their disclosure and so poorly assess the risk involved?

---

1 A "Friend Request" is an electronic invitation whereby one user asks to form a Facebook "Friendship" with another. A "Friendship" is a mutual and bidirectional relationship that is both performative (as a way to demonstrate social ties) and prescriptive (as it affects what information is shared between which users).

2 Rachel is not this student's real name. Facebook status update by "Rachel", FACEBOOK (March 24, 2009) on file with the author.

3 Facebook message from "Rachel" to Chris Peterson, FACEBOOK (March 24, 2009) on file with the author.

4 Andrew Levy, *The Ladettes Who Glorify Their Shameful Drunken Antics on Facebook*, MAIL ONLINE, November 5, 2007, http://www.dailymail.co.uk/news/article-491668/The-ladettes-glorify-shameful-drunken-antics-Facebook.html

5 Sarah Schweitzer, *Fisher College Expels Student Over Website Entries,* BOSTON.COM LOCAL NEWS, October 6, 2005, http://www.boston.com/news/local/articles/2005/10/06/fisher_college_expels_student_over_website_entries/.

6 *Facebook Remark Teenager Is Fired*, BBC NEWS, February 27, 2009, http://news.bbc.co.uk/2/hi/uk_news/england/essex/7914415.stm.

7 Jodi S. Cohen, *Cop Snares College Pals in Own Web*, CHI. TRIB., Aug. 3, 2006, at C1. Originally cited by James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137 (2009) at 1164-1165.

Some have argued that users of social network sites are exhibitionists who just don't *care* about privacy.[8] This viewpoint is completely contradicted by behavioral data[9] and ethnographic accounts.[10] Members of social network sites, as a rule, worry terribly about unwanted exposure. Any argument predicated on the presumption that users "just don't care" about privacy is counterfactual to its core: it is orthogonal to the way people actually think and behave on social network sites.

Other analyses that engage these social dynamics[11] provide more convincing explanations. Professor James Grimmelmann compellingly argues that users "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."[12] In his "Saving Facebook", Grimmelmann presents an exhaustive account of the social dynamics of Facebook, explains how these practices and norms give rise to privacy problems, and describes a number of policy interventions that mesh with, rather than grate against, the social milieu of Facebook.[13]

Grimmelmann's is far and away the best analysis of privacy on Facebook in the legal literature. It lays the groundwork of an emerging conceptual framework that explains privacy in networked publics. It continues an ongoing discussion among jurists, behavioral scientists, and engineers about privacy problems on social network sites.

This Article contributes to this conversation by exploring a critical, complementary, and largely neglected part of the problem: the *environment* of Facebook. Any study of privacy that does not engage the environment within which individuals practice privacy is conceptually incomplete. Privacy and the environment are inextricably linked: the practices of the former interact with the dynamics and heuristics of the latter. As the social psychologist Irwin Altman explained in *The Environment and Social Behavior*:

> Environment and behavior are closely intertwined, almost to the point of being inseparable. Their inseparability says more than the traditional dictum that "environment affects behavior." It also states that behavior cannot be understood independent of its intrinsic relationship to the environment and that the very definition of behavior must be within an environmental context. . . What is now called for [is] recognition that the appropriate unit of study is a people-environment unit.[14]

In other words, privacy is mutually constituted by the individual and her environment. They are inextricably interdependent variables. That is why environmental analyses are so important: the physical world and Facebook have extremely different information architectures and so are *necessarily* different when it comes to practicing privacy. To that end, this Article conducts a complementary and comprehensive analysis of the privacy environment of Facebook, provides a conceptual framework for understanding how its information architecture impacts user privacy practices, and describes various interventions by markets, law, or code and why they are likely or unlikely to help.

B. THE ARTICLE: FOCUS, TERMS AND SCOPE

---

8 Robert J. Samuelson, *A Web of Exhibitionists,* WASH. POST, September 20, 2006, http://www.washingtonpost.com/wp-dyn/content/article/2006/09/19/AR2006091901439.html.

9 *See generally* Alessandro Acquisti & Ralph Gross, *Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook*, PRIVACY-ENHANCING TECH.: 6TH INT'L WORKSHOP 36 (George Danezis & Philippe Golle eds. 2006), http://privacy.cs.cmu.edu/dataprivacy/projects/facebook/facebook2.pdf.

10 *See generally* boyd, Taken Out Of Context: American Teen Sociality In Networked Publics (Fall 2008) (unpublished Ph.D. dissertation, University of California-Berkeley, School of Information), http://www.danah.org/papers/TakenOutOfContext.pdf.

11 I borrow this term from James Grimmelmann. *See generally* Grimmelmann, *Saving Facebook*, *supra* note __.

12 Grimmelmann, *Saving Facebook*, *supra* note __, at 1160.

13 Grimmelmann, *Saving Facebook*, *supra* note __, at 1195-1202.

14 IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR 205 (Wadsworth Publishing Company, 1975). Originally cited in Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, BULLETIN OF SCIENCE, TECHNOLOGY & SOCIETY,Vol. 28, No. 1, p. 20-36, (2008).

This Article adopts Facebook as its primary case study. At the time of writing Facebook is the world's largest social network site.[15] It is also one of the most active, with over half of the site's 300 million users logging on at least once a day.[16] While certain aspects of this analysis must necessarily be limited by and to the specificities of Facebook's design, the central thesis of this Article—that design and privacy are interrelated—broadly applies to social network sites as a class. Facebook is merely an illustrative (and certainly neither comprehensive nor exhaustive) example.

When I say "environment" I generally mean the properties and structure of a space, specifically those that affect user decisions, practices, and risk assessments within it. I also occasionally refer to this as "architecture" or use the two words interchangeably. However, when I speak of architecture in this Article I am almost never referencing Lessig's definition of architecture as a modality of regulation[17] but rather invoking Thaler and Sunstein's metaphor for the "[organization] of the context in which people make decisions."[18]

I distinguish between the two not to dispute the Lessigian thesis but rather to clarify my argument. Lessig's idea that "code is law"[19]—or, more precisely, that "code does the work of law, but does it in an architectural way"[20]—explains one way in which the design of a digital space affects human behavior within that space. No doubt there is an element of what Lessig would call "objective constraint"[21] in the privacy controls (or lack thereof) of Facebook, because, hackers aside, users may only do what they have been allowed to do by the site's designers. However, this Article is less concerned with these objective constraints than in the broader question of how users interact with Facebook, how its design frames their expectations and guides their behavior, and to what extent its informational properties concord with their norms.

This is not, I should also stress, an argument from technological determinism. This Article does not contend that the technology of Facebook *controls* the social practices of its users. Indeed, users often repurpose certain aspects of Facebook's design for wholly unexpected social purposes.[22] Instead, this Article analyzes the emerging ecology of privacy on Facebook by examining the interdependent effects of its design and the practices of its occupants.

I'll also use "friend" or "friendship" as distinct from "Friend" or "Friendship." The former refers to social relations in the physical world; the latter, to those relations articulated within Facebook. Part III.C will explain that though these two groups often overlap, they are very different social categories: as danah boyd[23] has written, "it's not to anyone's advantage to assume that the rules of friendship apply to Friendship."[24]

The structure of the Article is as follows:

Part II sketches the social dynamics of Facebook. It tracks the transformation of Facebook from a small and culturally homogenous college community to an enormous and culturally heterogenous global network. It then draws upon behavioral and ethnographic data to explain how people use social network sites. Part II concludes by reviewing several case studies of privacy violations on Facebook.

---

15 Erick Schonfeld, *Facebook Is Not Only The World's Largest Social Network, It Is Also The Fastest Growing*, TECHCRUNCH, August 12, 2008, http://www.techcrunch.com/2008/08/12/facebook-is-not-only-the-worlds-largest-social-network-it-is-also-the-fastest-growing/.

16 *Facebook | Factsheet,* FACEBOOK, http://www.facebook.com/press/info.php?factsheet.

17 Lawrence Lessig, *The New Chicago School,* 26 J. LEGAL. STUD. 661, 663; *available at* http://www.lessig.org/content/articles/works/LessigNewchicschool.pdf. *see also* LAWRENCE LESSIG, CODE: VERSION 2.0 340 (Basic Books, 2006); available at http://pdf.codev2.cc/Lessig-Codev2.pdf.

18 *See* RICHARD THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS 8 (Yale University Press, 2008) (definition of a "choice architect").

19 *See generally* Lessig, Code, supra note __

20 James Grimmelmann, Note, *Regulation by Software,* 114 YALE L.J. 1719, 1721; available at http://www.yalelawjournal.org/pdf/114-7/Grimmelmann.pdf.

21 Lessig, *Chicago* and CODE, *supra* note ___.

22 *See, e.g.,* boyd, Taken Out of Context, *supra* note __, at 147; Grimmelmann, *Saving Facebook*, *supra* note __, at 1152.

23 danah boyd does not capitalize her name. *See* danah boyd, *What's in a Name?*, DANAH.ORG, http://www.danah.org/name.html.

24 *See* danah boyd, *Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama*, DANAH.ORG, September 8, 2006, http://www.danah.org/papers/FacebookAndPrivacy.html.

Part III adopts Professor Helen Nissenbaum's theory of privacy as contextual integrity. It explains why contextual integrity is a useful way to think about privacy problems on Facebook. It describes how the norms of contextual integrity relate to the informational properties of an environment and identifies ways in which the informational properties of Facebook's environment differ greatly from that of the physical world. It concludes by inspecting three counterfactual and counterintuitive "technological fictions" of Facebook—Flat Friendship, Invisible Audiences, and Strange Disclosure Defaults—and describing how each contributes to the collapse of contextual integrity.

Part IV discusses what might be done. It incorporates insights from behavioral economics to explain why markets won't fix the problem. It recommends some helpful legal interventions but also outlines areas in which law is bound to fall short. Part IV concludes by demonstrating how code—in the guise of thoughtful, intentional design—may be the most powerful tool for reconstructing contexts.

Part V suggests solutions. It offers a set of technological tweaks that would empower users to practice privacy. It draws upon research in computer science to offer general design principles to which context-conscious developers should adhere. It concludes with a message of cautious optimism to the emerging community of jurists, behavioral scientists, and engineers thinking about privacy in networked publics.

II. FACEBOOK AND SOCIAL BEHAVIOR

A. A BRIEF HISTORY OF FACEBOOK

Finding Hotties at Harvard, Keeping Friends at College

In 2003 a Harvard freshman, his advanced spurned by cute classmate, sulked and schemed alone in his room. This is a familiar college story—it happens all the time. Rarely does such a situation amount to more than an intemperate drunk dial and a nasty hangover. In this case, however, it led to the creation of the largest social network site in the world.

That night, this romantic rejection inspired Mark Zuckerberg to compare "hot" Harvard students by creating an online version of his dorm's "Facebook," a print directory of student pictures and interests designed to help new students meet each other.[25] Zuckerberg hacked into the university's servers, downloaded photos of his classmates, and uploaded them to a site called FaceMash.com, where students could vote to decide which classmate was cutest. The site registered over 22,000 views in a matter of hours before school officials shut it down. Zuckerberg was reprimanded for violating student privacy and sent back to his room where he continued to code.[26]

In February 2004, Zuckerberg launched thefacebook.com. The site, which Zuckerberg claimed to have coded in a week,[27] was very simple: students with Harvard email addresses could upload a profile photo, their course schedule, and a list of their personal interests.[28] Perhaps still smarting from his reprimand in the fall—or preternaturally wary of bad publicity—Zuckerberg tried to forestall fears about unwanted exposure:

> There are pretty intensive privacy options," [Zuckerberg] said. "You can limit who can see your information, if you only want current students to see your information, or people in your year, in your house, in your classes. You can limit a search so that only a friend or a

25 Claire Hoffman, *The Battle for Facebook*, ROLLING STONE, June 26, 2008, available at http://www.rollingstone.com/news/story/21129674/the_battle_for_facebook.

26 *See* Katherine Kaplan, *FaceMash Creator Survives Ad Board,* HARVARD CRIMSON, November 19, 2003, http://www.thecrimson.com/article.aspx?ref=350143.

27 This has become a point of contention. As Hoffman describes *supra* note __, Zuckerberg was later sued by a few other students who claimed they had hired him to produce a social network site for them, and that he had stolen the code for that site and used it to launch thefacebook.com. Zuckerberg's former business partners later settled for $65 million. *Facebook settled for 65 million: ConnectU law firm*, THE AGE, February 12, 2009, http://news.theage.com.au/breaking-news-technology/facebook-settled-for-65-million-connectu-law-firm-20090212-85i5.html.

28 Alan Tabak, *Hundreds Register for New Facebook Website*, HARVARD CRIMSON, February 9, 2004, http://www.thecrimson.com/article.aspx?ref=357292.

> friend of a friend can look you up. People have very good control over who can see their information.[29]

Facebook was an instant success. Over a thousand students registered within the first week.[30] In March 2004, Facebook extended its service to other Ivy League schools, although it did not initially allow students at different campuses to Friend each other. The site continued to add functionality, including the ability to create and join Groups and to comment on another person's profile using the Wall.[31] By December 2004, the site boasted over one million users across all of its networks. In keeping with subversive nerd chic, Zuckerberg listed his job description as "Founder, Master and Commander [and] Enemy of the State" on Facebook.[32]

The site continued to grow throughout 2005. Zuckerberg and his cofounders took a leave of absence from Harvard and relocated to Palo Alto. They moved in with Sean Parker, a cofounder of Napster, who escorted Zuckerberg around the venture capital circuit.[33] The site raised over $12 million in initial seed money as colleges continued to be added to the network one-by-one. By August, 832 school networks boasted 3.4 million members, 360,000 of them freshman, with over 8,000 new members joining every day.[34]

By the beginning of the fall semester in 2005 Facebook was ubiquitous. 85% of American college students had an account on the site, and 60% used it daily.[35] Its comparative simplicity—no photos, no applications, just a list of interests and a comment box—did not keep millions of students from joining the site and "Friending" all their classmates. Each profile defaulted to public within its network, so students of one university could automatically browse everything about another person.

Little Brother is Watching You: High Schools and Photo Sharing

In September of 2005, Facebook opened to high school students.[36] There were significant restrictions: Facebook required the new users to be vetted by a current Facebook member who had graduated from the same secondary school or by a validated high school classmate. College kids could not join high school networks. According to Facebook cofounder Chris Hughes, this design was meant to mimic actual social circumstances:

> In general, a guiding value of ours is making Facebook a resource for college kids that is directly tied to their everyday lives. So the decision to keep the [high school and college] networks separate sort of followed from that—high schoolers and college kids aren't really interacting on a day-to-day basis, so their networks shouldn't overlap.[37]

However, this design was not sufficient for at least some users of the site, who wrestled with the problem of communicating college content to those outside the college context. As two students wrote in *The Daily Princetonian*:

> [Last] week, when we each accepted friendships from girls born after the fall of the Berlin Wall, we got angry. Really angry. Suddenly, we had to begin removing tags from photos of us drinking, erasing wall postings referring to awkward hookups and getting rid of anything else

---

29 Tabak *supra* note __

30 Tabak *supra* note __

31 For an extended treatment of Facebook's features see Grimmelmann, *supra* note __, at 1144-1149 and generally.

32 Hoffman *supra* note __

33 Hoffman *supra* note __

34 Mary Colurso, *Making connections Freshmen start college with pre-assembled crews gathered from a variety of places*, BIRMINGHAM NEWS, August 21, 2005, at Lifestyle; Pg. 1E Vol. 118 No. 138.

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

36 *Facebook | Timeline,* FACEBOOK, http://www.facebook.com/press/info.php?timeline.

37 See Chris Peterson, *High School Facebook*, THE VIRGINIA INFORMER, October 2005, http://web.wm.edu/so/virginiainformer/archives/oct2005/highschoolfacebook.php/.

> that might negatively influence younger siblings or get back to once-adoring high school teachers. But even beyond that, there's just something about high school facebook that feels wrong.[38]

In October 2005 Facebook introduced the Photos application, allowing students to upload albums and "tag" their friends.[39] A generation of students with digital cameras suddenly had a place to post the photos. By October 2009, four years after Photos was launched, Facebook users had uploaded a total of 80 billion pictures, with 600,000 accessed by users every second from 30,000 servers.[40]

With tremendous quantities of tagged photos came tremendous quantities of documented college hijinks, and with tremendous quantities of documented college hijinks came trouble. In November 2006, Penn State police made headlines after they used photos and groups from Facebook to identify rioters who had stormed the field following a football game against Ohio State.[41] Though many students were horrified to find their social space being turned against them, pundits primly clucked at their naïveté:

> Groups such as "I rushed the field after the OSU game (and lived!)" are acting as "laundry lists of suspects" for the police to interview, said Communications and Law Professor Clay Calvert. . . ."If it's accessible to the public, it's fair game," Calvert said. "People have expectations of privacy in cyberspace that don't exist."[42]

Still, such incidents were comparatively rare and didn't discourage the majority of users. The site continued to grow and by winter 5.5 million students had registered.[43] Many Facebook users reconciled their differences with the upstart high school networks, recognizing that there was no great gap between the social norms of teenagers and the recently teenaged. And, since everyone on Facebook fell into one of these two categories, they acted like it: posting obscene messages, listing alcohol and drugs among their favorite activities, and generally behaving as one would at a large and raucous house party.

Then, their parents came home.[44]

Here Comes Everybody: 300 Million Users and Beyond

In September 2006, Facebook opened registration to anyone with an email address.[45] Its membership skyrocketed as adults flocked to Facebook. In May 2007, Facebook launched its developer program, which allowed third party coders to run their own applications within Facebook.[46] Facebook quickly transformed from a small and personal web community to a large and impersonal social platform.

The more Facebook opened up to the outside world, the more users began to feel exposed and self-conscious about their data. As bosses, teachers, parents and employers joined Facebook, students began to

---

38 See Danny Shea and Mark Feinstein, *An Open Letter to Mark Zuckerberg,* THE DAILY PRINCETONIAN, March 9, 2006, http://www.dailyprincetonian.com/2006/03/09/14810/. Originally cited in boyd, Taken Out of Context, *supra* note __, at 104.

39 *Tag (metadata),* WIKIPEDIA, http://en.wikipedia.org/wiki/Tag_%28metadata%29. When user A tags user B in a photo, that photo becomes publicly associated with user B on Facebook.

40 Rich Miller, *Facebook Now Has 30,000 Servers,* DATACENTERKNOWLEDGE.COM, October 13, 2009, http://www.datacenterknowledge.com/archives/2009/10/13/facebook-now-has-30000-servers/.

41 Devon Lash, *Site Used to Aid Investigation*, THE DAILY COLLEGIAN, November 10, 2005, http://www.collegian.psu.edu/archive/2005/11/11-10-05tdc/11-10-05dnews-09.asp.

42 Lash *supra* note __.

43 *Facebook | Timeline supra* note __.

44 *See, e.g., Oh Crap. My Parents Joined Facebook,* MYPARENTSJOINEDFACEBOOK.COM, http://myparentsjoinedfacebook.com/ ("CONGRATULATIONS! YOUR PARENTS JUST JOINED FACEBOOK. YOUR LIFE IS OFFICIALLY OVER. So, you finally caved. You've accepted a friend request from your Mom, Dad, crazy Aunt Ida, and your college roommate's newly divorced mother. Well here's your chance to get back at them for taking away your public privacy. Email us at: myparentsjoinedfacebook@gmail.com because we want to laugh at your Mom's ridiculous Facebook status and the embarrassing message your Dad wrote on your wall too! If you want your relative to remain anonymous include that in the email. Family. Can't Facebook with 'em, can't unFriend 'em! This site is edited by Jeanne & Erika who love their parents dearly.")

45 *Facebook | Timeline* supra note __.

46 *Facebook Platform Launches*, FACEBOOK DEVELOPER BLOG, May 27, 2007, http://developers.facebook.com/news.php?blog=1&story=21.

reevaluate their presence online. What had once been a safe place to "hang out" with one's friends now posed a potential danger to reputation and career prospects. Universities advised students to delete their Facebook profiles before applying for jobs.[47] A general malaise spread throughout the Facebook community as students felt forced to choose between posting pictures from parties and Friending their family.[48]

By fall 2009, what had begun as a way for awkward Harvard undergraduates to meet each other was completely transformed by the addition of 300 million members, and an unbearable tension had arisen between Facebook's design, its members, their social purposes, and their privacy.[49]

B. THE SOCIAL DYNAMICS OF FACEBOOK: REAL FRIENDS AND IMPRESSION MANAGEMENT

In order to understand the sort of privacy problems afflicting Facebook users we need to understand what Professor James Grimmelmann calls the "social dynamics" of the site.[50] Privacy analyses (and interventions), Grimmelmann argues, must always be attuned to and consonant with the social norms and practices of the community.

Perhaps the most interesting (and potentially counterintuitive) fact about Facebook is that it is not a social *networking* site, but rather a social *network* site.[51] In other words, Facebook is not about meeting new people but rather maintaining contact with people whom one already knows. Mayer and Puller found that only 0.4% of Facebook friendships consisted of "online only" interactions.[52] danah boyd concurred, describing social network sites as malls for modern teens: spaces to socialize, "hang out," and construct their social identity.[53]

The key privacy implication of the "real relationships" phenomenon is that *all interactions on social network sites are animated and governed by preexisting social norms, roles, and expectations*. boyd writes that "the popularity of mySpace is deeply rooted in how the site supports sociality amongst preexisting friend groups."[54] For example, some southern Christian youth believe mySpace's purpose is to organize Bible studies because that is how their friends use the service.[55] When users create their Facebook profiles, articulate Friendship with other users, and interact with them online, they are both reacting to and reconstituting anew their social contexts by "writing community into being."[56] boyd describes youth behavior on social network sites as "performances" in Goffman's dramaturgical sense.[57] As Grimmelmann writes:

> [S]ocial-network-site profiles are wholly social artifacts: controlled impressions for a specific audience, as much performative as informative. . . I should add that profiles aren't just ex-

---

47 For example, Resident Assistants at the University of Massachusetts were routinely warned to delete their Facebook accounts rather than risk compromising their job because of posted evidence of illicit activity.

48 *See generally* the case studies of Part II.D.

49 *See, e.g., Oh Crap, My Parents Joined Facebook, supra* note __.

50 *See generally* Grimmelmann, *Saving Facebook*, *supra* note __.

51 danah boyd and Nicole Ellison, *Social network sites: Definition, history, and scholarship*, JOURNAL OF COMPUTER-MEDIATED COMMUNICATION, Vol. 13, article 11, 2007, available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html. Facebook was originally designed to be a social networking site, a site where awkward Harvard undergraduates could go to easy find other people who enjoyed Lord of the Rings fanfiction as much as they did. When a student listed an item of interest, the list itself became a link, which, when clicked, would print all other students at the school who listed that item as well. To some extent the current Facebook design is path-dependent to this old social purpose, which may explain why there is so much tension between the "Share Everything" model and its members today.

52 Adalbert Mayer and Stephen Puller, *The old boy (and girl) network: Social network formation on university campuses*, JOURNAL OF PUBLIC ECONOMICS, 2008, Vol. 92, p. 329, at 329.

53 *See generally* boyd, Taken Out of Context, *supra* note __.

54 *See* boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life, in* YOUTH, IDENTITY, AND DIGITAL MEDIA, 126 (David Buckingham ed., 2008), available at http://www.danah.org/papers/WhyYouthHeart.pdf.

55 *See* boyd, *My Friends, mySpace: American Youth Socialization on Social Network Sites,* THE BERKMAN CENTER FOR INTERNET & SOCIETY, June 18, 2007, http://cyber.law.harvard.edu/interactive/events/luncheon/2007/06/boyd, at 16:00.

56 *See* boyd, *Friends, Friendsters, and mySpace Top 8: Writing Community Into Being on Social Network Sites,* FIRST MONDAY, December 4, 2006, http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/1418/1336. Though boyd was writing specifically about the mySpace "Top 8" feature—in which users are required to list their very best friends in a way that is published publicly on their profile page—the idea is broadly applicable to any social network site which features an articulated and accessible contacts list. Additionally, an enterprising coder recently recreated the Top 8 functionality with a Facebook app, available at http://www.facebook.com/apps/application.php?id=2425101550.

57 *See generally* boyd, Taken Out of Context, *supra* note __, esp. at 119.

> pressive 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, and the paper-doll aspect of a social-network-site profile encourages this dynamic.[58]

An exhaustive account of the social dynamics of social network sites would fill many volumes. It is sufficient for this Article to establish two uncontroversial yet important and interwoven premises:

- First: *friends preexist Friends*. Put another way, though not all friends are Friends, almost all Friends are friends. Thus, the overwhelming majority of Facebook relationships are digital representations of their corporeal counterparts, and as such are animated by the social roles, expectations, and norms from the "real world."

- Second: *profiles are performative*. They are crafted to present a certain person to a specific audience. Profiles, as Grimmelmann puts it, are "gloriously direct tool[s]. . . for impression management." And, because friends preexist Friends, all of those impressions must be managed in concordance with certain social norms and roles.

C. WHY USERS CARE ABOUT PRIVACY: EXHIBITIONISTS DON'T GO "ICK"

The twin axioms that a) friends preexist Friends and b) profiles are performative tell us something about how and why people use Facebook. A third important element of these social dynamics is the privacy preferences of Facebook users. And the fascinating thing about Facebook users is that they really, *really* care about privacy.

This finding doesn't square with the narrative of social network sites. Popular opinion presumes that members of social network sites—especially the young—simply aren't concerned with privacy, or that their social practices are somehow incompatible with privacy. Columnist Robert Samuelson, writing in the *Washington Post*, decried social network sites as nothing but homes for attention whores.[59] "Exhibitionism is now a big business," Samuelson blustered with the all-knowing air often associated with knowing nothing at all. He continued:

> What's interesting culturally and politically is that [the popularity of Facebook] contradicts the belief that people fear the Internet will violate their right to privacy. In reality, millions of Americans are gleefully discarding—or at least cheerfully compromising—their right to privacy. People seem to crave popularity or celebrity more than they fear the loss of privacy.[60]

Strong stuff—but Samuelson was dead wrong. The data demonstrate Facebook users care deeply about their privacy.

In 2006—while Facebook still limited membership to students—Acquisti and Gross conducted a comprehensive survey of users at an undergraduate university.[61] They asked students to describe how concerned they were about different issues (both in the 'public debate' and within their personal life) along a 7 point scale. One of these issues was privacy on social network sites.

Now if Samuelson were correct, and Facebook users don't care about privacy, then they should have ranked privacy policies very low on a list of concerns. Instead, they ranked privacy policies near the *top* of the list, and were "were more concerned (with statistically significant differences) about threats to their personal

---

58 Grimmelmann, *Saving Facebook*, at 1153.

59 *Attention Whore*, URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=attention+whore. A slang term commonly used by digital natives to refer to persons who post trivial and uninteresting tidbits about their life on the Internet in the desperate hope that someone will care about them. It may also refer to an unattractive person who posts photos of themselves for other unattractive and undersexed people in the hopes that they will be complimented on their wilting and unremarkable physique. See the entry for more examples.

60 Samuelson, *supra* note __.

61 Acquisti and Gross, *supra* note __, at 8.

privacy than about terrorism or global warming. . . "[62] Students were also asked to rate how concerned they would be if "[a] stranger knew where you lived and the location and schedule of the classes you [took],"[63] a proxy for the sort of information available on most Facebook accounts at the time. 81% of students said they were concerned to some degree and nearly 46% said it was of the highest concern.[64]

There are also ample behavioral data that exhibit users repurposing properties of the site to manage exposure.[65] danah boyd describes how users change their names, profile pictures, ages, or locations so that they can't be found via search functions.[66] Sometimes these tools follow social conventions known only to the user's intended audience, such as when a 16 year old reverses the digits in her age to appear 61, or when teenagers from a specific town all claim to be from Christmas Island.[67]

Nor are users particularly concerned about the "usual suspects" when it comes to privacy violations. Digital natives, according to boyd, generally aren't worried about government or advertisers aggregating their information for surveillance or marketing purposes. Rather, users are generally trying to shield themselves from the prying eyes of parents, professors, police officers, and others who hold direct control over and differ normatively from themselves.[68]

To review, students consistently report on surveys that they are very concerned about their privacy on social network sites. Users often take conscious action to try to control access to their profile. They are not, as Samuelson grumpily characterized them, "exhibitionists." Exhibitionists don't care about their privacy. That's why they're exhibitionists. They don't have a sense of embarrassment or revulsion when their "personal information" is shown to others. For Facebook users, such displays feel "icky" and are assiduously avoided.[69]

D. CASE STUDIES

This section outlines some typical privacy problems on Facebook:

- In 2006, two students at the University of Illinois were urinating on the front of a bar. When a police officer approached, Marc Chiles escaped while Adam Gartner was detained. Gartner denied knowing Chiles. Later, the officer accessed Facebook and scoured student profiles. When he realized Chiles and Gartner were Friends on Facebook the officer charged the latter with obstruction of justice. "I had no idea that old people were wise to Facebook," Gartner said. "I thought they referred to it as a doohickey that kids play with. I got bone-crushed." The director of public safety at the University of Illinois later said "[my] feeling about Facebook is, don't post anything you wouldn't want your mother or your future employers reading or seeing."[70]

---

62 Acquisti and Gross, *supra* note __, at 8.

63 Acquisti and Gross, *supra* note __, at 8.

64 Acquisti and Gross, *supra* note __, at 8.

65 One might think of this as an example of users harnessing "generative privacy" to create ad-hoc barriers to expose. For more on generativity, *see generally* JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT (2008).

66 boyd, Taken Out of Context, *supra* note __, at 147.

67 Grimmelmann, *Saving Facebook, supra* note __, at 1152.

68 *See* boyd, *My Friends, myspac*e, *supra* note __, at 42:00. Although boyd wrote primarily about mySpace, she found- as have I—that the same practices held true on Facebook. Of course, one might change one's Facebook name for completely for reasons unrelated to privacy concerns. Often this is done as a joke, as when a stodgy white geek changes his profile photo to a picture of the gangster rapper DMX, or when one young woman I know changed her name to "Alitasaurus" after an acquaintance likened her to a baby dinosaur. Facebook is for social performances, and not all social performances are conducted with the primary intent to protect privacy. However, the number of people who change data about themselves in order to hide from unwanted visitors is nonzero and nontrivial, and the practice is evidence of an interest in privacy.

69 boyd, *Privacy Trainwreck, supra* note __: "What happened with Facebook was not about a change in the bit state—it was about people feeling icky." I choose the word "ick" advisedly. boyd writes that her subjects often characterized such violations (a parent or teacher friending a child, for example) in terms of revulsion or disgust: "For example, when asked if she thought her teachers were on MySpace, Traviesa, the 15-year-old from Los Angeles, responded by saying, "That's nasty!" (see boyd, Taken Out of Context, *supra* note __, at 144). Aria, a 20-year-old college student from California, took this sentiment one step further, noting, "I don't really believe that 'online social networking' is something you can do with someone whose genetic material you inherited without subverting the laws of nature.""

70 *See* Cohen, *supra* note __.

- In 2007, the *Daily Mail* published dozens of photos of intoxicated college girls. "Drunkenly dancing on tables or collapsing in the street used to be a source of acute embarrassment for young women the morning after the night before," crowed the tabloid. "Today, they are more likely to boast about it—to the world, with pictures—on social networking sites."[71] The photos had been culled from a Facebook group called "30 Reasons Girls Should Call It A Night." One student pictured, taken by surprise as she had not posted the photos herself, found herself beleaguered by calls from overseas organizations offering money for sexually explicit interviews.[72] A Google search of this student's name still returns the *Daily Mail* article as the first result.

- In 2008, Katherine Evans was a high school student in Florida. Frustrated by a teacher's alleged unwillingness to assist her with schoolwork, Evans created a Facebook group dedicated to "hating" the teacher. After a few days and in a more temperate mood, she deleted the group. Two months later, she was suspended for "cyberbullying" the teacher. Evans is currently suing the school district, arguing that the suspension breached her rights and blemishes her record.[73] Evans' experience recalls that of Cameron Walker, the president of Fisher College student government, who was expelled after he "damaged the reputation" of a campus police officer by joining a Facebook group critical of the officer's treatment of students.[74]

- In 2009, a 16-year-old employed by a marketing firm in England returned home from work and wrote on her Facebook that her job was "boring." She was promptly fired after colleagues accessed her profile and passed on the post to her supervisor. "[This] display of disrespect and dissatisfaction undermined her relationship with the company," a representative of the firm said. "Had [she] put up a poster on the staff notice board making the same comments and invited other staff to read it there would have been the same result." Skeptics argued that employers rarely followed their employees to the local bar to eavesdrop on any griping that regularly occurred there.[75]

- By 2009 many students found themselves in the uneasy position of having to decide whether to Friend parents or others outside the college context. "Alright im just gonna put this out there. . . It is really weird that Adults are on facebook!!" wrote Jess, a college senior.[76] When asked why it was "weird," she elaborated "because my moms friends are n facebook. . . its jsut weird. and they also do it to watch every moment of there kids life and not give them privacy."[77] Another student reported that "the whole system feels wrong. I can't ignore a 'friend request' from the mother of my girlfriend, sure she's great in real life, but I want to keep that part of my life separate from my life I shared with folks in college. . . It's odd, but it's like I'm too connected."[78] These concerns and complaints echo those of Rachel, who trusted her grandmother but nevertheless felt uncomfortable exposing every aspect of her college experience to someone outside the college context.

III. PRIVACY AND THE ENVIRONMENT

A. PRIVACY AND PERFORMANCE: CONTEXTUAL INTEGRITY ON SOCIAL NETWORK SITES

---

71 *See* Levy, *supra* note __.

72 In person interview with "Amanda", a University of Massachusetts junior who requested anonymity, February, 2009.

73 *See* Carmen Gentile, *Student Fights Record of 'Cyberbullying'",* N.Y. TIMES, February 8, 2009, page A20, available at http://www.nytimes.com/2009/02/08/us/08cyberbully.html.

74 *See* Schweitzer, *supra* note __.

75 *See Facebook Remark Teenager Is Fired, supra* note __. *See also* Brian Krebs, *Court Rules Against Teacher in MySpace 'Drunken Pirate' Case*, THE WASHINGTON POST, December 3, 2008, http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html, for the case of Stacy Snyder, a 25 year old student-teacher who was denied her degree in education because a picture she posted to her mySpace showed her drinking from a red cup with the caption "drunken pirate."

76 Facebook status update by "Jess", FACEBOOK (April 22, 2009), on file with the author.

77 Facebook message from "Jess" to Chris Peterson, FACEBOOK (April 22, 2009), on file with the author.

78 Private message from "Robert" to Chris Peterson, SOMETHINGAWFUL FORUMS (March 27, 2009), on file with the author.

Return for a moment to Rachel's story. Hers hasn't been a problem for previous generations of college students. Before Facebook, it was easy to keep drinking games in the dorm room and Grandma in the family room. Unless a young woman went out of her way to begin a beer pong tournament over Christmas dinner, college and family life were mostly kept separate, and the catchphrase "going away to college" possessed a normative as well as geographical significance.

For Rachel and other digital natives,[79] however, this is no longer necessarily true. Networked publics—the virtual "spaces" within which an increasing number of people spend an increasing amount of time[80]—break down the physical separation of social situations and make it difficult for users to know who is watching.[81] They also befuddle users by removing or remaking the architectural heuristics that guide privacy practices in the physical world. Social network sites possess certain counterintuitive communicative properties that subtly but fundamentally change how individuals represent and situate themselves.[82]

This realization is the analytical key that unlocks the cause of the privacy problem. In the physical world, Rachel not only *conducts herself* differently with her grandmother than with her college friends, she *is a different person* with her grandmother than with her college friends, because "to *be* a given kind of person. . . is not merely to possess the required attributes, but also to sustain the standards of conduct and appearance that one's social grouping attaches thereto."[83] Look at her language: she is worried that her grandmother's image of her "perfectly angelic self"—an image which Rachel has carefully crafted—will be "shattered forever" when juxtaposed against her bacchanal behavior. She suffers from a crisis in what the sociologist Erving Goffman called the presentation of self.[84] Accustomed, as we all are, to constituting different characters for different social contexts, she is horrified by the possibility that her worlds may collide.

This is true of all of the case studies. It is hardly uncommon for high school students tell their friends they "hate" a teacher as Katherine Evans did—but it is uncommon for them to say it to the teacher's face. Gartner and Chiles would have told anyone in the world they were friends that night—except for their arresting officer. Anyone who has never complained their job is boring has never had a job—but it becomes a firing offense once posted to Facebook. Engaging in drunken debauchery at a college party is the rule rather than the exception—but to have photos of it published in a newspaper is exceptionally embarrassing.

What is conceptually interesting about these case studies is that they don't jibe with our usual ideas about privacy problems. This isn't really about *secrecy*: none of the individuals in the case studies sought seclusion, they just wanted (or expected) to keep information away from certain people in certain circumstances. And it isn't really about *control*: no one was forced or required to post these data, but did so in the pursuit of presentation, and were blindsided by the contextual consequences.

The fundamental problem here is a breakdown in what the privacy theorist Helen Nissenbaum calls *contextual integrity*.[85] Echoing Goffman's work on social performance, Nissembaum argues that privacy is violated when individuals do not respect social norms of appropriateness and distribution.[86] The former prescribe what data may be shared in a given situation; the latter prescribe how and with whom data may be shared. When behavior appropriate for a bar is conducted in a church it violates norms of appropriateness; when a marketer learns that which was intended for a doctor it violates norms of distribution. Or, more formally:

---

79 "Digital natives" is a term generally used to refer to individuals who grew up with personal computers and prevalent Internet access such that they are "natives" and not "immigrants" to the pervasively networked world. *See, e.g.,* URS GASSER & JOHN PALFREY, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES, 2008.

80 For an extensive account of the meaning, growth, and character of "networked publics", see boyd, Taken Out of Context, *supra* note __, at 24.

81 *See, e.g.,* boyd, Taken Out of Context, *supra* note __, at 34.

82 *See, e.g.,* boyd, Taken Out of Context, *supra* note __, at 34.

83 ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE 75 (1959). Originally cited in boyd, Taken Out of Context, *supra* note __.

84 *See generally* GOFFMAN, *supra* note __.

85 *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (forthcoming 2010). *See also* JEFFREY ROSEN, THE UNWANTED GAZE: THE DESTRUCTION OF PRIVACY IN AMERICA (2000) (for a general application of the theory of contextual integrity to the Internet).

86 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119, 124; available at http://ssrn.com/abstract=534622.

> Contextual integrity is defined in terms of informational norms: it is preserved when informational norms are respected and violated when informational norms are breached. . . [The] capacities in which actors function are crucial to the moral legitimacy of certain flows of information. This holds true even when it appears that it does not—as when people remark that certain information is secret when they usually mean it is secret in relation to some actors, or constrained by a particular principle of transmission rather than absolutely. Usually, when we mind that information about us is shared, we mind not simply that it is being shared but that it is being shared in the wrong ways and with inappropriate others.[87]

> The central thesis of the framework of contextual integrity is that what bothers people, what we see as dangerous, threatening, disturbing, and annoying, what makes us indignant, resistant, unsettled, and outraged in our experience of contemporary systems and practices of information gathering, aggregation, analysis, and dissemination is not that they diminish our control and pierce our secrecy, but that they transgress context-relevant informational norms.[88]

Nissenbaum's normative framework describes perfectly the privacy problems of social network sites as experienced by their users. The case studies are characterized by information shared "in the wrong way and with inappropriate others."[89] The collapse of social contexts—exposing Grandma to beer bongs—transgresses context-relevant informational norms by changing how and to whom information is distributed and communicated. And though Nissenbaum, by her own admission, is not a student of social networks, the hypothesis she hazards about their privacy problems is pitch-perfect:

> Were we to investigate cases in which people have experienced nasty surprises of discovery, we would find that they have understood themselves to be operating in one context and governed by the norms of that context, only to find that others have taken them to be operating in a different one. In other words, the nasty surprises are evidence of a clash of contexts: participants who consider themselves acting in one capacity in one context are treated as if they are acting in another capacity in a different context. As a result, subjects experience

---

87 *See* NISSENBAUM, *supra* note __, at 140-142.

88 *See* NISSENBAUM, *supra* note __, at 186. *See also* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, LAW AND PHILOSOPHY, Vol. 17, 559-596, 581, (1998); available at http://www.jstor.org/stable/3505189 ("Most people have a robust sense of the information about them that is relevant, appropriate, or proper to particular circumstances, situations, or relationships. When information is judged appropriate for a particular situation it usually is readily shared; when appropriate information is recorded and applied appropriately to a particular circumstance it draws no objection. People do not object to providing to doctors, for example, the details of their physical condition, discussing their children's problems with their children's teachers, divulging financial information to loan officers at banks, sharing with close friends the details of their romantic relationships. For the myriad transactions, situations and relationships in which people engage, there are norms. . . .governing how much information and what type of information is fitting for them.")

89 NISSENBAUM, *supra* note __, at 186. *Cf.* ARISTOTLE, THE NICHOMACHEAN ETHICS 214 (Wordsworth Editions 1996) (Compare the college student in note __ who believed that Friending parents "subverts the laws of nature" with Aristotle's observation that "[the] friendship between parents and children is not the same as that between ruler and ruled, nor indeed is the friendship of father for son the same as that of son for father, nor that of husband for wife as that of wife for husband; for each of these persons has. . . different motives for their regard, and so the affection and friendship they feel are different."); James Rachels, *Why Privacy Is Important*, PHILOSOPHY AND PUBLIC AFFAIRS, Vol. 4, No 4, p. 323-333, at 383 (1975); available at http://www.jstor.org/stable/2265077. ("[The relationships] people have to one another involves a conception of how it is appropriate for them to behave with each other, and what is more, a conception of the kind and degree of knowledge concerning one another which it is appropriate for them to have.)"; Rachels, *id*, at 327 ("It is not merely accidental that we vary our behavior with different people according to the different social relationships that we have with them. Rather, the different patterns of behavior are (partly) what define the different relationships; they are an integral part of what makes the different relationships what they are."); Rachels, *id*, at 326 (""[T]here is a close connection between our ability to control who hasaccess to us and to information about us, and our ability to create andmaintain different sorts of social relationships with differentpeople. . . privacy is necessary if we are to maintain the variety ofsocial relationships with other people that we want to have and that iswhy it is important to us."); Elizabeth Beardsley, *Privacy, Autonomy, and Selective Disclosure*, *in* NOMOS XIII 65, 70 (Pennock and Chapman ed., Atherton Press 1971) ("Selective disclosure [is] the conceptual core of the norm of privacy."); ALTMAN, *supra* note __, at 40 ("Most people are more or less able to separate the different roles in their lives; their functioning in one situation (for example, as a husband or a father) is separate from their role in other settings (for example, as a business executive)."); *id* at 51 ("The essence of this discussion is that privacy mechanisms define the limits and boundaries of the self. When the permeability of those boundaries is under the control of a person, a sense of individuality develops. But it is not the inclusion or exclusion of others that is vital to self-definition; it is the ability to regulate contact when desired. If I can control what is me and not me, if I can define what is me and not me, and if I can observe the limits and scope of my control, then I have taken major steps toward understanding and defining what I am. Thus privacy mechanisms serve to help to define me."); CLAY SHIRKY, HERE COMES EVERYBODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS 85 (2008) ("The bloggers and the social network users operating in small groups are part of a community, and they are enjoying something analogous to the privacy of the mall. On any given day you could go to the food court in a mall and find a group of teenagers hanging out and talking to each other. They are in public, and you could certainly sit at the next table over and listen in on them if you wanted to. And what would they be saying to one another? They'd be saying, "I can't believe I missed you last night!!! Trac talked to you and said you were TRASHED off your ASS!" They'd be doing something similar to what they are doing on LiveJournal or Xanga, in other words, but if you were listening in to their conversation at the mall, as opposed to reading their post, it would be clear that you were the weird one.")

> a particular transmission of information as a transgression of context-relative information norms that may be considered in perfect compliance with the informational norms of a different context.[90]

Contextual integrity precisely explains privacy problems on social network sites. It harmonizes with actual practice, resolving the dissonance between stated concern for privacy and the actual behavior of users. As Nissenbaum notes, "there is no paradox in caring deeply about privacy and, at the same time, eagerly sharing information as long as the sharing and withholding conform with the principled conditions prescribed by governing contextual norms."[91]

The theory of contextual integrity explains *how* privacy problems occur on social network sites: individuals inappropriately transmit information and collapse contexts. In order to understand *why* these collapses occur—that is, why the same individuals who weave their offline presentation with nimble dexterity fumble it away so easily online—it is necessary to explore the role of the environment in preserving or dismantling contextual integrity.

B. THE ENVIRONMENTAL UNDERPINNINGS OF CONTEXTUAL INTEGRITY

It is important to remember that norms of appropriateness and distribution aren't static things. Like all social constructs, they are in flux, constantly being contested and reconstituted. One might expect that the conflicts over information norms on social network sites are thus unremarkable. It is not at all uncommon for different generations or cultures to disagree about the sorts of behavior that are acceptable for a given social situation or relationship (appropriateness) or the ways in which information may acceptably flow or circulate between or among social situations and relationships (distribution).

But that's not what's happening on social network sites. Rachel doesn't contest her grandmother's norms about the social unacceptability of drinking games. To the contrary, she *respects* them, striving to observe different standards of behavior around her grandmother and attempting to separate her college norms from her family norms. The same is true for the rest of the case studies, all of which were characterized by contextually crossed wires, not an earnest disagreement about the propriety of alcoholic paraphernalia.

Neither is it true that social network sites are a normative vacuum, and that these are merely shockwaves caused by the the rocky rise of a new set of norms specific to Facebook. As noted in Part II.B, all Facebook Friendships are infused with and animated by the roles and expectations of preexisting friendships. To argue otherwise is inconsistent with actual practice. As Nissenbaum notes:

> I reject the idea that social networking sites define a newly emergent, *sui generis* social context with its own internal rules [and] that there are no entrenched norms with which we need to contend. What seems to make more sense is a conception of these sites as a medium of interaction, transaction, information exchange, communication, and much more, serving and extending the transactional range of a diverse variety of social contexts. In a similar vein, one might conceive of the telephone system not as constituting a distinctive context, but as a medium for interactions occurring within diverse distinctive contexts, such as family, workplace, and medical [interactions] governed by norms of respective social contexts and [acquiring] significance from their occurrences within them.[92]

Instead, we are witnessing something far more radical and interesting on Facebook: a "change in behavioral settings"[93] caused by the deterioration of certain architectural properties that previously afforded nor-

---

90 NISSENBAUM, *supra* note __, at 225.

91 NISSENBAUM, *supra* note __, at 187.

92 NISSENBAUM, *supra* note __, at 223.

93 JOSHUA MEYROWITZ, NO SENSE OF PLACE: THE IMPACT OF ELECTRONIC MEDIA ON SOCIAL BEHAVIOR *ix.* Meyrowitz, as danah boyd notes, wrote before the widespread impact of the Internet, but his theory is indispensable to any analysis of digital spaces.

matively distinct social situations.[94] The breakdown in contextual integrity on social network sites can be attributed at least in part to the design of the social space of Facebook. Put another way, it is not really that norms are changing, but that the space within which performances are conducted and self-presentation crafted has changed.[95] The shape of something as fluid as a social situation depends on the design of its enclosure. Our understanding of the boundaries and informational dynamics of a "situation" is a byproduct of the properties of the physical world.[96] These properties are so familiar that we take them for granted but they are quite different in any digital environment.[97]

Consider the potential implications of these properties for our behavior. It is totally uncontroversial to suggest that *spaces have norms*: one doesn't generally wear a bikini to church, for example. The often unsaid assumption that undergirds this observation, however, is that *norms have spaces*, for in order because there to be a norm against wearing bikinis within the space of a church, there must first be a church-space that is *situationally distinct from* other spaces. One behaves differently in a bar than in a church in part because they occupy different spaces. One behaves differently at a wedding reception than at a bingo game even if they occupy the same hall because they occur at different times. This physical separation of social situations is a byproduct of the properties of the corporeal world. Walls, roofs, and fences not only keep intruders out, they define specific audiences or communities within which social norms operate, and make it easy to see where and to whom information flows.[98]

Facebook is different. As Professor Joshua Meyrowitz has written, "electronic media have undermined the traditional relationship between physical setting and social situation. . . electronic media may create new social environments that reshape behavior in ways that go beyond the specific products delivered."[99] Such undermining occurs on social network sites, where unimaginably complex social relations collapse to the infinitely thin plane of a single profile. Meyrowitz noted that within the electronic medium, "one can be an [observer] being physically present; one can communicate 'directly' with others without meeting in the same place. As a result, the physical structures that once divided our society have been greatly reduced in social significance."[100] He offers an example drawn from personal experience:

> When I returned home [from a summer vacation in Europe during college] I began to share [my experiences] with my friends, family, and other people I knew. But I did not give everyone I spoke to exactly the same account of my trip. My parents, for example, heard about the safe and clean hotels in which I stayed and about how my trip had made me less of a picky eater. In contrast, my friends heard an account filled with danger, adventure, and a little romance. My professors heard about the "educational" aspects of my trip. . . each of my many audiences heard a different account. Did I lie to any of these people? Not really. But I told them different truths.

---

94 *Cf* Jonathan Gruden, *Desituating Action: Digital Representation of Context*, HUMAN COMPUTER INTERACTION, Vol. 16, Issue 2, p. 269-286, 279 (2001), available at http://research.microsoft.com/en-us/um/redmond/groups/coet/grudin/hci-contextaware.pdf. ("Why then the uneasiness, the widespread attention to privacy? It may reflect an awareness at some level of something more fundamental than privacy that is being challenged: The steady erosion of clearly situated action. We are losing control and knowledge of the consequences of our actions, because if what we do is represented digitally, it can appear anywhere and at any time in the future. We no longer control access to anything we disclose.")

95 boyd, Taken Out of Context, *supra* note __, at 34.

96 *See generally* MEYROWITZ, *supra* note __.

97 *See, e.g.,* Lawrence Lessig, *The Architecture of Privacy,* 1 VAND. J. ENT. L. & PRAC. 56, available at http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf.

98 *See* MEYROWITZ, *supra* note __, at *vii* ("Sociologists have long noted that people behave differently in different 'social' situations, depending on where one is and who one is with. Implicit in such an approach is the idea that behavior in a given situation is also affected by where one is not, and who is not there."); *id* at 5 ("The basic argument here is that many of the traditionally perceived differences among people of different social 'groups,' different stages of socialization, and different levels of authority were supported by the division of people in to very different experiential worlds."); *id* at 35 ("It is not surprising that most of those who have studied the effects of situations on behavior have focused on encounters that occur in given places. Until recently, place-bound, face-to-face interaction was the only means of gaining 'direct' access to the sights and sounds of another's behavior. The physical barriers and boundaries marked by walls and fences as well as the passageways provided by doors and corridors directed the flow of people and determined [interactions].")

99 MEYROWITZ, *supra* note __, at 7.

100 MEYROWITZ, *supra* note __, at *vii*.

> [But consider] what would have happened to the various accounts of my European vacation if, on my return, my parents had decided to throw a surprise homecoming party to which they invited all my friends, relatives, professors, and neighbors. What would have happened to my description of my trip if I could not have separated my audiences?. . . Clearly almost any account designed for a specific audience would have offended or bored parts of the combined audience. . . .I might have been able to adapt quickly to the combined situation and said [something] bland enough to offend no one. The point is that when distinct social settings are combined, once appropriate behavior may become inappropriate.[101]

Meyrowitz's hypothetical horror story is the daily dilemma of the digital native. Every day, college students returning from semesters abroad must decide how to share photos with friends. Meyrowitz, or any member of his generation, would have found this a simple task: go home to show parents some photos, then go to some other place or some other time and show the rest to friends. Facebook, by contrast, is a system that communicates everything to everyone at the same time and in the same space. Facebook does not facilitate the segregation of audiences by which "the individual ensures that those before whom he plays one of his parts will not be the same individuals before whom he plays a different part in another setting."[102] Different users handle this problem in different ways. Some err on the side of caution and upload nothing to avoid giving offense and become hopelessly bland. Others post everything and shock their recently Friended grandmothers. These are not problems that existed before the technology of social network sites: as danah boyd has said, digital natives are the first generation to grow up living in celebrity-style publics.[103]

I cannot stress enough that Facebook is a space with informational properties wholly unlike those of the physical world. It is an "environment that is fundamentally unnatural, in conflict with the one we evolved to live in."[104] The problems of privacy on Facebook are thus not *caused* by contests of norms, though such contests certainly occur. Instead, they are caused by Facebook's design, which upends many of the properties presumed by informational norms and consequently makes them difficult or impossible to respect. The physical world is ephemeral; Facebook is recorded and searchable.[105] The physical world makes publishing difficult; Facebook makes publishing the default.[106] In the physical world, social situations are structurally separate; on Facebook, they are collapsed to a single space.[107]

Notice that here the metaphor of "architecture" as objective constraint and that of "architecture" as subjective heuristic run right into each other. To see what I mean, consider a wall. A wall has both objective and subjective effects on communication. A wall muffles sound, and that objectively constrains the individual. It also gives rise to a subjective heuristic, because experience informs the individual that walls muffle sound. The individual, once familiar with this property of walls, expects it, and her behavior is informed by this expectation. The objective constraint (muffling sound) produces a subjective heuristic (the user calibrating volume based on their expectations of the effects of objective constraints).

This system works fine in the physical world, because people expect a wall to muffle sound and it actually does muffle sound. The problem comes when the constraint and its heuristic become disassociated, as with a false mirror that appears to reflect but actually reveals.[108] Facebook is *full* of false mirrors. The *architectural*

---

101 MEYROWITZ, *supra* note __, at 1.

102 GOFFMAN, *supra* note __, at 49.

103 boyd, *My Friends, my.Space*, *supra* note __, at 33:25. *See e.g.* LAMEBOOK, http://lamebook.com (the functional equivalent of a shaming tabloid for Facebookers).

104, Gruden, *supra* note __, writing of the Internet's effect on privacy.

105 *See generally* Lessig, *The Architecture of Privacy*, *supra* note __.

106 *See* CLAY SHIRKY, HERE COMES EVERYODY: THE POWER OF ORGANIZING WITHOUT ORGANIZATIONS 77 ("Publishing used to require access to a printing press, and as a result was something limited to a tiny fraction of the population, and reaching a population outside a geographically limited area was even more restricted. . . An individual with a camera or a keyboard is now a non-profit of one, and self-publishing is now the normal case.")

107 *See generally* MEYROWITZ, *supra* note __.

108 *Cf* GOFFMAN, *supra* note __, at 119 ("A somewhat related instance of special backstage difficulty is to be found in the architecture of some current housing projects. For walls that are really thin partitions can separate domestic establishments visually, but allow the backstage and frontstage activity of one unit to sound through into the neighboring establishment.")

heuristics of privacy are completely broken. The people-environment unit on Facebook is totally different than that of the physical world because the informational properties of the Facebook space are totally different.[109]

The next sections review three key components that contribute to the collapse of contexts. I use the term "technological fiction" to refer to certain elements of Facebook's design. These are properties of the Facebook space which do not concord with the architectural heuristics of its users. They are contrivances of Facebook's design which, like all fictions, simplify extraordinarily complex interpersonal interactions. They reduce or distort social situations and relations and are often result in the user experiencing something counterfactual to what is actually occurring. Technological fictions intervene at the evaluative layer of the decisional process and greatly impact how people use the technology.

C. FLAT FRIENDSHIPS

Facebook Friendships are crude devices: two users are either Friends or they are not.[110] In formal terms, Facebook Friendships are "indistinguishable with respect to tie strength."[111] By default, any information posted by a user on Facebook may be accessed by any one of their Friends.

While practice suggests Facebook Friends are unlikely to be complete strangers, the act of "Friending" doesn't describe the quality of the preexisting relationship between users. Friending patterns on social network sites are often characterized as "promiscuous" or as following a "Law of Amiable Inclusiveness"[112] such that knowing someone is sufficient cause to Friend them[113] (as Friending is a key mechanism by which digital natives accrue social capital).[114] Furthermore, Facebook does not differentiate between what is revealed to different Friends, and therefore doesn't recognize the preexisting normative and dramaturgical distinctions in relationships. If users are truly writing their communities into being, they are doing so in a crabbed hand with a blotchy pen. As boyd writes,

> The term "friend" in the context of social network sites is not the same as in everyday vernacular. And people know this. This is why they used to say fun things like "Well, she's my Friendster but not my friend." (The language doesn't work out so cleanly on Facebook.) The term is terrible but it means something different on these sites; it's not to anyone's advantage to assume that the rules of friendship apply to Friendship.[115]

Flat Friendships are technological fictions because they rarely resemble the user's preexisting social relations. Beyond the simple acknowledgement of "yes, I've met you," Friendship asks and says nothing qualitative about the actual relationship between two Friends. It does not inquire how or within what normative context they know each other. Friendship cares nothing for the preexisting social roles and expectations that actually animate the friendship. In the physical world, people differentiate disclosure with the precision of a surgeon's scalpel, but on Facebook they are given only a hatchet, relegated to hacking their way through dense social brush where their only options are to offend or deFriend everyone they know.

This fiction is deeply unfamiliar, counterintuitive and counterproductive to privacy. The mental model is completely off. Social relations are not, in the sterile language of sociology, indistinguishable with respect to tie strength. Social networks are rich and earthy and differentiated and distinguishable. This is more than a

---

109 *Cf, e.g.,* boyd, Faceted/Id: Managing Representation in a Digital World 36 (August 2002) (Unpublished Master's thesis for the MIT Media Lab), available at http://www.danah.org/papers/Thesis.FacetedIdentity.pdf.

110 It seems interesting that Facebook's Friend/notFriend dichotomy mirrors the secret/public dichotomy often found in the law.

111 Kevin Lewis et al., *Tastes, ties, and time: A new social network dataset using Facebook.com* 332, SOCIAL NETWORKS, Vol. 30, Issue 4, p.330-342, (2008), available at http://www.cs.trinity.edu/~yzhang/reu/2009/Program/JournalClub/Facebook.pdf.

112 *See* Randall Stross, *When Everyone's a Friend, Is Anything Private?*, N.Y. TIMES, March 7, 2009, available at http://www.nytimes.com/2009/03/08/business/08digi.html.

113 See boyd, "Friends, friendsters, and top 8," *supra* note __, at 11. ("[Users] tend to Friend actual friends, acquaintances, family members, or colleagues.") Promiscuous Friending is a key mechanism by which digital natives accrue social capital.

114 See Nicole B. Ellison et. al., *The beenfits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites*, JOURNAL OF COMPUTER-MEDIATED COMMUNICATION, 12(4) article 1 (2007), available at http://jcmc.indiana.edu/vol12/issue4/ellison.html.

115 See boyd, "Facebook's Privacy Trainwreck.", *supra* note __.

mere academic or aesthetic quibble. The flat nature of Friendship is a root cause of the crisis of self-presentation and breakdown of contextual integrity on Facebook, because without a way to differentiate disclosure between Friends, every member of Facebook is haunted by the specter of Meyrowitz's "welcome home party."

D. INVISIBLE AUDIENCES

The sort of things we say often depend on who we think are listening. As James Grimmelmann notes, "[we] don't say private things when the wrong people are listening in. To know whether they might be, we rely on social and architectural heuristics to help us envision our potential audience."[116]

For example, people tend to modulate the volume of their voice during conversation depending on the sensitivity of the content and who is within earshot. This is a privacy practice of the physical world. However, even something as simple as volume control requires a great deal of information about one's situation. The physical world provides this situational data readily: both the social heuristics (i.e. "are there children present?") and the architectural heuristics (i.e. "how easily does my voice carry in this particular room?") are easily apprehended.

Electronic media are different. Public figures cannot see the audience behind the lens of the television camera, and users of social network sites can't detect who might be watching from the other end of an Internet connection.[117] danah boyd has memorably characterized this as a problem of "invisible audiences", noting that since "not all audiences are visible when a person is contributing online, nor are they necessarily co-present" it can be extremely difficult to fulfill normative expectations of social roles.[118]

To understand how Invisible Audiences might deceive performers, consider the story of Stokely Carmichael.[119] As one of the nation's preeminent black activists in the Civil Rights era, he regularly spoke before black and white audiences about racial equality. Carmichael easily tailored his voice to the situation, modifying manner and rhetoric to adapt to his audience.

In the late 1960s Carmichael was invited to appear on television and radio broadcasts. In the physical world Carmichael targeted his audience by differentiating his disclosure, but on television his audience was invisible behind the lens. Whereas he had once changed styles as he changed spaces—speaking very differently at the tony Whitewater Hotel than at a raucous gathering in Detroit[120]—on television he preached before a diverse and invisible congregation. Carmichael couldn't modify his style, but he also couldn't speak "neutrally," since that would alienate all of his audiences. Carmichael adopted a comparatively radical style, inadvertently alienated white audiences, and became marginalized in the public eye.[121]

---

116 Grimmelmann, *Saving Facebook, supra* note __, at 1162.

117 This depends to some degree upon the site. mySpace profiles, for instance, are public by default, which means that they are open to the entire web. That is a *massive* invisible audience. Facebook, on the other hand, defaults to being "private" to one's Friends and Networks. These are still invisible audiences, but they are audiences that have at least been tacitly (and usually unconsciously) approved by the user. While "known" invisible audiences may mitigate the problem they do not solve them. True, a user may know intellectually that their profile photo is visible to all 1000 of their Friends. At the same time, they don't think about their relationship with each person and whether the photo is appropriate for all contexts.

118 See boyd, Taken Out of Context, *supra* note __, at 34. *See also* Grimmelmann, *Saving Facebook, supra* note __, at 1162, where he identifies the social heuristics of "Nobody in here but us chickens" and "I think we're alone now."

119 The analysis of Stokely Carmichael as an example of treacherously invisible audiences is based on similar treatments in the work of MEYROWITZ, *supra* note __, and boyd, Taken Out of Context, *supra* note __.

120 Wayne Brockriede & Robert L. Scott, *Stokely Carmichael: Two Speeches on Black Power*, *in* LANGUAGE, COMMUNICATION, AND RHETORIC IN BLACK AMERICA (Molefi K. Asante ed., 1972). Compare Carmichael's speech about integration before a primarily white audience, *id* at181 ("Its goal was to make the white community accessible to 'qualified' Negroes and presumably each year a few more Negroes armed with their passports—a couple of university degrees—would escape into middle-class America and adopt the attitudes and lifestyles of that group; and one day the Harlems and the Watts would stand empty, a tribute to the success of integration.") with his speech on the same subject before a primarily black audience, *id* at 181 ("Baby, they ain't doing nothing but absorbing the best that we have. It's time that we bring them back into our community. You need to tell LBJ and all them white folk that we don't have to move into white schools to get a better education. . . all they need to do is stop exploiting and oppressing our communities and we are going to take care [of them].")

121 Carmichael was aware of the media's reductive depictions of him and criticized them at length. Like everything else, the style of his critiques depended on whether his audience was white, *id* at 185 (". . . Negroes are dependent on, and at the discretion of, forces and institutions within the white society which have little interest in representing us honestly.") or black, *id* at 185 ("Those guys over there. They're called the press. I got up one morning and read a story. They were talking about a cat named Stokely Carmichael. I say he must be a bad nigger. . . I had to get up and look in the mirror to make sure it was me!")

The story of Stokely Carmichael demonstrates how difficult it is to respect norms of appropriateness when the audience is invisible. danah boyd notes that in "unmediated spaces, it is common to have a sense for who is present and can witness a particular performance,"[122] but no such feedback exists on Facebook. Similarly, Professor Jonathan Zittrain has described the Internet as having a certain "autistic" quality in that it doesn't convey a sense of who is "with", situationally speaking, at any given time in any given space.[123]

Invisible Audiences are another technological fiction of Facebook because they rob users of situational awareness. Facebook users generally realize that *someone* is accessing their data (that is of course the point of Facebook), but they don't necessarily know who is accessing it or what content they view. Like suspects in an interrogation room, users know that someone is behind the false mirror, but they don't know who is watching and consequently what role they should play. boyd describes how the inability to perceive audiences on Facebook prevents users from realizing their misrepresentations:

> Unexpected collisions, like running into one's boss while out with friends, can create awkwardness, but since both parties are typically aware of the collision, it can often be easy to make quick adjustments to one's behavior to address the awkward situation. In networked publics, contexts often collide such that the performer is unaware of audiences from different contexts, magnifying the awkwardness and making adjustments impossible.[124]

In the physical world people can see their audiences and situate themselves accordingly. On Facebook, even if audiences are *known* intellectually, they aren't *salient* viscerally, and so users may sometimes disclose information unintentionally. Every Facebook user has had the experience of posting an item, having it commented on by someone they didn't really "know" could see it, and feeling that sense of "ick" that signals a violation of privacy. Invisible Audiences have the potential to turn anyone into a celebrity, not because they bestow particular fame or fortune but because they watch with unseen eyes, obscure norms of appropriateness, and cause contexts to collide.

E. STRANGE SHARING DEFAULTS

The default design of the physical world requires a great deal of effort to share information. Gossips aside, the properties of real space are such that information at rest tends to stay at rest, and information in motion tends to come to rest rather quickly. For much of human history, the distance and velocity with which information could travel were constrained by the loudness of the crier or the speed of the messenger. Even the advent of publishing didn't do much to change this dynamic, as it still requires costly time and effort to move newspapers and books.[125] In the physical world, data are dead weight, and only through intentional action do they move around.

These properties beget expectations, which in turn produce architectural heuristics. When an individual relocates to a new town, they don't expect that merely moving there broadcasts their religious beliefs and sexual preferences to every other resident. In populated areas like cities, even the most gregarious may never encounter more than a relative handful of individuals, much less share their entire life story. Dead weight data create strong expectations that information needs to be "pushed" around.

The dynamics of Facebook are completely different. The introduction of the News Feed—which automatically published and updated a list of every action each user took on Facebook to their Friends, rather than requiring Friends to affirmatively access their profile—famously transformed Facebook from a "pull" to

---

122 See boyd, Taken Out of Context, *supra* note __, at 34.

123 *See* Jonathan Zittrain, *A Neighborhood Watch in Cyberspace*, CHRONICLE OF HIGHER EDUCATION, April 2, 2009, available at http://chronicle.com/wiredcampus/article/3692/jonathan-zittrain-a-neighborhood-watch-in-cyberspace-not-a-security-czar, ("Right now each PC has a metaphorically autistic experience: It surfs from one site to the next with no awareness of what other PC's are doing.")

124 See boyd, Taken Out of Context, *supra* note __, at 38.

125 see shirky at note __ (was 100 as of last revision; the "information moving around" post) from like page 79

a "push" environment[126] overnight. This change in the default design caused a "privacy lurch"[127] as users, accustomed to one informational environment, suddenly found that same actions now reverberated to a broader audience, as if a bullhorn had been unknowingly affixed to whispering lips.[128] A more recent "lurch" occurred in late 2009, when Facebook removed certain privacy settings (including the ability to hide one's Friends from other users) and made more content publicly accessible default, a decision at least one commentator referred to as "Facebook's Great Betrayal."[129]

Or, consider the registration page for Facebook, which allows users to join "networks." These networks were originally college campuses but have since grown to include high schools and companies. Until recently, they also included geographic regions, such as large cities or towns. Facebook sets the default such that when one posts anything to their profile it is immediately accessible to all members of all of their networks. Two notable exceptions are photos and videos. For these media, the default is *global* access. Upload a photo album, and by default any member of Facebook anywhere in the world can see it.

These Strange Sharing Defaults are technological fictions because they do not accord with user expectations. No one thinks that moving to Oakland means pushing all their information at every other resident, but joining the Oakland network on Facebook did exactly that, despite the fact that "doing things on the basis of 'networks' doesn't help draw socially meaningful lines."[130] The fact that a student and their parent and professor all live in Palo Alto does not mean that they are going to react the same way to photos of a college party, and it seems highly unlikely that the nearly 900,000 members of the Boston network really agree on what constitutes appropriate behavior.

To Facebook's credit it phased out regional networks in late 2009, recognizing that "they did not adequately reflect a world where people choose exactly the audience with whom they wish to share."[131] While that seems like a fine first step, Facebook apparently missed the point by about a mile, because the *global* publishing default of photos and videos (and nudging of users to ever-more indiscreet preferences in the wake of the changeover) still disrespects any norm of distribution, and seem likely to create even more privacy problems than the regional networks did.[132]

Facebook was, is, and continues to be designed with disclosure in mind.[133] It makes dead weight data fly around the world in ways people would never expect. Facebook assumes that networks which describe membership within a community should also prescribe access for that community. Strange Sharing Defaults run counter to user expectations, are diametrically opposed to norms of distribution, and contribute directly to the collapse of contextual integrity.

IV. RECONSTRUCTING COLLAPSED CONTEXTS

A. WHY FACEBOOK SHOULD CARE

These technological fictions are key deficiencies in the privacy architecture of Facebook. They rob users of the architectural heuristics on which they rely to situate themselves and keep contexts apart. Perhaps un-

---

126 *See* Grimmelmann, *Saving Facebook*, *supra* note __, at 1169.

127 *See* Grimmelmann, *Saving Facebook*, *supra* note __, at 1201.

128 *See* danah boyd, *Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama, supra* note __ (the metaphor of the music suddenly stopping at a party is particularly apt here).

129 Ryan Tate, *Facebook's Great Betrayal,* GAWKER, December 14, 2009, available at http://gawker.com/5426176/facebooks-great-betrayal.

130 Telephone interview with James Grimmelmann, Professor, New York Law School (January 15, 2009).

131 Chris Kelly, *Improving Sharing Through Control, Simplicity and Connection,* FACEBOOK BLOG, July 1, 2009, available at http://blog.facebook.com/blog.php?post=101470352130.

132 Ryan Tate, *Facebook's New "Privacy" Scheme Smells Like an Anti-Privacy Plot,* Gawker, December 2, 2009, available at http://gawker.com/5417145/facebooks-new-privacy-scheme-sme.

133 *See* Mark Zuckerberg, *An Open Letter from Mark Zuckerberg,* FACEBOOK BLOG, September 8, 2006, at http://blog.facebook.com/blog.php?post=2208562130, announcing the creation of a group called "Free Flow of Information on the Internet" for those dedicated to it. This principle, of course, is about as vague and safe as a politician's self-professed love of mother, country, and apple pie, while its *implementation*, with defaults that do not seem to respect any norms of distribution, tell a slightly different story.

surprisingly, designing a system on the principle of "Share Everything" causes users to share more than they might initially suppose.

From the perspective of Facebook, however, this seems like a feature, not a bug. Facebook's value derives from its users data. An architecture that enables sharing would seem to enhance profitability, while an architecture that restricts sharing would seem to diminish it. However, the reality is subtler than that. While in the short run the "Share Everything" model makes sense, in the long run Facebook's interests parallel those of its users. The counterintuitive truth is that Facebook benefits when it facilitates the privacy practices of its users. It *needs* a strong privacy architecture to survive.

When users experience a privacy violation, they close down, clam up, and may even (in extreme cases) deactivate their accounts, all of which are unconditionally *bad* for Facebook. The current Facebook policy that privileges sharing is premised on the erroneous assumption that as it becomes easier to share information people will always share more. That's true, but only up to a point. As it becomes easier to share information, people will share more, until they share too much, experience an "ick" moment, and clam up. In other words, with the present Facebook design, people share more and more until suddenly they share less. "Ick" moments aren't in Facebook's interests either. If users are confident in their contexts they will trust Facebook more, and though they may reveal less information to any one particular Friend they still necessarily reveal everything to Facebook.

Facebook's business model depends on its users sharing information through the site. People only reveal information to Facebook if they trust Facebook to protect their privacy. The more robust the privacy architecture, the safer the user feels; the safer the user feels, the more the user trusts Facebook; the more the user trusts Facebook, the more they share and everybody wins.[134]

B. WHY MARKETS WON'T WORK

Markets may provide means by which individuals manage their privacy. Just as they may switch vacuum cleaners if they find their current brand insufficiently powerful, users might simply stop using a technology if they believe its costs to their privacy outweigh its other benefits. No laws prohibit the building of glass houses because the market's aversion does the job. Devout cyberlibertarians might argue that if users really care about privacy they will simply stop using Facebook or jump to the first privacy-sensitive competitor that comes along. If the collapse of contexts is really such a big deal, Facebook should respond to the market's demand for an architecture that affords contextual integrity, and trust the invisible hand to reconstruct contexts on its own.

Faith in such solutions, though, is predicated on certain presumptions, including the classical economic premise that individuals make choices (including those affecting their privacy) according to their rational self-interest. Some economists who study privacy tend to assume that "individuals are forward lookers, utility maximizers, Bayesian updaters who are fully informed or base their decisions on probabilities coming from known random distributions."[135] In English, this means that individuals fully understand the implications of their practices on their present or future privacy by instantaneously calculating the equilibrium of the payoffs and consequences of a given disclosure. According to classical economists, privacy practices are just normal transactions, driven by rational cost-benefit analyses. There is even an equation modeling the tradeoffs of "privacy transactions":[136]

---

134 Unless, of course, users are tricked into a false sense of security. Obviously, Facebook should not *deceive* users into thinking that the site is safer than it actually is. There is no reason, however, that a better privacy architecture need be deceptive. In fact, a large part of this critique is that the *current* architecture is deceptive and should be revised to more accurately convey the risks of disclosure to the user. There is an entirely separate issue about whether or not Facebook *deserves* the trust of its users, a question that is not explored here.

135 Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making* 26, IEEE SECURITY AND PRIVACY, Vol. 3, 26-33 (2005), available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.

136 Alessandro Acquisti, *Privacy in Electronic Commerce and the Economics of Immediate Gratification* 22, PROCEEDINGS OF THE ACM ELECTRONIC COMMERCE CONFERENCE, 21-29 (2004), available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf.

$$\max_{d} U_t = \delta\left(v_E\left(a\right), p^d\left(a\right)\right) + \gamma\left(v_E\left(t\right), p^d\left(t\right)\right) - c_t^d \quad (1)$$

Of course, people don't *actually* think about privacy this way. Privacy practices are animated by a sloppy muck of norms, expectations, and cognitive biases, not multivariable mathematical models. The decisions that drive privacy transactions are, like all human decisions, "predictably irrational."[137] According to behavioral scientists, there are systemic—meaning both universal and predictable—cognitive biases that affect privacy practices.

In 2004, the behavioral economist Alessandro Acquisti published a paper explaining the "dichotomies between privacy attitudes and behavior that [have] been noted in the literature but never explained."[138] In other words, he studied why individuals (such as Facebook users) who claimed to care about privacy didn't always act as if they did. Acquisti discovered a number of cognitive biases that help resolve the tension between the subjective preferences and the objective affect of users.

Acquisti found that privacy transactions are often characterized by *incomplete information* and *bounded rationality*. Most of the costs of protecting privacy (i.e., time spent adjusting privacy preferences) are immediate and salient, whereas most of the payoffs (i.e., not having contexts collapse) are only felt after the fact. The cognitive imbalance between the salience of immediate costs and the obscurity of future payoffs lead users to systematically underestimate the risks and not accurately express their subjective valuation of privacy.[139] Furthermore, *hyperbolic discounting*—the tendency to discount future events at different rates than near-term events—may impact privacy practices as people "heavily discount the (low) probability of (high) future risks" and regularly underinsure themselves.[140] All of these biases would seem to explain the otherwise counterintuitive finding that the strength of Facebook privacy settings isn't predicted by initial stated user concern for privacy but rather by whether a user has recently experienced an "ick" moment or privacy event.[141]

Additionally, Acquisti found that privacy transactions may be influenced by an *optimism bias*. The optimism bias causes individuals to irrationally believe that a problem which afflicts others will not afflict them. Classic examples include the fact that 95% of students expect to score above the median grade in a class; 90% of all drivers believe they are better than average; and, despite the widespread knowledge that around half of all marriages end in divorce, almost zero percent of engaged couples believe they'll split.[142] Within the domain of privacy, Acquisti found that individuals are not able to accurately comprehend the high risks resulting from cumulative iterations of low-risk activities, such as the "whole risk associated with revealing different pieces of personal information [which is higher] than the sum of the individual risks associated with each piece of data."[143] The optimism bias leads users to routinely underestimate the chances that "it will happen to them" and thus causes them to systemically underinsure their privacy.

Finally, there is the *power of the default*. The power of the default means that sometimes users are simply too lazy, confused, or irrational to make a choice and instead just stick with the default option. The default exerts tremendous power even over decisions normally considered deeply personal. For instance, a study of

---

137 *See generally* DAN ARIELY, PREDICTABLY IRRATIONAL: THE HIDDEN FORCES THAT SHAPE OUR DECISIONS, 2008.

138 *See* Acquisti, *Immediate Gratification, supra* note __, at 25.

139 *See* Acquisti, *Immediate Gratification, supra* note __, at 27.

140 *See* Acquisti, *Immediate Gratification, supra* note __, at 28.

141 Email from Professor Ian Brown to Chris Peterson (September 7, 2008). Rachel and Jess from the case studies didn't think too much about privacy on Facebook until they were confronted with the immediate problem of whether or not to Friend their family members. Many students with whom I have spoken have said that their "privacy event" idea describes their own reactions across many domains of Internet communication—how likely one is to use a real photo on mySpace, how likely one is to reveal their name or location on an Internet messageboard, and so forth. Users make the best decisions, that most closely align with their actual subjective privacy preferences, immediately after experiencing a privacy violation, when the payoffs are finally salient and are understood to outweigh the costs.

142 THALER & SUNSTEIN, *supra* note __, at 32.

143 See Acquisti, *Immediate Gratification*, *supra* note __, at 28 (providing classic example of the "associated risk" bias in smoking, as smokers often don't grasp that the harm of long term smoking is greater than the sum of cigarettes smoked).

Iowa residents showed that even though 97% of respondents favored organ donation in the event of a fatal car crash, only 64% of those who said they would donate exercised the minimal effort to check the box on their drivers licenses.[144] A second study showed that this discrepancy could not be attributed to a spiritual revelation at the DMV. In the first condition, users were asked to check a box if they wanted to donate their organs. 42% did so. In the second condition, users were asked to check a box if they did *not* want to donate their organs. Only 12% checked the box, while the rest "chose" to donate their organs.[145] The effect appears dramatically between cultures that are otherwise very similar. Compare, for example, the 12% rate of organ donation in Germany (where citizens opt-in) to the 99% donation rate in Austria (where citizens opt-out).[146] Of course, the power of the default doesn't just affect how likely one is to give up a liver: it affects the setting (or neglecting) of privacy controls too.

And remember, all of these biases are active and dominant *in familiar environments,* environments that human beings have evolved within and are adept at navigating. Facebook is emphatically *not* such an environment, and so all of these biases are even more powerful. According to Facebook Chief Privacy Officer Chris Kelly, only 20% of Facebook users ever touch their privacy settings,[147] and a 2007 study by the security firm Sophos found that 75% of Facebook users never changed the default setting allowing any member of their network to view everything on their profile.[148] Even if users could level-up into some sort of hyper-rationality, they would still have to contend with Facebook's interface to effect their preferences. Sonia Livingstone describes watching some teenagers struggle with the default privacy settings:

> When asked, a fair proportion of those interviewed hesitated to show how to change their privacy settings, often clicking on the wrong options before managing this task, and showing some nervousness about the unintended consequences of changing settings. . . For example, having set his profile to private, Billy tells me it that cannot be changed to public. Leo wanted his profile to be public, since it advertises his band, yet still says uncertainly: 'I might have ticked the box, but I'm not 100 percent sure if I did'. Or again, Ellie signed up for the London network instead of that for her school when she first joined Facebook and now cannot change this, saying: 'I probably can, but I'm not quite, I'm not so great that, I haven't learned all the tricks to it yet'. The result is that she sees the private information for [many Londoners] but not that of her schoolmates.[149]

Perhaps this is why Gross and Acquisti found that almost a fifth of Facebook users think they have no control over who can read their Facebook profile.[150] Additionally, they found that users did not connect the dots between their privacy preferences and the effects of their disclosure:

> Almost 16% of respondents who expressed the highest concern (7 on the Likert scale) for the scenario in which a stranger knew their schedule of classes and where they lived provide nevertheless both pieces of information.[151]

These data suggest that Facebook privacy decisions are driven by anything but rational consideration. Instead, users routinely, systemically, and predictably underestimate privacy risks and thus underinsure against them, often realizing their mistake only after the fact. The power of the default makes it hard to know what users "really want," because while users affect their settings, settings also affect their users. Finally, even those

---

144 THALER & SUNSTEIN, *supra* note __, at 177.

145 THALER & SUNSTEIN, *supra* note __, at 178.

146 THALER & SUNSTEIN, *supra* note __, at 178.

147 Stross, *supra* note __.

148 *Sophos ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves*, SOPHOS, August 14, 2007, available at http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html.

149 Sonia Livingstone, *Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self- expression* 406, NEW MEDIA & SOCIETY, Vol. 10, 393-411 (2008).

150 Acquisti and Gross, *supra* note __, at 16.

151 Acquisti and Gross, *supra* note __, at 11.

users who do want to move beyond the defaults are often confused by the technical controls and their effects. If users cannot accurately express their actual privacy preferences, then even if Facebook were inclined to listen to its users it would not receive accurate privacy signals. Inaccurate privacy signals create a feedback gap and cause privacy failures.[152]

Market solutions also presuppose a competitive field with sufficiently low transaction costs. If users don't like Facebook's privacy policies, a cyberlibertarian might say, they can walk. No intervention necessary. Don't like the tools Stanley makes? Buy Black and Decker. Problem solved.

Choosing between social networks, however, is nothing like choosing between drills, or cars, or washing machines. People choose social network sites not by the technology but, as danah boyd notes, by "where [their] friends are."[153] Social networks, in other words, are characterized by increasing returns.[154] The tipping point for any new social software comes not when they introduce some new functionality or feature but when a critical mass of users makes it socially sensible to join. Thus, any potential competitor to Facebook faces the crippling disadvantage of *not being Facebook*.

The mere existence of other social network sites like mySpace or LinkedIn doesn't necessarily solve the anticompetitive question. Few use mySpace or LinkedIn or Facebook for the same social purposes, just as no one would rent a taxi when circumstances demanded a limosuine. The services provided by social network sites are complementary, not substitutes. The extraordinarily high transaction costs of porting one's data and contacts between social network sites locks users into Facebook, "empowers the site owner and disempowers the user,"[155] and further discourages competition. And even if data portability laws were enacted, there is every reason to believe that porting data between social network sites would cause more privacy problems than it would solve.[156]

The lack of meaningful competition, data portability, or usable privacy settings means that the only effective "market" solution to Facebook privacy problems is to deactivate one's account, an untenable option for the digital natives who rely on Facebook to build social capital.[157] Many users find Facebook to be as socially indispensable as email or the telephone, meaning they "will put up with a bad deal rather than make the effort of replicating all their personal data and 'friends" connections elsewhere."[158] The network effects of Facebook are tremendous and often overpower deep privacy concerns by users: Acquisti and Gross report that almost 90% of the undergraduates who expressed the *highest* level of concern for threats to their privacy still joined Facebook.[159] Age is a better predictor of whether one joins Facebook than concern for privacy,[160] which points to the existence of a powerful network effect overriding users' personal privacy preferences.[161] The market has yet to provide a solution to Facebook privacy problems, and all of the above are but a few reasons to suspect that it can't.

---

152 *See* Grimmelmann, *Saving Facebook, supra* note __, at 1178-1179 ("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 how much privacy users expect when they sign up for a social network site and how much they get. 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.")

153 boyd, Taken Out of Context, *supra* note __, at 108.

154 *See, e.g.,* BRIAN W. ARTHUR, INCREASING RETURNS AND PATH DEPENDENCE IN THE ECONOMY (1997).

155 Lilian Edwards and Ian Brown, *Data Control and Social Networking: Irreconcilable Ideas?*, *in* HARBORING DATA: INFORMATION SECURITY, LAW AND THE CORPORATION, 226 (Ed. Andrea Matwyshyn, 2009).

156 *See* Grimmelmann, *Saving Facebook, supra* note __, at 1193.

157 danah boyd and Nicole Ellison, *Social network sites: Definition, history, and scholarship, supra* note __,

158 Lilian Edwards and Ian Brown, *supra* note __, at 226.

159 Lilian Edwards and Ian Brown, *supra* note __, at 226.

160 Acquisti and Gross, *supra* note __, at 5.

161 *Cf* Acquisti and Gross, *supra* note __, at 12 (". . . privacy concerns may drive older. . . college members away from Facebook, [but] even high privacy concerns [are] not driving undergraduate students away from it.")

C. WHY LAW WILL ONLY WORK SOMETIMES

Regulation is a favored tool of policymakers. However, like market solutions, legal interventions are predicated upon a certain set of presumptions that may or may not hold true in the social network space. Policymakers must not only engage with the social dynamics of Facebook, as Grimmelmann has noted, but also with its *environmental* dynamics.

This argument isn't anything new. Lawrence Lessig has extensively discussed the difficulty of taking legal principles developed within the architecture of the physical world and translating them to the architecture of the digital world.[162] But it is still worth emphasizing just *how different* the informational environments of the physical world and Facebook are. Part III.B outlined some of these distinctions already, but let us examine further a single case example, the case of publishing.

Even the most ardent privacy scholars don't usually think of published content as private. Indeed, Warren and Brandeis, in their headlong dash to develop a right to privacy, paused just long enough to admit "[t]he right to privacy ceases upon the publication of the facts by the individual."[163] Warren and Brandeis presumed the act of publication communicated an author's intent to make it public. This made sense when publishing was difficult, because it was safe to assume that if someone spent the time, money, and effort to crank out a pamphlet on a printing press they intended it to be seen by as many people as possible.[164]

New media explode this assumption by drastically cutting or even reversing the costs. It is a mistake, the technologist Clay Shirky argues, to assume that just because content is made broadly accessible that the author intends it to be broadly accessed:

> In a world where publishing is effortless, the decision to publish something isn't terribly momentous.[165]
>
> We misread these seemingly inane posts because we're so unused to seeing written material in public that isn't intended for us.[166]
>
> The distinction between communications and broadcast media was always a function of technology rather than a deep truth about human nature.[167]
>
> [But community] now shades in audience; it's as if your phone could turn into a radio station at the turn of a knob.[168]

In the age of Warren and Brandeis the technological affordances of the time implied that if one published something one wanted it public. On the Internet in general, and on Facebook in particular, those converse is true: publishing is costless, and delimiting disclosure is difficult.

But what is factual has never been a particularly good guide to what is legal. American privacy law presumes that "[t]here can be no privacy in that which is already public."[169] According to Friedrich, all information is either secret or public, and "[in] the legal perspective the problem of privacy is primarily that of protecting the private sphere against intruders, whether governmental or other."[170] This public / private dichotomy can be called the "secrecy regime", because courts "sometimes seem to believe that once a personal fact

---

162 *See generally* Lawrence Lessig, *architecture of privacy*, *supra* note __; Lessig, *code*, *supra* note __ (especially chapter nine).

163 Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 218 (1890).

164 *See e.g.* Shirky, *supra* note __, at 70-80, comparing the impact of publishing on the scribal tradition to the impact of new media on journalism.

165 Shirky, *supra* note __, at 79.

166 Shirky, *supra* note __, at 85.

167 Shirky, *supra* note __, at 86.

168 Shirky, *supra* note __, at 89.

169 DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET 161 (2008).

170 Carl J. Friedrich, *Secrecy vs. Privacy, The Democratic Dilemma*, *in* NOMOS XIII 105 (John Chapman ed., 1971).

is known by even a few people, there's no longer a privacy interest in it."[171] The secrecy regime only works inasmuch as the individual is interested in secluding themselves, but Facebook users don't retreat from the complexity of advancing civilization,[172] they *embrace* it. As Grimmelmann writes, "the first task of technology law is always to understand how people actually use the technology,"[173] and no one on Facebook is *trying* to keep information secret. That's not the *point* of Facebook.

For architectural, social, and political[174] reasons, relying on law to fix problem of privacy on Facebook is an iffy approach. Law can solve some, but not all of the problems. Interventionists should keep two general guidelines in mind:

Law Can Help Protect Users From Facebook And Each Other

In these circumstances, law protects privacy best when it prescribes certain standards of information gathering and exchange that accord with norms of distribution. Law can require Facebook to share information in certain ways and forbid it from sharing information in other ways. It can proscribe other users from publicizing certain information and provide remedies if they do it anyway. James Grimmelmann has already developed an excellent set of legal interventions that can incrementally improve privacy on social network sites.[175] Examples include:

- Public Disclosure Torts. Grimmelmann advocates a public disclosure tort based on Lior Strahilevitz's social network theory of privacy.[176] Strahilevitz argues that it is possible to determine, based on the study of real-life social networks, when information "crosses" from one group (or context) of individuals to another. For example, an individual speaking at an HIV support group might not be technically secret but may reasonably expect that her speech remain within the group.[177] Under Strahilevitz's framework, such an individual would retain an expectation of privacy in her speech. That expectation might be broken by another individual—for example a local television reporter—broadcasting the information to people *outside* of the social network of the HIV support group.[178] Thus, if user A reveals information to a small set of other users, including user B, and user B subsequently publicizes that information to a broader community, user B could be liable.[179]

- Technical Controls Constituting Fourth Amendment Expectations. Certainly, much of what is posted to Facebook is fair game for police: no extraordinary steps were required for the arresting officer to divine the Facebook Friendship of Chiles and Gartner. However, if users take affirmative steps to protect their information by employing technical controls, both Grimmelmann and Matthew Hodge recommend they be required to present a search warrant.[180] As Hodge notes, "a user is entitled 'at least, to the modicum of privacy its design affords, certainly to the extent that he will not be joined by an uninvited guest or spied upon by probing eyes.'"[181]

---

171 Grimmelmann, *Saving Facebook, supra* note __, at 1195.

172 Warren and Brandeis, *supra* note __, at 196 ("The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual. . . invasions upon his privacy [subject] him to mental pain and distress, far greater than could be inflicted by mere bodily injury.")

173 Grimmelmann, *Saving Facebook, supra* note __, at 1139.

174 After losing a lawsuit over its intrusive Beacon program, *infra* at __, Facebook hired lobbyists to affect future privacy policy. *Facebook hires team to lobby governments on privacy issues,* THE TELEGRAPH, December 29, 2009, http://www.telegraph.co.uk/technology/facebook/6904309/Facebook-hires-team-to-lobby-governments-on-privacy-issues.html.

175 Grimmelmann, *Saving Facebook, supra* note __, at 1195.

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

177 Lior Strahilevitz, *A Social Networks Theory of Privacy, supra* note __, at 942 (discussing Multimedia WMAZ v. Kubach, 443 S.E.2d 491).

178 *id*

179 *Cf* Grimmelmann, *Saving Facebook, supra* note __, at 1196.

180 *See, e.g.,* Grimmelmann, *Saving Facebook, supra* note __, at 1197.

181 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, 110 (2006).

- Rights of Publicity. Perhaps the most famous flareup on Facebook was that of its Beacon program,[182] whereby participating partners could collect information about a Facebook user on their site (e.g. that Joe just rented *Biodome*) and post that information to the user's Friends via the News Feed (e.g. "Joe just rented *Biodome!* Stop by Blockbuster today!"). In addition to the potential embarrassment associated with sharing purchasing habits with everyone on Facebook,[183] Grimmelmann and others argue that Beacon inappropriately capitalized on the user's commercial rights to their name and likeness.[184] There is also an excellent case to be made under Strahilevitz's framework for a disclosure problem here: I may not want Mary to know what I'm telling Merck.

These are all reasonable steps that would help shore up the norms of distribution by restoring some method to the madness of Facebook.

Law Can't Help Protect Users From Themselves

Unfortunately, these interventions can't solve all of the problems on Facebook. In fact, they are helpless before arguably the *biggest* enemy of privacy Facebook users face: themselves.

None of the above interventions, for example, would assist anyone in our case studies, with the possible exception of preventing the public disclosure of personal photos in the *Daily Mail*. Recall that the case studies were not characterized by one user or corporation "invading" the "secret" space of another, but rather by a user finding it difficult to manage their self-presentation and losing control of contexts.

Law can't solve this problem because it is not the sort of problem law solves. Law can't help users make better decisions. As Lessig has noted, law functions primarily as a *post hoc* constraint, not an *ex ante* heuristic.[185] It can't overcome the behavioral biases that lead users to undervalue their privacy or misapprehend the reach of their disclosure. Law can't restore the missing or misleading architectural heuristics or repair the decisional environment of Facebook that cause slips in self-presentation.

D. HOW CODE COULD HELP

As a form of architecture, code functions both as an objective constraint limiting behavior[186] and a subjective heuristic guiding behavior.[187] Code affects all behavior online, because "technology is not neutral. Each technology has properties—affordances—that make it easier to do some activities, harder to do others. The easier ones get done, the harder ones neglected."[188] The design of Facebook doesn't afford contextual integrity because its technological fictions make it difficult for users to respect norms of distribution and appropriateness.

It doesn't have to be this way. Friendships are flat, audiences invisible, and defaults counterintuitive not because of any law of man or nature but because Facebook designed them to be so. The architecture of an online space, unlike the architecture of the physical world, can be easily changed. Lessig wrote that "we don't

---

182 *Facebook Beacon,* WIKIPEDIA, http://en.wikipedia.org/wiki/Facebook_Beacon.

183 *See, e.g.,* Jack, to Michael Arrington, *Facebook Privacy Issue Won't Die,* TECHCRUNCH, http://www.techcrunch.com/2007/11/26/facebook-privacy-issue-wont-die/#comment-1795020 (November 26, 2007) ("OMG. Facebook is publishing users' private information. I just joined a STD dating site named pozgroup.com. If they are partnered with facebook by any kind of way, and facebook publishs my disease to the public, I have to die.") *See also* Jonathan Trenn, *Facebook Beacon isn't in the user's interest (that means you)*, MARKETING CONVERSATION, November 24, 2007, http://marketingconversation.com/2007/11/24/facebook-beacon-inst-in-the-users-interest-that-means-you/.

184 Grimmelmann, *Saving Facebook, supra* note __, at 1197.

185 *See, e.g.,* Lessig, Code, *supra* note __, at 340. Of course, law is much more than a mere set of commands—it has expressive and constitutive functions as well. *See e.g.* Ryan Goodman, *Beyond the Enforcement Principle: Sodomy Laws, Social Norms, and Social Panoptics,* 89 CAL L. REV. 664.

186 *See, e.g.,* Lessig, *id.*

187 *See, e.g.,* Lior Strahilevitz, *Charismatic Code, Social Norms, and the Emergence of Cooperation on the File-Swapping Networks,* 89 VA. L. REV. 505, available at http://ssrn.com/abstract=329700.

188 DONALD NORMAN, THINGS THAT MAKE US SMART 243 (1993).

find cyberspace, we build it, and saying that this is how cyberspace is is not to say that this is how cyberspace has to be."[189] The same might be said of Facebook.

This is not to say that *privacy* can be "built" or "architected." Privacy is lived and practiced, not designed on blueprints and hammered into shape. When people practice contextual integrity they respect the norms incident to their immediate social situation. They don't try to develop comprehensive rules that could describe any social situation they might ever encounter in the future. James Grimmelmann is right to point out that it is "deeply alien to the human mind to manage privacy using rigid *ex ante* rules."[190] What's more, superbly powerful and precise technical controls would be too unwieldy and difficult for anyone to actually use.[191]

The code solution to Facebook's privacy problem isn't to continue the granularity arms race. Infinitely precise technical controls aren't helpful to (or usable by) anyone. But there is another component to this failure of privacy practices, and that is the fact that these technical controls are employed within an environment lacking the architectural heuristics that inform privacy practices. The failure of Facebook's privacy tools has less to do with insufficient technical controls than with its deficient privacy environment.

To understand the distinction, think about privacy in spoken communication. There are speech privacy practices, practices that respect norms of distribution and appropriateness. Changing volume is a privacy practice. Raising one's voice implies that one means to be heard, while lowering one's voice implies that one means to confide. This is a kind of "technical setting" on privacy in speech.

However, the privacy practice of changing volumes presupposes two things about the properties of the space in which one speaks. First, respecting norms of appropriateness requires visible audiences so that one may situate oneself normatively. Second, respecting norms of distribution presumes that one can accurately calibrate the volume of one's voice to reach the desired audience and no further. These properties are presumed because they are integral to the architecture of the physical world.

Of course, Facebook *doesn't* have these properties. Facebook provides people with powerful privacy tools but not an environment that privileges privacy. When a Facebook user uploads a photo album, in theory they can set access permissions to that album down to the level of individual Friends. That's a privacy practice. It often fails, partially because it is difficult to set *ex ante* rules, but also because Facebook's design withholds from users the architectural heuristics they rely on in the real world. In the physical world, when one is deciding whether to disclose a photo, one is aware of their social situation, who is looking on, and who is listening in. Facebook, though, doesn't make this obvious at the point of upload or any time thereafter. Often users don't realize which Friends can see which photos until after they've already left a comment.

---

189 Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869, 888 (1996), available at http://ssrn.com/abstract=41681.

190 Grimmelmann, *Saving Facebook, supra* note __, at 1185.

191 *Cf* Grimmelmann, *Saving Facebook, supra* note __, at 1186 ("We think about privacy in terms of social rules and social roles, not in terms of access control lists and file permissions. 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. 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."); Clay Shirky, *RELATIONSHIP: A vocabulary for describing relationships between people*, MANY2MANY CORANTE, March 16, 2004, http://many.corante.com/archives/2004/03/16/relationship_a_vocabulary_for_describing_relationships_between_people.php. ("Take any moderately complex real-world work relationship of yours and try to fit it here. We start off with employerOf/employedBy, models of clarity, but what if you are employed by a colleague you collaborate with?. . . The whole list is like that -- we get friendOf, then for a semantic richness bonus, closeFriendOf. But if we're going that route, where's veryCloseFriendOf? sleepsWith? usedToSleepWith? Where's wentToHighSchoolWith?. . . The RELATIONSHIP list should make it obvious that explicit linguistic clarity in human relations is a pipe dream."); Email from danah boyd to Chris Peterson (November 9, 2008)("Those lists are a disaster. There are certain relations you can clearly mark—biological family for example. But people's relations to others are much more nuanced than that. If you look at what groups they create on LJ, they make a "Friends" group and then they make "Everybody but X" groups. It's pretty funny. Those models are only good when they are flexible. When they are written into stone, they fall apart in implementation.)

Privacy practices cannot be analyzed apart from the environment wherein they occur,[192] and the Facebook environment, as currently architected, is set against privacy practices.[193] Its design cripples the use of any technical controls as privacy practices before the user even begins by desituating users, decontextualizing information, disrespecting norms, and generally making it impossible for users to use what few tools they have. On the other hand, code that situates users, contextualizes information, and respects norms makes it easier for users to use the tools at their disposal.

Code also boasts strategic advantages as a solution. For example, it is easier to implement, self-executing, and universal when compared to law.[194] Moreover, good code facilitates market responses, as an architecture that helps users overcome their cognitive biases would result in more accurate privacy signals and a tighter feedback loop.

Bigger, better privacy settings won't solve the problem on their own: no social network site has more robust, diverse, granular, or powerful privacy controls than Facebook, yet it remains plagued by privacy problems. Using code to reconstruct context means building not only on better privacy controls but also providing a better environment within which they may be employed. Code can make it easier for users to respect norms of distribution and appropriateness by making information flow intuitively throughout Facebook. The goal should be, as Irwin Altman put it, to translate "the concept of privacy and its associated mechanisms [into] design principles that reflect changing social interaction."[195]

V. RENOVATING FACEBOOK'S PRIVACY ARCHITECTURE

A. GUIDING PRINCIPLES

It is extraordinarily difficult to design good privacy environments. Different sites require different solutions depending on different uses: the sort of decisional environment that would suit the use of Facebook might be overkill for a user of LinkedIn and might not be enough for mySpace. However, there are broad principles that might guide specific solutions. The problems of privacy on Facebook occur mostly because technological fictions disrespect norms of distribution. Flat Friendships do not accurately describe social relations, Invisible Audiences prevent users from tailoring their presentation to fit their situation, and Strange Sharing Defaults broadcast user information to complete strangers.

If the problem of privacy on Facebook arises from this tension between user expectations and the actual dynamics of the design, the system should be redesigned to respect user norms. Users must have both the tools to protect their privacy *and* an environment that provides them with sufficient architectural heuristics to employ these tools effectively. As Irwin Altman, the great psychologist of design, wrote:

> A general principle is that we should attempt to design responsive environments, which permit easy alternation between a state of separateness and a state of togetherness. If privacy has a shifting dialectic quality, then, ideally, we should offer people environments that can be responsive to their shifting desires for contact or absence of contact with others. . . The logic of our framework calls for more use of changeable environments so as to permit the greater responsiveness to changing needs for privacy.[196]

---

192 ALTMAN, *supra note* __.

193 *Cf* Lessig, *Reading, supra* note __, at 888 ("For the openness of this architecture means this: That there is no "natural" or simple or "automatic" way to keep people out, because there are no natural or real borders that close off access to those who should not have access. If borders in cyberspace are not walls, if cyberspace is set against walls, if people can enter as they wish, or as who they wish, then there is no simple way to select who should go where. In the terms that I have offered, there is no architecture to zone people into their proper place.")

194 Edwards & Brown, *supra* note __, at 223 ("Adjusting code is a far more effective privacy-protection mechanism than adjusting the text of contractual privacy policies, for the very obvious reason that conditions imposed by code cannot be "breached" as such (code can of course be hacked, but this is likely to be beyond the competence of most). Code is also a far more efficient way to regulate norms consistently in a transnational environment than law, even privately-ordered law such as contract. The same Facebook code can run in the UK and the USA enforcing the same privacy norms. By contrast privacy policies and terms and conditions may need adjustment to reflect individual national laws.")

195 ALTMAN, *supra* note __, at 209.

196 ALTMAN, *supra* note __, at 207.

> The designers need to deal with the behaviors that users employ to achieve desired levels of interaction. They should ask, for instance, How are territories used? What mechanisms and combinations of mechanisms are employed to regulate social interaction? These questions are behavioral and focus on the user as an active, coping organism that interacts with and employs the physical environment and other behaviors in various combinations. Thus these design questions imply the theme of creating responsive environments that users can interact with and that become extensions of their behavioral repertoires.[197]

Enacting these principles would help "transform difficult tasks into easy ones"[198] and enable users to more easily practice privacy on Facebook. The following sections revisit the technological fictions and describe some ways in which they might be redesigned.

B. THE WISDOM OF FRIENDS: LOOSELY TYPED PRIVACY CLUSTERS

Recall the technological fiction of Flat Friendships. Though users tend to only Friend people they know, and thus bring to Facebook a whole bundle of norms and roles and expectations, Facebook ignores that which preexists it and treats all Friendships equally. Friendship does not resemble any sort of friendship that actually exists and disempowers users by removing their ability to tailor disclosure to contexts. Rachel doesn't think she can differentiate between the information she broadcasts to her college friends and the information she broadcasts to her grandmother. She might like to create different groups or types of Friends and demarcate her self-presentation along these lines.

As a matter of fact, she can, by leveraging a little known and less used feature called the "Friends List." Launched in March 2008, the Friends List feature allows users to create groups of their Friends. Clicking the "Friends" link on the top navigational bar brings users to a page where they may make a new list and select which of their Friends should be placed within that list. Users may then choose which Lists may access which data. For example, a user might grant her "College" list access to a photo album filled with pictures of drunken debauchery but not the "Family" list. A more powerful version of the Friends List feature could allow users to construct very different identities or "personas" for each list.[199]

The human-computer interaction literature supports this basic approach. For example, Lai and Patil conducted a study where they asked users of a small social network application to set privacy permissions that controlled the access different contacts had to personal information stored in the network, such as cell phone numbers, AOL Instant Messenger handles, and personal calendars.[200] Users could differentiate their disclosure by individual, by custom-made groups, by a "Team" mode dictated by the application, or to share "globally" with the entire network. 70% of users managed their permissions at the group level.[201] Lai and Patil report that:

> Participant feedback indicates that the preference for Groups was driven primarily by the fact that it provides enough flexibility for controlling access to personal information, without requiring too much burden to set up and configure. Participants indicated that Global and Team modes weren't flexible enough, while Individuals required configuring more details than necessary. . . The average number of groups created was 4 [and we] found a lot of

---

197 ALTMAN, *supra* note __, at 212.

198 DONALD NORMAN, THE DESIGN OF EVERYDAY THINGS 188 (1988).

199 *See also* Aaron Shelmire, Social Networks and the Professional/Private Life Boundary, (unpublished graduate research conducted for Professor Lorrie Cranor at Carnegie-Mellon University, on file with the author); Jason Hong & Giovanni Iachello, *End-User Privacy in Human–Computer Interaction*, FOUNDATIONS AND TRENDS IN HUMAN–COMPUTER INTERACTION. Vol. 1, No. 1, p. 1–137, (2007), at 53 ("The concept of profiles has been further developed into the more general idea of "identity management." Here, users have several identities, or "personas," which can be used to perform different online transactions. For example, users could have an "anonymous persona" to surf general web sites, a "domestic persona" for accessing retail web sites, and an "office persona" for accessing corporate intranets. Decoupling personas from individuals can reduce the information collected about a single individual."); danah boyd, Faceted/ID, *supra* note __.

200 Jennifer Lai & Sameer Patil, *Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application*, PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (CHI '05), p. 101-110 (2005).

201 Lai and Patil, *supra* note __, at 104.

> commonality among group definitions. Typically, specified groups exhibited a concentric circle pattern with less and less awareness being shared as one moved away from the center. In some cases the center was "family" and in others it was "team." [202]
>
> Defining permissions at group level appears to provide the flexibility needed to appropriately manage the balance between awareness and privacy without undue burden.[203]

A study conducted by Olson and company discovered similar "clusters" within user contacts.[204] According to Hong,

> Olson et al. probed information sharing practices in interpersonal settings. They surveyed the propensity to share information such as availability to communication, contact information, and personal communication preferences with other people. Olson et al. identified clusters, based on the type of information respondents would share and the recipient of the information (i.e., family and friends, close colleagues, remote colleagues, and others). Expectedly, Olson et al.'s study showed that individuals would share more sensitive information with closer acquaintances.[205]

The research supports the existence of socially and situationally meaningful privacy clusters. Users don't need to attempt the (impossible) task of exactly replicating each real-life friendship on Facebook, they just need to differentiate their disclosure along the lines of privacy clusters.

Yet despite this obvious instrumentality, Friends Lists remain chronically underused. This discrepancy between the theoretical utility of the Friends List and the actual underutilization of the Friends List as a way to create contexts seems to have two causes. First, few people seem to be aware that the Friends List feature can be used to manage impressions, personas, and privacy.[206] It is not intuitively understood as a mechanism for impression management. Facebook does not clearly indicate that the Friends List can be used to practice privacy, and most users don't seem to have figured it out on their own.

Second, even if users realize that they can use Friends Lists to manage their privacy, Facebook does not facilitate the process. When users create a new Friends List, they are greeted by two things: a blank white box and a list of every single Friend they have on Facebook. It is essentially impossible to look at a list of hundreds of Friends and try to recreate privacy clusters out of whole cloth with zero situational or social guidance. In other words, the fact that Friends Lists are not often employed as tools to help practice privacy says less about their potential utility and more about their current implementation, which Grimmelmann has characterized as an "interface failure."[207]

Facebook could very easily relaunch the Lists and promote them as a mechanism to circumscribe privacy clusters.[208] It could explicitly publicize them as impression management tools to keep one's boss from seeing the same content as one's roommate. If its privacy utility were made more obvious, users like Rachel might rush to adopt a solution that could allow them to disclose very different things to their grandmother than to their drinking buddies.

---

202 Lai and Patil, *supra* note __, at 106.

203 Lai and Patil, *supra* note __, at 108.

204 J.S. Olson et. al., *A study of preferences for sharing and privacy*, PROCEEDINGS: CHI '05 EXTENDED ABSTRACTS ON HUMAN FACTORS IN COMPUTING SYSTEMS (2005), available at http://research.microsoft.com/en-us/um/people/horvitz/privacy_chi2005.pdf.

205 Hong & Iachello, *supra* note __, at 29.

206 For example, two leading cyberlaw scholars who have written extensively about Facebook were asked about the Friends List feature during the course of research. The first used it, but only as a way to make mailing lists, so that he could send out communiques to different groups if he was in the area for a book talk, conference, and so forth. The second was completely unaware that it existed. If the experts in the field don't recognize it as a way to manage privacy, what hope does the average user have?

207 Interview with James Grimmelmann, *supra* note __.

208 *See* Lai and Patil, *supra* note __, at 108 ("Our findings provide strong support for providing grouping functionality in awareness systems for *more than contact list organization*." [emphasis added])

Facebook could also help users overcome cognitive barriers by making it easier for them to recreate social contexts online. It could, for instance, perform basic network analysis on a user's network to inform them of what clusters may already exist, and perhaps to create default Friends Lists for them automatically.[209] After all, Facebook knows the political leanings, musical tastes, shared links, entrance and exit routes, posting patterns, and network structure of everyone on Facebook. Facebook knows the degree to which a user's friends are homophilous or heterophilous, who is Friends with whom, and how much sharing goes on between a user's mutual Friends. In many ways, Facebook knows more about its users' social networks than do the users themselves. If Facebook wished to design for more usable privacy, it could harness the knowledge in the network and create default groups that mimicked preexisting social contexts based on the massive quantity of data it has collected about user social networks.[210]

For most of its history the social homogeneity of Facebook's users helped protect contextual integrity and made robust privacy settings redundant. There was no need to discriminate between social contexts when only college students were members of the site and everyone was governed by the same college norms. In an age when everyone and their grandmother is joining Facebook, this approach is no longer sufficient to preserve contextual integrity.

Friends Lists can restore spatial separation to social situations. In the physical world, Stokely Carmichael could choose different voices to appeal to different norms, and he could do this because the separation of spaces allowed him to distinguish between audiences.[211] Broadcasting, however, removed the walls separating the norms, and Carmichael could no longer target his speech using the guidelines of space. If the Friends List were redesigned to be a more intuitively useful impression management system, they could keep social contexts apart and be invaluable to the practice of privacy.

C. RESTORING A SENSE OF PLACE: FEEDBACK, SALIENCE, AND VISIBILITY

Restoring structural separation to social situations and contexts won't itself solve the crisis of self-presentation because users must still contend with Invisible Audiences. Often it is impossible for a Facebook users to perceive how or to whom they present themselves. Facebook suffers from what Donald Norman might call the "gulf of Evaluation." As Norman explains:

> There are several gulfs that separate mental states from physical ones. Each gulf represents one aspect of the distance between the mental representations of the person and the physical [states] of the environment. . . .Does the system provide a representation that can be directly perceived and that is directly interpretable in terms of the intentions and expectations of the person? The Gulf of Evaluation reflects the amount of effort that a person must exert to interpret the physical state of the system and to determine how well the expectations and intentions have been met.[212]

The gulf of Evaluation on Facebook is caused by the disconnect between the user's imagined audience and the user's actual audience. For example, suppose a user posts a photo album. If and when a user sets the privacy preferences at the point of upload, they are never directly told who can see those photos. There is a feedback gap where there should be a loop. danah boyd describes how Facebook users often find that they

---

209 *See* Lai and Patil, *supra* note __, at 108 ("Configuration burden could be further reduced by providing templates of settings for commonly used group. . . Defaults for templates could be based on a quick user study of the target population. . . Since the majority of users rarely modify default settings, getting defaults right ensures a balanced privacy-awareness setting from the outset. Even if only 75- 80% of the defaults are appropriately set, the user is perhaps more likely to fine-tune the rest. Setting defaults to broad- cast more awareness information than necessary can undermine individual privacy, and may lead to underutilization (or even abandonment) of the system."); NORMAN, POET, *supra* note __, at 157 ("Even when designers become users, their deep understanding and close contact with the device they are designing means that they operate it almost entirely from knowledge in the head. The user, especially the first time or infrequent user, must rely almost entirely on knowledge in the world. That's a big difference, fundamental to design.")

210 *See also* danah boyd, Faceted/ID, *supra* note __, at Chapter 8 (proposal for detecting and developing contexts using software tools).

211 *See* MEYROWITZ, *supra* note __, at 35 ("The physical barriers and boundaries marked by walls and fences as well as the passageways provided by doors and corridors directed the flow of people and determined [interactions].")

212 *See* NORMAN, DOET, *supra* note __, at 50-51. Norman also identifies as "gulf of Execution," which he identifies as "[the] difference between the intentions and the allowable actions." (*id).* Insufficient privacy controls are a gulf of Execution.

could access content not intended for them, or that their intended audience did not match their actual audiences:

> Over and over again, I interview teens (and adults) who think that they've set their privacy settings to do one thing and are shocked (and sometimes horrified) to learn that their privacy settings do something else. [People] are often unaware of the visibility of content [and] continue to get themselves into trouble. . . [213]

Invisible Audiences—and the resulting absence of feedback, visibility, and salience—are key deficiencies in the Facebook privacy environment. Facebook should make its users more aware of their situation, their audience, and their information. Their present disassociation creates a gulf of Evaluation as users don't connect abstract access privileges to concrete personal data. One step would be to move the privacy settings closer to the content they control,[214] as danah boyd suggests:

> Why are privacy settings still an abstract process removed from the context of the content itself? You should understand the visibility of an act during the moment of the act itself and whenever you are accessing the tracings of the act. [Put] privacy information into the context of the content itself. When I post a photo in my album, let me see a list of EVERYONE who can view that photo. When I look at a photo on someone's profile, let me see everyone else who can view that photo before I go to write a comment. You don't get people to understand the scale of visibility by tweetling a few privacy settings every few months and having no idea what "Friends of Friends" actually means. If you have that setting on and you go to post a photo and realize that it will be visible to 5,000 people included 10 ex-lovers, you're going to think twice. Or you're going to change your privacy settings. . . Why not let them grok how visible their acts are by providing a feedback loop that'll let them see what's going on?[215]

Another software tool that might help users bridge the gulf of Evaluation is the technology of "privacy mirrors" introduced by Mynatt and Nguyen.[216] According to them, the real enemy of privacy practices in ubiquitous computing is not Big Brother but "interfaces that do not give people the needed tools of awareness and control to comprehend and shape the behavior of the system."[217] According to Hong, just as real mirrors are used to police self-presentation in the physical world (informing an individual when her hair is mussed or shirt soiled) "privacy mirrors provide useful feedback to users by reflecting what the system currently knows about them."[218]

Facebook recently implemented an embryonic privacy mirror known as the ViewAs function.[219] The ViewAs function allows users to assume the perspective of one of their Friends and view their own profile as their Friend does. While this function is a step in the right direction, it is not robust enough to really tell users everything they need to know. The ViewAs function only allows one to assume the "mask" of another user for certain content. Clicking the "Video" or "Photos" sections of the profile, for example, removes the mask, and the user is left uncertain about what may be accessed. Furthermore, most users seem completely unaware

---

213 danah boyd, *Putting Privacy Settings in the Context of Use (in Facebook and elsewhere)*, APOPHENIA BLOG, October 22, 2008, http://www.zephoria.org/thoughts/archives/2008/10/22/putting_privacy.html. While the general counterintuitive effects of Facebook privacy controls more accurately consists of as a gulf of Execution, the inability to see the outcome is a gulf of Evaluation.

214 On Facebook, the content (i.e. photos in a photo album) and their controls (i.e. the preferences delegating or withholding access) are almost never located on the same page.

215 boyd, *context of use*, *supra* note __.

216 *See* Elizabeth Mynatt & David Nguyen, *Making Ubiquitous Computing Visible.* ACM CHI 2001 CONFERENCE WORKSHOP: BUILDING THE UBIQUITOUS COMPUTING USER EXPERIENCE (2001), available at http://www2.parc.com/csl/projects/ubicomp-workshop/positionpapers/mynatt.pdf. *See also* boyd, Master's Thesis, *supra* note __, at 55.

217 Mynatt & Nguyen, *supra* note __, at 1.

218 Hong & Iachello, *supra* note __, at 82.

219 The ViewAs can be accessed at http://www.facebook.com/profile.php?viewas=XXX, where XXX is the profile ID number of the individual one wishes to impersonate.

of the ViewAs function. It needs to be made more powerful and accessible before it achieves its true potential.

Attaching access to data more directly as boyd describes and implementing more robust privacy mirrors might help users better visualize potential disclosures. Another option would be to help users visualize *actual* disclosures. That is, Facebook could be designed such that users were informed whenever Friends *actually* accessed their photos, videos, or Wall.

In a series of studies at Carnegie Mellon, Dr. Lorrie Cranor and her team investigated the effect of access feedback on user privacy.[220] Cranor developed applications that tracked user locations based on the GPS in their cellphones. Participants in the experiments, like in the work of Lai and Patil, were then allowed to set very flexible access privileges that controlled which of their contacts could query their location.[221] In one condition, users were given feedback in the form of a list of query requests and whether or not they were granted. In the other condition, users received no feedback at all.

Feedback functionality was a hot commodity among her test group. According to Cranor, the "majority of people in both conditions wanted feedback. . . 76.9% of those who had it were happy they did and 83.3% of those who did not have it wanted it." Feedback was also a crucial component of the privacy process:

> [Most] users are not good at articulating these preferences. The accuracy of the policies they define increases only marginally over time unless they are given tools that help them better understand how their policies behave in practice. . . [Users] often have difficulty anticipating how people they invite will use the application.[222]

> To be effective, user interfaces have to be designed to increase user understanding of how the application is. . . used. We have found that simple bubbles that discreetly pop up (e.g. at the bottom of a laptop screen) to notify users that their location is being requested can go a long way in helping users feel more comfortable with the application.[223]

Cranor and her team also employed several machine-learning algorithms that continually prompted users for new, ostensibly more accurate privacy settings as they continued to use the application. In one condition, users were asked to create access rules. Depending on these rules the algorithm either granted or withheld access. These results were returned to the users and compared with their actual privacy preferences. Users were then asked to revise the rules and run the access program to see how usable the technical controls were. Users generally had 59% accuracy with their initial rule set and 65% with their revised rules. When assisted by an automated case-based reasoning program the accuracy reached 82%.[224]

Cranor's findings also supports one of the key theoretical claims made in Part V.A: namely, that a better privacy architecture is in Facebook's interests. According to her research, 84% of the users who had the feedback functionality believed it made them more likely to share their location through the application.[225] Cranor concludes that:

> [Feedback] does not cause users to lock down or severely restrict their information sharing, certainly a present fear of many [social network sites], but may actually lead to more open

---

220 *See* Lorrie Cranor et. al., *Who's Viewed You? The Impact of Feedback in a Mobile Location-Sharing Application*, PROCEEDINGS OF THE 27TH INTERNATIONAL CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS CHI 2009, p. 2003-2012 (2009), available at http://www.cs.cmu.edu/~sadeh/Publications/Privacy/CHI2009.pdf. *See also* Lorrie Cranor et. al., *Understanding and capturing people's privacy policies in a mobile social networking application*, JOURNAL OF PERSONAL AND UBIQUITOUS COMPUTING, Vol. 13, Issue 6, p. 401-412 (2009).

221 *See* Cranor et. al., *Who's Viewed You, supra* note __. Participants differentiated their disclosure along a wide array of contextual attributes, including the identity of the person making the request, the time of day the request was made, and their current physical location. Participants could also choose to reveal their location with varying degrees of specificity. For instance, a participant located at Harvard could choose to reveal themselves as within "Massachusetts", "Cambridge," or "Lowell House" depending on the contextual attributes.

222 *See* Cranor et. al., *Capturing Privacy Preferences, supra* note __, at 402.

223 *See* Cranor et. al., *Capturing Privacy Preferences, supra* note __, at 406.

224 *See* Cranor et. al., *Who's Viewed You, supra* note __, at 407.

225 *See* Cranor et. al., *Who's Viewed You, supra* note __, at 2009.

> policies. . . Providing feedback to users about when and by whom they have been queried tends to make them more comfortable about sharing location information.[226]

There isn't anything particularly revolutionary about such a feature: OKCupid, Yahoo Personals, Friendster, Orkut, and LinkedIn all offer similar functionality. The participants in Cranor's study overwhelmingly preferred the feedback condition over the no-feedback condition. It made them feel safer and they disclosed more to the site. Implementing feedback seems like a no-brainer.

And yet, such a Viewer Tracking system could clash with strong social norms on Facebook. "Facebook Stalking"[227] remains, to one degree or another, a tolerated practice. Most users know that sometimes Friends of theirs—whether out of earnest interest or lascivious intent—will occasionally linger on their profiles, flip casually through their photos, and browse through their activities. However, if this behavior were shone under the withering light of a feedback system, most users would feel uneasy if they actually realized what they subconsciously knew had been happening all along. As bad as it may be for Rachel to not realize who accesses her profile, she might feel even more uncomfortable if she learned that the creepy kid from her math class was spending hours every day looking at her profile photos.[228]

There is tension, to say the least, between the possibilities afforded by a more robust privacy architecture and the existing social dynamics of Facebook. However, this tension give rise to a serious discussions weighing all the interests of all the parties involved. The Facebook community should be asking tough questions about where the privacy equilibrium is and what tradeoffs need to be made to reach it.

D. SMARTER DEFAULTS: NORMS, NETWORKS, AND PROACTIVE PRIVACY

The final glaring deficiencies in Facebook's privacy environment are the default settings that 80% of users never change. These settings push profile information to all of a user's Friends and their photos and videos to the entire world. These dynamics are completely counterintuitive and in no way respect user norms of distribution. To be sure, defaults can be changed, but they rarely are,[229] leading Brown and Edwards to argue that defaults *disempower* users.[230] Kesan and Shah note a "subtle but profound concern that default settings will not be seen as defaults but accepted as unchangeable. After all, if people don't know about defaults, they will assume that any alternative settings are impossible or unreasonable."[231] This is the heart of the power of the default, and it is the reason that so many users on Facebook find so much of their information traveling through the network in such counterintuitive ways.

The power of the default, however, isn't a moral agent with an inherent intent to trip up users. Facebook may be currently designed with Strange Sharing Defaults that impair the privacy practices of its users, but, as Brown and Edwards explain, "some thought about the effect of defaults could [produce] a more privacy-protective result which [is] nonetheless compatible with the primary social networking focus of the site."

What sort of defaults might facilitate privacy practices? Kesan and Shah insist on what is known as the "would have wanted" standard, loosely defined as "what the parties would have bargained for if the costs of negotiating were sufficiently low."[232] However, as Brown and Edwards suggest, the trouble with this approach is that users wouldn't necessarily have bargained in a manner consistent with their subjective preferences because of the behavioral economics of privacy.[233] The cognitive biases identified by Acquisti would still have been in play at the negotiating table and caused users to misapprehend risks and discount privacy perils.

---

226 *See* Cranor et. al., *Who's Viewed You, supra* note __, at 2011.

227 *Facebook Stalking,* URBAN DICTIONARY, http://www.urbandictionary.com/define.php?term=facebook%20stalking.

228 *See* Grimmelmann, *Saving Facebook,* at 1169-1170.

229 *See* Stross, *supra* note __ (quoting Facebook Chief Privacy Officer Chris Kelly saying that only 20% of users ever touch their privacy settings).

230 Edwards and Brown, *supra* note __, at 224.

231 Jay Kesan & Rajiv Shah, *Setting Software Defaults: Perspectives from Law, Computer Science, and Behavioral Economics*, 82 NOTRE DAME L. REV. 583, 596(2006), available at http://ssrn.com/abstract=906816.

232 Kesan & Shah, *supra* note __, at 618.

233 Edwards and Brown, *supra* note __, at 224.

Though the "would have wanted" standard is often a good rule of thumb, it isn't appropriate for these circumstances.

Instead, *defaults should be modeled after the norms of distribution*. Similarly, *environments should respect architectural heuristics*. Contextual integrity is violated when information does not flow through the network as users expect it should. The obvious solution is to design the network such that information flows consistent with user expectations and norms.

For example, before Facebook phased out regional networks, the defaults effected that when a user joined the Boston network they shared every bit of their profile information with every stranger in the city. No one actually expected or wanted this. It does not accord with norms of distribution. When Facebook eliminated regional networks they took the first step in the right direction. However, it isn't enough: joining any other sort of network (such as a company or campus) still pushes the information out to everyone else at Microsoft or Michigan State. The default could—and should—be set such that information is restricted to Friends only and requires affirmative, conscious action to push information out to the rest of the network. Facebook should respect norms of distribution and restore dead weight to data.

The current defaults also say that when a user joins Facebook their profile is automatically at its most open. Brown and Edwards believe that each new profile, when it is generated, should default to the most private settings. This approach, they argue, "would inform all users that privacy settings do exist, and force them to learn how to make use of them before they moved on to networking."[234] Grimmelmann disagrees, noting that "[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."[235] While Grimmelmann is correct about the ultimate results he is perhaps too dismissive of the instructive merits of the idea. After all, even if Facebook users immediately turn off the privacy settings, at least they learn there *are* privacy settings and have to learn how to use them in order to shut them off. Donald Norman might call this a "forcing function"[236]: like a dead man's switch, the conscious action required to disable privacy settings can only have an educational effect.

Other forcing functions could be employed to consistently "nudge"[237] users into better privacy practices, as Cranor found when popup alerts informed and assisted users.[238] Just as Facebook could perform a network analysis to help users create better Friends Lists, it could also help keep users informed of any changes in the network that may affect their privacy. For instance, suppose Alice is friends with Bob. Bob has recently joined a company network for a company at which Alice may someday want to work. This may change what Alice wants to share with Bob, especially if by default any friends of Bob can see any pictures of Alice. Facebook, of course, is aware of these changes in the network. Facebook might automatically prompt Alice with a notice informing her about the network change, note any implications for their privacy that might result from the change, and provide them with a menu to easily update their privacy settings considering the change. This is just one of many possible instrumentalities that a "smart" network could offer to help users practice their privacy. Such a proactive (as opposed to passive) design would make changing social circumstances more salient to the user and help keep their contexts current.

This might be thought of as an application of "libertarian paternalism"[239] to the problem of Facebook privacy. It doesn't require any mandates, either from the government or the company. Nobody is prohibited from blasting all their personal information to everyone in their network. Nobody is forced to have a private profile. These counterintuitive conventions are just no longer empowered by the default. As a guideline, any

---

234 Edwards and Brown, *supra* note __, at 225.

235 Grimmelmann, *Saving Facebook, supra* note __, at 1187.

236 Norman, *DOET, supra* note __, at 131.

237 *See, e.g.,* THALER & SUNSTEIN, NUDGE, *supra* note __.

238 *See* Cranor et. al., *Capturing Privacy Preferences, supra* note __, at 406.

239 *See generally,* Richard Thaler & Cass Sunstein, *Libertarian Paternalism Is Not an Oxymoron*, 70 U. CHI. L. REV. 1159 (2003). *See also* THALER & SUNSTEIN, NUDGE, *supra* note __.

environment that respects the norms of distribution of the physical world should attempt to replicate the architectural heuristics and communicative properties of the physical world, at least in its default form. Such environments natively support user privacy practices as the power of the default can afford privacy rather than impair it.

CONCLUSION

WORLDS COLLIDE

In an episode of the sitcom *Seinfeld* entitled "The Pool Guy," George becomes upset when Jerry introduces their mutual friend Elaine to George's fiancee Susan. Susan has been outside their social "world," but George fears that if she begins hanging out with his friends it will end poorly for him:

> GEORGE: You have no idea of the magnitude of this thing. If she is allowed to infiltrate this world, then George Costanza as you know him ceases to exist! You see, right now, I have Relationship George, but there is also Independent George. That's the George you know, the George you grew up with -- Movie George, Coffee Shop George, Liar George, Bawdy George!
>
> JERRY: I, I love that George.
>
> GEORGE: Me Too! And he's dying Jerry! If Relationship George walks through this door, he will kill Independent George! A George, divided against itself, cannot stand! [240]

The crisis of self-presentation suffered by George now afflicts all users of Facebook. Like Rachel and her grandmother, George is concerned that walls separating "Independent George" from "Relationship George" will break down, and that when his worlds collide part of his autonomy of identity will die along with it.

Of course, on *Seinfeld* it all works out fine. Susan discovers she doesn't enjoy spending time with George's friends. She stops going to movies with them and no longer chats with Elaine on the telephone. This solves George's problem. He can go to the coffee shop to be Independent George, and back to his apartment to be Relationship George. He can travel between spaces to switch between situations.

On Facebook, it's not so simple. While the properties of George's environment natively support contextual integrity, the design of Facebook collapses contexts. The technological fictions that riddle its architecture prevent users from usefully employing its otherwise powerful privacy tools. The lack of the environmental cues that people use to recognize and define social situations impair privacy practices. George had it easy. Digital natives—and everyone else in the booming social network space—will have a much harder time reconstituting themselves.

But it's not entirely hopeless. If we can see this problem for what it is—a problem of self-presentation, of contextual integrity, and of the environment within which decisions are made—then we can take steps to fix it. Law and code are not powerless here: they can protect user data and provide better architectural heuristics that more accurately inform user decisions. No solution is perfect: law may be too heavy-handed or not powerful enough; code may still confuse or lull users into a false sense of security; and too much fidelity to contextual integrity runs the risk of technological conservatism at the expense of progress.[241] Managed care-

---

240 *Seinfeld: The Pool Guy* (NBC television broadcast November 16, 1995). Fan transcription available at *Seinfeld: The Pool Guy,* SEINFELDSCRIPTS.COM, http://www.seinfeldscripts.com/ThePoolGuy.html. "Independent George" scene available at *Seinfeld: Independent George,* YOUTUBE, http://www.youtube.com/watch?v=SxuYdzs4SS8. Originally cited in Patricia Sanchez Abril, Perspective, *A (My)Space of One's Own: On Privacy and Online Social Networks*, 6 NW. J. TECH. & INTELL. PROP. 73, 84 (2007).

241 *Cf* NISSENBAUM, *supra* note __, at 159 (Noting that a criticism levied against contextual integrity is that "as long as contextual integrity is tied solely to actual practice, as long as it merely defines a heuristic for detecting effectively when novel practices deviate from entrenched norms, it can be judged an instrument of [the tyranny of the normal.]") The News Feed, for example, upended norms of distribution, caused much consternation when it was introduced, and has since become more or less accepted and incorporated into expectations. To privilege contextual integrity is not so much to be anti-innovation, but rather to simply realize that users have certain expectations about information flows, and that there will be privacy problems whenever expectations and reality are not aligned.

fully, however, these solutions can strike the proper balance, harmonize with user expectations and desires, and shore up the rickety privacy architecture of Facebook.