DRAFT - FOR COMMENT

SAVING FACE

The Privacy Architecture Of Facebook

Senior Thesis

University of Massachusetts-Amherst, Spring 2009

Chris Peterson

TABLE OF CONTENTS

Acknowledgements 6

Abstract 7

Introduction: Losing Face 8

Part 1: Facebook and Social Behavior 11

A BRIEF HISTORY OF FACEBOOK 11

1.1: Finding Hotties At Harvard, Keeping Friends At College *11*

1.2: Little Brother Is Watching You: High Schools And Photo Sharing *13*

1.3: Here Comes Everybody: 200 Million users And Beyond *14*

THE SOCIAL PRACTICES OF FACEBOOK 15

1.4: Real Friends And Weak Ties *15*

1.5: Privacy Practices and Concerns on Facebook: Exhibitionists Don't Go 'Ick' *18*

CASE STUDIES 20

1.6: A Series of Stories *20*

Part 2: The Problem of Privacy on Facebook 22

WHAT IS THE PROBLEM? *22*

2.1: Identifying the Interests *22*

2.2: Privacy as Contextual Integrity *23*

PRIVACY, THE ENVIRONMENT, AND THE DYNAMICS OF DISCLOSURE 28

2.3: The Architecture of Privacy 28

2.4: The Privacy Architecture of Facebook 30

FACEBOOK'S COUNTERFACTUAL DESIGN 33

2.5: The Technological Fictions of Facebook 33

2.6: Flat Friendships 34

2.7: Invisible Audiences 35

2.8: Strange Disclosure Defaults 38

Part 3: Reconstructing Collapsed Contexts 39

WHAT SHOULD BE DONE 39

3.1: Why Facebook Should Care 39

3.2: Why Law Won't Work 41

3.3: Why Markets Won't Work 44

3.4: Why Code Could Work 50

CREATING AN ENVIRONMENT THAT PRIVILEGES PRIVACY 54

3.5: Some Guiding Principles For Usable Privacy 54

3.6: The Wisdom of Friends: Loosely Typed Privacy Clusters 55

3.7: Restoring a Sense of Place: Feedback, Salience, and Visibility 61

3.8: Smarter Defaults: Norms, Networks, and Proactive Privacy 65

3.9 The Caveats of Code 68

Conclusion: Saving Face 72

BIBLIOGRAPHY 74

Acknowledgements

Professors Katsh and Gaitenby are great professors, colleagues, and friends. I would like to especially thank Alan for his endless patience as I pitched idea after idea - each less worthy than the last - at him during long afternoons in Gordon Hall. It is hard to imagine a better thesis committee. They were patient with my crossdisciplinary aspirations, recognizing that desperate times call for diverse methods. I am incredibly grateful for their assistance in this project and would love to work with them again.

Professor Jensen here at UMass, Professor Zittrain at Harvard, Professor Brown at the Oxford Internet Institute, and Professor Grimmelmann at NYLS all helped orient me at critical times in my research. Professors Cranor and Acquisti of Carnegie Mellon and danah boyd graciously put up with my pestering emails about their respective works.

Finally, I would like to thank Facebook. Since June 7, 2005, at 12:03 PM PST, for better or for worse, it has been my constant college companion. The last few years were exciting. The next few will be interesting. I don't know what will happen. I can't wait to see.

Abstract

Facebook has grown from a simple social utility for college freshman to the largest social network site in the world. However, its rise has not been without controversy or user dilemmas, the most pressing of which involve problems of privacy.

Surveys and social practices show that users care deeply about their privacy on Facebook. A series of case studies review the privacy violations commonly reported by Facebook users. These data show that the violations are caused by a loss of what the privacy theorist Helen Nissenbaum calls "contextual integrity." The problem of privacy on Facebook is the problem that arises when worlds collide, when norms get caught in the crossfire between communities, when the walls that separate social situations come crashing down. It is, as danah boyd has described, a problem of collapsed contexts.

Lawrence Lessig argued that architecture affords or impairs privacy, and Facebook's architecture uniquely facilitates the breakdown of contextual integrity. Specifically, several technological fictions of Facebook - including Flat Friendship, Invisible Audiences, and Strange Disclosure Defaults - do not respect norms of distribution, hinder the observance of norms of appropriateness, and make it difficult to practice privacy.

It is difficult to reconstruct contexts. Privacy law was developed to protect against intrusions on seclusion and cannot be easily adapted to the problem of collapsed contexts. Market solutions are led astray by cognitive biases and a lack of competition. Code, however, can create a better privacy environment. By building a privacy architecture that is more intuitively navigable and practicable, Facebook can empower its users to reconstruct contexts, practice privacy, and save face among colliding communities.

Introduction: Losing Face

On April 12, 2009, a college junior named Rachel faced a problem that few users of Facebook had ever seriously contemplated. Her Facebook status broadcast her distress out into the electronic ether. "my grandmother just friend requested me," it read. "no. Facebook, you have gone too far!" [1]

Rachel and her grandmother are close. She trusts her grandmother. She confides in her grandmother. She tells her grandmother "private" things. She is certainly closer to her grandmother than 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.* [2]

This thesis is about Facebook. It argues that the world's largest social utility has revolutionized the environment within which people communicate. Specifically, it finds that Facebook challenges intuitive ideas of identity and privacy practices by changing the informational dynamics of the space within which individuals represent and situate themselves. It provides a conceptual framework for understanding the sort of privacy violations that take place on Facebook, explains how the design of Facebook enabled these problems, and describes some concrete steps that might help solve the problem.

---

1 Rachel is not this student's real name, but her status update is real.

2 Personal correspondence with "Rachel."

This thesis contends that Rachel's dilemma, while doubtlessly novel and disturbing to her, is in fact a familiar problem. It is the problem that arises when worlds collide, when norms get caught in the crossfire between communities, when the walls that separate social situations come crashing down. It is, in short, a problem of collapsed contexts.

It is also a problem of privacy, though not of privacy as the law constructs it, for the dominant American legal tradition "recognizes as private only that which is completely secret."[3] Law cannot understand how Rachel can feel that Friending her grandmother compromised her privacy when all of her existing Friends - most of whom she did not trust or confide in nearly as much as her grandmother - had access to the same information. No matter how strongly Rachel feels her privacy was compromised, law does not and cannot imagine how or why.

In order to explain how Rachel's experience might be considered a problem of privacy, this thesis adopts Helen Nissenbaum's model of privacy as contextual integrity. Echoing Goffman's work on social performance and presentation theory, Nissembaum argues that privacy is violated when individuals do not respect social norms of distribution and appropriateness. 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.

These privacy norms arise from expectations about how information circulates in the physical world. The norm of distribution, for instance, presumes a certain informational environment, because the way data flows through any space is in part a function of the architectural properties of that space. Locks forbid entry; walls muffle sound; curtains block prying eyes. This thesis describes how the architectural cues of the physical world inform the privacy practices of individuals.

The architectural properties of Facebook, however, cause contexts to collapse. Information flows outward in unfamiliar ways that don't respect norms of distribution. Individuals cannot differentiate disclosure among their different relationships because all of their information is equally accessible to everyone they know. They cannot tailor their expression to their audience because their audience is invisible. They cannot make sense of a

---

3 See Solove, The Future of Reputation, at 161. See also Section 3.2.

world that automatically broadcasts their information to everyone else. They cannot maintain contextual integrity because everyone they know accesses the same content in the same space at the same time.

This thesis incorporates danah boyd's[4] ethnography of social network sites[5] to find that the chief privacy tensions on Facebook aren't felt between users and governments or corporations but instead between dueling social contexts. Facebook users are not primarily concerned with datamining, advertisers, or any traditional "privacy" violations under the law.[6] Instead, users experience privacy problems on Facebook when counterintuitive dynamics of disclosure collapse contexts by spreading information through the network in ways that do not respect user norms of distribution, as when Rachel worried about her grandmother learning all about college life.

This thesis argues that neither law nor markets can solve this problem. Instead, the power of code[7] should be harnessed to help reconstruct contexts. This does not mean, however, that the solution is to simply build more powerful privacy controls. Privacy controls are good, but they are only half of the problem. Code needs to create a better privacy architecture, or an environment which better enables the practice of privacy. If Facebook were designed to behave more like real life - if the informational properties of Facebook were more similar to the informational properties of the physical world - then users would find it easier to keep their contexts intact, their worlds apart, and their privacy protected.

This thesis is divided into three parts. Part 1 provides a brief history of Facebook, reviews the data on Facebook privacy practices, and chronicles case studies of privacy violations as experienced by Facebook users. Part 2 outlines the theory of contextual integrity, explains the role of architecture in keeping contexts intact, and identifies aspects of Facebook that contribute to their collapse. Part 3 looks at the tools commonly employed to protect privacy, demonstrates why only code can help reconstruct contexts, and advances some general design principles that might assist users in the practice of privacy.

---

4 danah boyd does not capitalize her name.

5 See boyd, "Taken Out of Context."

6 See boyd, "My Friends, mySpace" at 33:00.

7 Meaning computer code, or, in Lessig's terms, "West Coast Code."

Part 1: Facebook and Social Behavior

A Brief History of Facebook

1.1: Finding Hotties At Harvard, Keeping Friends At College

One night in the fall of 2003 a college freshman sat in his dorm room. His advances had been spurned by a cute girl in his class. He was drinking alone, trying to forget about this particular girl and scheming about ways to try to find a new one. This is a familiar college story. Happens all the time. Rarely does such a situation amount to more than perhaps an intemperate drunk dial and a nasty hangover. In this instance, however, it led to the creation of the largest social network site in the world.

That night, according to *Rolling Stone*, Mark Zuckerberg got the idea of comparing "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.[8] 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 being discovered and shut down by school officials. Zuckerberg was reprimanded for violating student privacy and sent back to his room where he continued to code.[9]

In February 2004, Zuckerberg launched thefacebook.com. The site, which Zuckerberg claimed to have coded in a week,[10] was very simple: students with Harvard email addresses could upload a profile photo, their course schedule, and a list of their personal interests.[11] Perhaps still smarting from his reprimand in the fall - or preternaturally wary of bad publicity - Zuckerberg said he designed Facebook to include powerful technical controls:

---

8 See Hoffman.

9 See Kaplan.

10 This has become a point of contention. As Hoffman's article describes, 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 sued successfully for $65 million.

11 See Tabak.

> *"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 friend of a friend can look you up. People have very good control over who can see their information."*[12]

Facebook was an instant success. Over a thousand students registered within the first week.[13] 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 social functionality, including the ability to create and join Groups and to comment on another person's profile using the Wall. By December 2004, the site had over one million users across all of its networks. Embracing the nerd chic, Zuckerberg listed his job description as "Founder, Master and Commander [and] Enemy of the State" on Facebook.[14]

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 brought Zuckerberg around the venture capital circuit.[15] The site raised over $12 million in initial seed money as colleges continued to be added to the network one-by-one. The fact that colleges were kept structurally separate[16] and a total lack of paid advertising did not prevent the site from spreading virally. By August, 832 school networks boasted 3.4 million members, 360,000 of them freshman, with over 8,000 new members joining every day.[17]

By the beginning of the fall semester in 2005, Facebook was ubiquitous at almost every college campus in the United States. 85% of college students had an account on the site, and 60% used it daily.[18] Its comparative simplicity - no photos, no groups, no applications, just a list of interests and a comment box - did not keep millions of students from joining the site and "Friending" everyone they knew at school. Each profile defaulted to

---

12 *Id.*

13 See Tabak.

14 See Hoffman.

15 *Id.*

16 For example, http://harvard.thefacebook.com was a different community from http://wm.thefacebook.com. Making one's profile visible to the former did not do so for the latter, and originally users could not Friend other users at other campuses.

17 See Colurso.

18 See Arrington.

public within its network, so students of one university could automatically browse everything about another person, in keeping with the school's original mandate to help find new friends or solidify weak ties. Facebook soon became *the* way to socialize at college.

1.2: Little Brother Is Watching You: High Schools And Photo Sharing

In September of 2005, Facebook announced that high school students could join the site.[19] There were significant restrictions: high school students needed to be invited by a current Facebook member who had graduated from the same secondary school or by a validated high school classmate. Like the original design of the college networks, high schools were kept structurally separate: college kids could not join high school networks, although they could Friend members. According to Facebook cofounder Chris Hughes, this design was meant to mimic actual social contexts:

> *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.*[20]

However, this design was not sufficient for at least some users of the site, who for the first time had to wrestle with the problem of communicating college content to those outside the college context. As two college 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 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.*[21]

In October 2005 Facebook introduced the Photos application, allowing any Facebook user to upload an unlimited number of digital pictures to the website. Students could also "tag" friends in the photos themselves such that the images would then be associated with the account of the person tagged. A generation of students with digital cameras sud-

---

19 See "Facebook | Timeline."

20 See Peterson.

21 See Shea and Feinstein. See also boyd, "Taken Out of Context" at 104.

denly had a central location to post the photos. By October 2008, three years after Photos was launched, Facebook users had uploaded a total of 10 billion pictures. Three terabytes of new photos were uploaded every day and 300,000 images were served to the users of the site every second.[22]

With massive amounts of tagged photos came massive amounts of documented college hijinks, and with massive amounts 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.[23] While many students were horrified that their social space was being turned against them, other 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."*[24]

Still, such incidents were comparatively rare and didn't discourage the majority of users. The site continued to grow and by December 5.5 million students had registered.[25] 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: leaving 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.

1.3: Here Comes Everybody: 200 Million users And Beyond

In September 2006, Facebook opened registration to anyone with an email address.[26] Its membership skyrocketed as adults flocked to Facebook. In May 2007, Facebook launched its developer platform, which allowed third party coders to hack their own pro-

---

22 See Beaver.

23 See Lash.

24 *Id.* See Section 3.2 to understand why Calvert was correct from a legal perspective.

25 See "Facebook | Timeline."

26 *Id.*

grams together to run within Facebook as add-ons. 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 Facebook content. As bosses, teachers, parents and employers joined Facebook, students began to reevaluate their presence online. What had once been a safe place to "hang out" with one's friends now endangered one's reputation and career prospects. Universities advised students to delete their Facebook profiles before applying for jobs.[27] A general malaise spread throughout the Facebook community as students were forced to choose between posting pictures from parties and Friending their fathers. By May 2009 what had begun as a way for awkward Harvard undergraduates to meet each other had been completely transformed by the addition of 200 million members, and an unbearable tension had arisen between Facebook's design, its members, their social purposes, and how they practiced privacy.

The Social Practices of Facebook

1.4: Real Friends And Weak Ties

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.[28] In other words, Facebook is not about meeting new people but rather friending people whom one already knows. It is less like a Yellowpages than a Rolodex; less like a cocktail party than an evening in with friends; less like JigSaw[29] and more like an AIM buddy list. Mayer and Puller found that only 0.4% of Facebook friendships consisted of "online only" interactions.[30] danah boyd concurred, describing social network sites as malls for modern teens: spaces to social-

---

27 For example, Resident Assistants at the University of Massachusetts were routinely warned to delete their Facebook accounts rather than compromise their job with pictures. In 2008 Resident Assistant Union agitated for a clause in the collective bargaining agreement that the University could not discipline Resident Assistants for material found on Facebook. The University refused to include it.

28 See boyd and Ellison, "Social Network Sites." Facebook, interestingly, was designed as a *networking* site. 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. 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. 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.

29 An internet Rolodox, where one can "buy" contact information with points. It's very odd. http://www.jigsaw.com/.

30 See Mayer and Puller, "The old boy (and girl) network," at 329.

ize, "hang out," to see and be seen, etc.[31] The average number of Friends any given user has is 120, remarkably close to the famous Dunbar number in anthropology and sociology.[32]

The implication of the "real relationships" phenomenon is that all Facebook interactions are animated and governed by preexisting social norms, roles, and expectations. boyd recounts how southern Christian youth think mySpace is a service for organizing Bible readings because that's what their friends use it for.[33] When users create their Facebook profiles, publicly Friend other users, and interact with friends online, they are both reacting to and reconstituting anew their preexisting social contexts by "writing community into being."[34] boyd describes youth behavior on social network sites as "performances" in Goffman's dramaturgical sense.[35] Or, as James Grimmelmann describes,

> *[S]ocial network site profiles are wholly social artifacts: controlled impressions for a specific audience, as much performative as informative. I should add that they're not just expressive of identity, but also constitutive of it. You are who 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.*[36]

While practices suggest Facebook Friends are unlikely to be complete strangers, that 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"[37] such that *knowing* someone is sufficient cause to Friend them.[38] Furthermore, Friendship does not distinguish between what is revealed to Friends, and therefore doesn't recognize the preexisting normative and dramatur-

---

31 See boyd, "Taken Out of Context."

32 See "Primates on Facebook."

33 See boyd, "My Friends, mySpace," at 16:00.

34 See boyd, "Friends, friendsters, and top 8." 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: http://www.facebook.com/apps/application.php?id=2425101550.

35 See boyd, "Taken Out of Context."

36 See Grimmelmann, "Saving Facebook," at 12.

37 See Stross.

38 See boyd, "Friends, friendsters, and top 8," at 11. "[Users] tend to Friend actual friends, acquaintances, family members, or colleagues."

gical distinctions in relationships.[39] 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.*[40]

The practice of promiscuous Friending, coupled with the effects of unqualified Friendship, has caused some to suggest that Facebook members must not care about privacy. Robert Samuelson, writing in the *Washington Post*, decried social network sites as nothing but homes for attention whores.[41] "Exhibitionism is now a big business," Samuelson declared, with the sort of all-knowing attitude that comes from 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.*[42]

Can this be true? Can it be that the introduction of a simple social network site has turned generations of Americans into shameless voyeurs? That, after enjoying the benefits of privacy for hundreds or thousands of years, Facebook came along and suddenly no one cares about it anymore?

---

39 See Section 2.5.

40 See boyd, "Facebook's Privacy Trainwreck."

41 An inimitable and indispensable term with many meanings, all of them derogatory, that precisely fits Samuelson's critique. It may refer to persons of either gender 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. There are endless shades and applications of the term, and more definitions can be found at http://www.urbandictionary.com/define.php?term=attention+whore.

42 See Samuelson.

1.5: Privacy Practices and Concerns on Facebook: Exhibitionists Don't Go 'Ick'

It's worth noting that Samuelson is not the first to so castigate a younger generation for not caring enough about privacy. One social critic wrote memorably that:

> *[A] new and far more deadly danger [to privacy] has arisen in the shape of the moral psychology of the young. That they intrude and outrage is patent and not the real problem. That problem has to do with their capacity for privacy, to enjoy and to sustain it in all its forms, and whether their form of personality is compatible with it.*[43]

While this argument may seem similar to Samuelson's, it was in fact written by Professor John W. Chapman in 1971 as a critique on the excesses of *Samuelson's* generation. Samuelson's critique, as popular and intuitive as it is, is really just another instance of a social practice as old as the species: complaining about how awful kids are today.[44] It is generationally descriptive, not analytically helpful: it relates Samuelson's interpretation of user practices but not the attitudes of the users themselves. Samuelson's belief that no one cares about privacy anymore is belied by survey and behavioral data that demonstrate Facebook users care a great deal about their privacy.

In 2006 - when Facebook still limited membership to students - Acquisti and Gross conducted a comprehensive survey of Facebook users at an undergraduate university.[45] 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 which was the privacy policy of social network sites.

If Facebook users don't care about privacy, then they should rank privacy policies very low on a list of concerns. But they didn't, instead ranking privacy policies near the *top* of their list. Students were "were more concerned (with statistically significant differences) about threats to their personal privacy than about terrorism or global warming..."[46] Students

---

43 See Chapman at 236.

44 Recall that hundreds of years before the common era Socrates chided that "the children now love luxury; they have bad manners, contempt for authority; they show disrespect for elders and love chatter in place of exercise. Children are now tyrants, not the servants of their households. They no longer rise when elders enter the room. They contradict their parents, chatter before company, gobble up dainties at the table, cross their legs, and tyrannize their teachers." See "Respectfully Quoted." Socrates began a long and illustrious tradition of old people complaining about young people. As a rule of thumb, whenever a critic argues that some perceived social problem is caused by the moral failures of the youth, the only thing that can be ascertained for sure is that the critic is now officially an old person.

45 See Acquisti and Gross, "Imagined Communities," at 8.

46 *Id.*

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],"[47] a question meant to simulate what could be accessed on most Facebook accounts at the time. When prompted with this question 81% of students said they were concerned to some degree and nearly 46% said it was of the highest concern.[48]

There are also ample behavioral data that suggest Facebook users *try* to protect their privacy by repurposing properties of the site's design to limit exposure.[49] danah boyd describes how users change their names, profile pictures, ages, or locations so that they can't be found via search functions.[50] Sometimes these tools follow social conventions known only to the user's imagined community, such as when a 16 year old reverses the digits in his or her age to appear 61, or when teenagers from a specific town all claim to be from Christmas Island.[51] Others restrict profile access to specific networks or lists of friends. Facebook users, 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, or police officers, those whom were most likely to hold direct control over and who operated in different social contexts than the users.[52]

To review, students consistently report on surveys that they are very concerned about their privacy on social network sites. Observations of user practices show that they often take affirmative steps to try to control access to their profile. It seems that whether you ask them or observe them, Facebook users care about their privacy. They are not, as Samuelson 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

---

47 *Id.*

48 *Id.*

49 This is perhaps an example of "privacy generativity" in action. See generally Zittrain, "The Future of the Internet."

50 boyd, "Taken Out of Context" at 147.

51 boyd "My Friends, mySpace" at 40:00.

52 See boyd, "My Friends, mySpace" 42:00. although boyd was writing 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. As boyd and Grimmelmann have outlined, 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 the practice is a key demonstration of what I believe to be a prevalent interest in protecting privacy.

their "personal information" is shown to others. For Facebook users, such displays feel "icky" and are to be avoided.[53]

Case Studies

1.6: A Series of Stories

Facebook users care about their privacy, and when data are disclosed under certain circumstances those users experience an "ick" moment that they understand as a violation of privacy. In order to analyze what's going on in these "ick" moments, this section reviews instances in which a user's privacy was allegedly infringed:

- In 2008, Katherine Evans was a high school student at Pembroke Pines in Florida. Frustrated by a teacher's alleged unwillingness to help her with her schoolwork, she created a Facebook group dedicated to "hating" the teacher. A few days later, 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.[54] Evans' experience recalls that of Cameron Walker, a member 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.[55]

- 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 doo-

---

53 When I asked students to describe exactly what a privacy violation on Facebook *felt* like, they often described it as a sense of disgust, of wrongness, of "ickyness." I am not alone in this. 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!" 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."" See boyd, "Taken Out of Context" at 144.

54 See Gentile.

55 See Schweitzer.

hickey 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."[56]

- 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 for 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." Others were unconvinced, noting that employers rarely followed their employees to the local bar to eavesdrop on any griping that might occur there.[57]

- 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." The photos had been culled from a Facebook group called "30 Reasons Girls Should Call It A Night." One student found herself beleaguered by calls from overseas organizations offering money for explicit interviews. The embarrassment was no ephemeral affair: a Google search of the student's name still returns the Daily Mail article as the first result.[58]

- In 2009 many students found themselves in the uneasy position of having to decide whether to Friend their 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. 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

---

56 See Cohen.

57 See "Facebook Remark Teenager Is Fired." This case is also reminiscent of another much-publicized case in which a 25 year old student-teacher 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." See Krebs.

58 See Levy. The student mentioned above is a University of Massachusetts undergraduate who requested anonymity for obvious reasons.

there kids life and not give them privacy." 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." These descriptions echo the experience of Rachel who trusted her grandmother but nevertheless felt uncomfortable exposing every aspect of her college life to someone outside the college context. [59]

Part 2: The Problem of Privacy on Facebook

WHAT IS THE PROBLEM?

2.1: Identifying the Interests

When someone claims that their privacy has been violated, they generally mean that one of those interests commonly included in the broad taxonomy of privacy has been injured.[60] Identifying the interest is critical, because interests are to privacy analyses as premises are to arguments: start from the wrong assumption, and it flaws every subsequent step in the process. Consider, for instance, the story of the Gill family as told by Prosser:

> *Typical is the bewilderment which a good many members of the bar have expressed over the holdings in the two Gill cases in California. Both of them involved publicity given to the same photograph, taken while the plaintiff was embracing his wife in the Farmers' Market in Los Angeles. In one of them, which involved only the question of disclosure by publishing the picture, it was held that there was nothing private about it, since it was a part of the public scene in a public place. In the other, which involved the use of the picture to illustrate an article on*

---

59 These quotes come from personal correspondence via Facebook and are on file with the author. All misspellings and grammatical mistakes have been left intact, and names have been changed.

60 As Solove explains, "Privacy violations consist of a web of related problems that are not connected by a common element, but nevertheless bear some resemblances to each other. We can determine whether to classify something as falling in the domain of privacy if it bears resemblance to other things we similarly classify. In other words, we use a form of analogical reasoning in which "[t]he key task," Cass Sunstein observes, "is to decide when there are relevant similarities and differences." Accordingly, there are no clear boundaries for what we should or should not refer to as "privacy." Some might object to the lack of clear boundaries, but this objection assumes that having definitive boundaries matters. The quest for a traditional definition of privacy has led to a rather fruitless and unresolved debate." See Solove, "I've Got Nothing To Hide" at 759. See also Solove, "A Taxonomy of Privacy."

> *the right and the wrong kind of love, with the innuendo that this was the wrong kind, liability was found for placing the plaintiff in a false light in the public eye. The two conclusions were based entirely upon the difference between the two branches of the tort.*[61]

The Gills experienced a privacy violation but were initially unable to find relief in the law. Their privacy interest protecting against an intrusion upon seclusion did not describe the violation: after all, they had been in public! It was not until they brought their case again, this time citing an interest in not being portrayed in a false light, that their violation made conceptual sense to the court, and a remedy could be prescribed.

According to Elizabeth Beardsley, the "most dependable clue to the content of [privacy norms] in any given society is found in the nature of conduct held to violate privacy."[62] Helen Nissenbaum's theory of contextual integrity can explain how the privacy of Katherine Evans, working teenagers, and Rachel were compromised, and help everyone understand exactly what went wrong.

2.2: Privacy as Contextual Integrity

Nissenbaum developed her theory of contextual integrity in response to what is sometimes called "the problem of privacy in public." In London, Nissenbaum reports, CCTV cameras surveilled much of the population. Some British citizens felt as if this violated their privacy, but were unable to explain exactly how, since it seems counterfactual to expect privacy in a public street. According to Nissenbaum, this confusion was caused by starting from the wrong premise:

> *As disturbing as the practices of public surveillance are, they seem to fall outside the scope of predominant theoretical approaches to privacy, which have concerned themselves primarily with two aspects of privacy—namely, maintaining privacy against intrusion into the intimate, private realms, and protecting the privacy of individuals against intrusion by agents of government...[W]ork within these traditions appears to suffer a theoretical blind spot when it comes to privacy in public, for while it has successfully advanced our understanding of the moral basis for privacy from some of the traditionally conceived threats...it has not kept*

61 See Prosser at 407.

62 See Beardsley at 56.

> *abreast of the privacy issues that have developed in the wake of advanced uses of information technology.*[63]

Nissenbaum argues that the predominant legal understanding of privacy as a means to prevent intrusions upon seclusion does not explain the violation felt by the publicly surveilled. As a general principle, "the law recognizes as private only information that is completely secret,"[64] but one is not meaningfully secret or secluded while walking down a public thoroughfare. If there is no intrusion, Nissenbaum explains, some other theory or explanation of privacy must exist for an individual to feel as if their privacy was compromised.

The explanation Nissenbaum provides describes privacy as contextual integrity. Contextual integrity, Nissenbaum explains, is maintained when norms of appropriateness and norms of distribution are respected.[65] Norms of appropriateness inform situational behavior: when someone is reverent in a church and debauched in a bar they behave appropriately. Norms of distribution influence informational flow: when a doctor keeps information confidential or a gossip spreads it around information flows as expected. According to Nissenbaum, "contextual integrity is maintained when both types of norms are upheld, and it is violated when either of the norms is violated."[66] Nissenbaum continues:

> *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.*[67]

---

63 See Nissenbaum, "Protecting Privacy in an Information Age" at 5.
64 See Solove, The Future of Reputation at 161.
65 See Nissenbaum, "Protecting Privacy in an Information Age" at 20.
66 *Id* at 20.
67 See Nissenbaum, "Privacy as Contextual Integrity" at 210.

These tendencies to "readily share" information depending on the context are privacy practices. The root of Nissenbaum's theory is that people behave differently with different people in different situations in order to maintain privacy. It means that individuals expect information to flow through the world depending on how they behave, where they behave, and who they behave with.

The idea that contextual integrity and its integral norms constitute a powerful privacy interest has been around for a long time. In his *Nichomachean Ethics* Aristotle examined whether "there is only one sort of friendship or several" to establish what relations properly existed between citizens.[68] In the 1960s, the philosopher James Rachels observed that "[the relationships] that 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."[69] When people differentiate disclosure to different individuals to respect social norms, Rachels argued, they not only respect relationships but constitute them.[70] The law professor Charles Fried defined privacy as the ability to differentiate disclosure between different people and believed that without it there could be no intimacy and no friendship.[71] Elizabeth Beardsley called this differentiation "selective disclosure" and thought it "the conceptual core of the norm of privacy."[72] In the domain of sociology, Irwin Altman defined privacy as the optimization between disclosure and withdrawal, writing that there are "different balances of opening and closing the self to others. In other words, there is an optimal degree of desired

---

68 See Aristotle.

69 See Rachels at 383.

70 See Rachels 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."

71 See Fried at 484.

72 See Beardsley at 70.

access of the self to others at any moment [and] privacy can involve a great diversity of social relationships."[73]

More recently, Lior Strahilevitz has advanced a complementary legal doctrine that would enforce privacy torts along the lines of real world social networks and thus respect norms of distribution.[74] Writing on the effect of the Internet on privacy, Jeffrey Rosen argues that contextual integrity is required to "[prevent] us from being misdefined and [misjudged] in a world of short attention spans, a world in which information can be easily confused with knowledge."[75] Clay Shirky characterizes "privacy in public" as "the privacy of the mall,"[76] arguing that while two individuals conversing in a mall certainly do so "in public" they would be shocked if a third party approached and began transcribing their every

---

73 See Altman at 11. See also Altman 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)." Compare also his discussion of privacy practices as being constitutive of identity, which danah boyd would later embrace in "Taken Out of Context" 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."

74 See Strahilevitz at 5: "I will argue that social network analysis is an indispensable tool for resolving disputes where the parties to a communication disagree about whether the recipient was entitled to share it with others." This approach is intriguing. While I will not analyze it as a formal matter of law - as will be shown, I believe that architectural solutions, rather than legal solutions, are the appropriate tools to solve Facebook privacy problems - I think Strahilevitz has the right idea about how law should take into account the social networks and norms of information flow when considering privacy torts. I will incorporate some of his ideas into my discussion of architecture solutions in subsequent sections.

75 See Rosen, The Unwanted Gaze, at 8.

76 See Shirky, Here Comes Everybody, at 85. "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."

word. Such behavior would violate social norms of appropriateness and distribution and probably change the content of their conversation as well.[77]

This idea of privacy as contextual integrity explains the violations experienced by the users in the case studies better than competing theories premised on other privacy interests.[78] The college student who believes that Friending parents "[subverts] the laws of nature"[79] echoes 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.*[80]

Similarly, the drunken students in the Daily Mail behaved in a manner totally appropriate for their social situation. They didn't care when the photos were distributed to their friends at college but felt violated once the photos circulated beyond the college context and into the wider world. Students gripe about professors to other students all the time, and Katherine Evans didn't mind if her friends knew she hated her teacher, but once her principal discovered her she experienced a loss of privacy. Similarly, a 16 year old employee is

---

77 The idea that a loss of contextual integrity changes the content of conversation is especially important in the work of Fried and Rachels, who both believe that differentiated disclosure is necessary for intimacy and intimacy necessary for friendship. See Fried at 487: "It is my thesis that privacy is not just one possible means among others to insure some other value, but that it is necessarily related to ends and relations of the most fundamental sort: respect, love, friendship and trust. Privacy is not merely a good technique for furthering these fundamental relations; rather without privacy they are simply inconceivable. They require a context of privacy or the possibility of privacy for their existence."; Rachels at 326: "[T]here is a close connection between our ability to control who has access to us and to information about us, and our ability to create and maintain different sorts of social relationships with different people...privacy is necessary if we are to maintain the variety of social relationships with other people that we want to have and that is why it is important to us."

78 There is one partial exception to this rule: the "intrusion" model may be appropriate to deal with privacy violations like the much-maligned Facebook Beacon program. Beacon tracked user activity outside of Facebook and published information to a user's Friends. So, for instance, if one rented a movie from Blockbuster's website, that fact was published to all of a user's Friends. Depending on the quality or content of the movie, this might prove embarrassing. Beacon was implemented across a number of merchant websites, including sites that sold birth control, pregnancy test, etc. When *these* highly private - we might say "secret" - transactions were broadcast to every Friend on Facebook, users were understandably upset. I do think that traditional privacy torts could apply to Beacon, as does James Grimmelmann, who suggests in "Saving Facebook" at 30 that the breach of confidence or misappropriation torts might be uniquely suited to deal with a problem like Beacon where Facebook has revealed information exchanged with a third party. Indeed, *any* instance in which Facebook goes out of their way to reveal secret user information could probably be remedied by traditional torts. However, the overwhelming bulk of privacy problems reported by Facebook users are not unjustifiable revelations by the company but rather instances in which collapsed contexts have given rise to tensions between formerly disparate social circles.

79 See boyd, "Taken Out of Context" at 144.

80 See Aristotle.

fired for posting a disparaging status update though her colleagues surely complain about their jobs down at the corner bar every Friday night. Finally, Adam Gartner would cheerfully have admitted knowing Marc Chiles to anyone but a police officer on that night in 2006. That they were friends was certainly not "secret." The police officer did not meaningfully "intrude" upon Gartner's seclusion when he saw that they had publicly Friended each other on Facebook. Yet Gartner still felt as if his privacy was violated, because he never expected his Friendship to be taken out of the context of Facebook and repurposed in a criminal investigation.

When users claim their privacy has been violated on Facebook, what they really signal is that there has been a collapse of contexts. According to Nissenbaum, contexts collapse when either norms of appropriateness or norms of distribution are disrupted. The privacy problems of Facebook are primarily caused by the latter, because the privacy architecture of Facebook is very different from the architecture of privacy.

Privacy, the Environment, and the Dynamics of Disclosure

2.3: The Architecture of Privacy

In 1999 Lawrence Lessig published "The Architecture of Privacy."[81] Much as Nissenbaum claims that contextual integrity depends in part upon social norms of distribution, Lessig writes that privacy depends in part on how information flows through any given space. According to Lessig, the architecture and technologies of the space determine this flow, which might be called the dynamics of disclosure of a space.[82] Altman conducted a similar analysis on the "people-environment unit" because he believed the individual and their environment mutually constitute all social behavior including privacy practices.[83]

---

81 See Lessig. "The Architecture of Privacy," which remains relatively unknown as one of Lessig's works: as of April 25 2009, *Shepard's* only lists 30 citations of the article. Compare that to the 142 citations (including five from the courts) of his "Reading the Constitution in Cyberspace." This may be due to the fact that it was published not long before the release of his seminal *Code*, into which he incorporated several of the key concepts. See Lessig, Code: Version 2.0, especially chapter 11.

82 I use this metaphor in part because the implicit comparison of privacy to the chaotic motion of liquids seems appropriate and accurate.

83 ASee ltman at 205: "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."

These environmental technologies are both complex and familiar, like those of monitoring and searching. Anyone who lives in a small town knows what it is like to be monitored by nosy neighbors, and a diary or a letter may be "searched" while it is read. But, as Lessig explains, for much of history these technologies were inefficient, and their inefficiency protected privacy. Without wiretaps monitoring is an earshot affair. Before computers, searching was laborious, slow, and there were no databases as we now understand them. Public life went mostly unrecorded, except for certain documents protected by locked safes and trespass law.

There are at least two other technologies of the physical world that affect what is generally considered private. The first is the technology of publishing, and the second is the technology of distinct social and situational spaces.

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."[84] 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.[85]

Another technology of the architecture of privacy is the design of social spaces. Recall Nissenbaum's description of norms of appropriateness. These norms are complex and informed by many factors, including race, age, gender, profession, marital status, and education. However, they are also informed by *physical spaces*. This means two things. First, *spaces have norms*. This claim is familiar and intuitive: one doesn't generally attend church in a bikini, for instance. Second, *norms have spaces*. This is less intuitive but critically important, for order for there to be a norm against wearing bikinis within the space of a church, there must first be a church that is physically distinct from other spaces.

This seems like a rather odd and obvious proposition. It shouldn't. The separation of social situations is merely a byproduct of the properties of the physical world. One behaves

---

84 See Warren and Brandeis, "The Right to Privacy," as well as Section 3.1.

85 See Shirky, Here Comes Everybody at 73, on the impact of publishing on the scribal tradition and the impact of new media on journalism as a profession.

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. By contrast, it is impossible to drink whiskey during a wedding in a bingo hall and still respect norms of appropriateness because no one would know how to behave in such a strange and wonderful situation. Walls, roofs, and fences not only keep intruders out, they define specific audiences or communities within which social norms operate. Separate physical spaces afford appropriateness by making it easy to see where and to whom information flows.[86]

The design of the physical world supports contextual integrity. Most of its interactions are unrecorded, ephemeral, and unsearchable. Since publishing is difficult it is generally presumed that to publish something implies an intent to make the information totally public and widely accessible. Finally, the physical or temporal separation of spaces demarcates social norms along the neat and orderly lines of deeds and schedules. These universal maxims inform social norms and expectations of privacy and make it easy to maintain contextual integrity in the corporeal world.

2.4: The Privacy Architecture of Facebook

By contrast, the privacy architecture of Facebook destroys contextual integrity, because almost every aspect of its design directly conflicts with norms of distribution. The way information flows through Facebook is nothing at all like the way information flows through

86 See Meyrowitz at the preface. "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."; 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."; at 7: "[E]lectronic 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."; and 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]."

the corporeal world.[87] It is an "environment that is fundamentally unnatural, in conflict with the one we evolved to live in."[88] This tension between individual and environment causes the most common privacy problems experienced by members of Facebook.

Consider the technologies of search and monitoring. In real life, they're an intrusion; on the Internet, they're a feature.[89] Online, every transaction is recorded. Searching billions of database entries in a matter of seconds is so trivial Google offers it for free. Facebook is no different: every data point is recorded, stored, and made searchable. This is the *point* of Facebook. There is zero utility to a social network site without content that can be easily found by those who wish to consume it.

Consider the technology of publishing. In the real world it is presumed that since publishing requires costly action it also implies an intent to make public. New media explodes this assumption by erasing the costs. It is a mistake, Shirky argues, to assume that just because content is made broadly accessible that the author intends it to be broadly accessed:

> *[Self]-publishing is now the normal case. In a world where publishing is effortless, the decision to publish something isn't terribly momentous. We misread these seemingly inane posts because we're so unused to seeing written material in public that isn't intended for us...The distinction between communications and broadcast media was always a function of technology rather than a deep truth about human nature. [But community] now shades in audience; it's as if your phone could turn into a radio station at the turn of a knob.*[90]

---

87 See Meyrowitz at 6: "Perhaps the best analogy...is an architectural one. Imagine that many of the walls that separate rooms, offices, and houses in our society were suddenly moved or removed and that many once distinct social situations were suddenly combined... We might still manage to act differently with different people, but our ability to segregate encounters would be greatly diminished. We could not play very different roles in different situations because the clear spatial segregation of situations would no longer exist....We would have trouble projecting a very different definition of ourselves to different people when so much other information about us was available to other audiences."

88 See Gruden at 2, writing of the Internet's effect on privacy.

89 See Lessig, "The Architecture of Privacy" at 61: "How should we understand this change? How should we understand its source? Its source is the change we will see in the architecture of a networked world. In real space, the default is that data are not collected. In real space, it takes effort--either the effort of a community, or the effort of a spy--to gather data. That is the architecture of the real world. And for most of our history, this architecture meant that any data so gathered were, in essence, useless. It was costly to hold, costly to use, and costly to collect. But the architecture of cyberspace is different."

90 See Shirky, Here Comes Everybody at 75-85 and 87-89. See also Shirky, "Interview for AOL Switched." danah boyd also confronted this question during her dissertation, when she had to choose whether or not to browse "public" mySpace profiles of users who clearly had not intended for her to view them.

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, this is no longer necessarily true.

Consider the way in which social network sites collapse once physically separate situations into a single social space.[91] In an electronic medium, Joshua Meyrowitz writes, "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."[92] By way of explanation, Meyrowitz 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.*
>
> *[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.*[93]

---

91 See Meyrowitz at 61: "Another way that new media may work to reshape socialization roles, therefore, is by affecting the traditional relationship between physical location and access to social information. The more a medium supports the relationship between physical isolation and informational isolation, the more it supports the separation of people into many distinct socialization "positions." The more a medium allows people to gain access to information without leaving old places and without severing old alliances, the more it fosters the homogenization of socialization stages."

92 See Meyrowitz at the preface.

93 *Id* at page 1.

Meyrowitz told this story to explain the problems electronic media posed to celebrities and public figures and some bleeding-edge executives,[94] yet it is normal folk who now experience his hypothetical dilemma. 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 the 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"[95] and in the same space. 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, complete with the attendant collapse of social contexts.[96]

Facebook's Counterfactual Design

2.5: The Technological Fictions of Facebook

On Facebook, social contexts are chiefly collapsed by aspects of the site's design that might be called *technological fictions*, which might be thought of as the computer science equivalent of a legal fiction. Legal fictions are law's counterfactuals: "situation[s] contrived by the law"[97] counterfactual to life as actually experienced. Think of the reasonable man or the corporate person. Both of these are legal constructs that simplify some complex social situation for convenience.

Similarly, when the design of a system does not reflect the true complexity of lived reality it creates a technological fiction. A technological fiction reduces or distorts social situations and relations. Legal fictions are primarily used by the law to help evaluate actions

---

94 *Id* 136, on the strange social situation of videoconferencing: "It is common for people who travel to a distant location to adapt, at least in part, to the behavior style of the 'natives.' New York executives who fly to California to complete contract negotiations, for example, expect to do business 'California style' while there. But electronic media create new placeless situations that have no traditional patterns of behavior. When New York and Californian business executives 'meet' via video teleconferences, they behave in a mixture of Californian and New York style that is both yet neither." See also Section 3.7 for the story of Stokely Carmichael.

95 *Id* at 87

96 boyd, "My Friends, mySpace" at 33:25.

97 See "Legal Fiction."

ex post facto (i.e. "would a 'reasonable man' have behaved in that way?") Technological fictions, on the other hand, impact the *actions themselves* by framing how users interact with and respond to their environment (i.e. "who am I 'with' right now?") Consider the following technological fictions of Facebook and how they might affect how users perceive spaces and social situations.

2.6: Flat Friendships

Facebook Friendships are crude devices: two users are either Friends or they are not.[98] In formal terms, Facebook Friendships are "indistinguishable with respect to tie strength."[99] By default, information posted by a user on Facebook may be accessed by any one of their Friends.[100]

Flat Friendships are technological fictions because they in no way represent the user's preexisting social relations. Beyond the simple acknowledgement of "yes, I've met you,"[101] Friendship asks and says nothing qualitative about the actual relationship between two Friends. It does not inquire how they know each other, or more importantly what overarching normative context within which they know each other. Friendship cares nothing for the preexisting social roles and norms that animate the relationship. In the corporeal 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 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 mere academic or aesthetic quibble. The flat nature of Friendship is the root cause of the vast majority of privacy problems and the chief hindrance to successful privacy practices on Facebook. Without a way to differentiate disclosure between Friends, every member of Facebook faces Meyrowitz's "welcome

---

98 It is very interesting, actually, that Facebook mirrors traditional privacy dichotomies in this way. Just as predominant legal theory can only conceive of information as either public or private so too does Facebook classify Friendship in binary terms.

99 See Lewis et al at 332.

100 An important caveat: as we shall see in Section 3.6, in March 2008 Facebook introduced a functionality called the "Friends List" that can be *repurposed* to differentiate disclosure and distinguish tie strengths. The default, however, is still binary.

101 See Section 1.4.

home party." The technology of Flat Friendships prevents users from respecting norms, distinguishing contexts, and practicing privacy.

2.7: Invisible Audiences

Social practices depend in part upon the audience for whom they are performed. As James Grimmelmann notes, "[w]e 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."[102]

For example, people tend to modulate the volume of their voice during conversation depending on the sensitivity of the content and who is in 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 social 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 far does my voice carry in this room?") are easily apprehended.

Electronic media are different. Public figures cannot see the audience behind the lens of the television camera,[103] and users of social network sites can't detect who might be watching from the other end of an Internet connection.[104] danah boyd has 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.[105]

To understand how Invisible Audiences might waylay norms of appropriateness consider the story of Stokely Carmichael. As one of the nation's preeminent black activists in

---

102 See Grimmelmann, "Saving Facebook" at 18

103 See for instance Section 3.7 for the story of Stokely Carmichael.

104 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 in those contexts. The invisibility of the audience robs it of salience and makes appraisal very difficult. Many studies in human-computer interaction have demonstrated that when users are made aware of who is viewing them they find it easier to target their audience and respect norms of appropriateness. For more on feedback, visibility, and salience see Section 3.7.

105 See boyd, "Taken Out of Context" at 34. See also Grimmelmann, "Saving Facebook" at 18, where he identifies the privacy heuristics of "Nobody in here but us chickens" and "I think we're alone now."

the Civil Rights era, he regularly spoke before black and white audiences about racial equality. His importance and influence were partially predicated on his ability to agreeably address different groups. Carmichael had what writers call a keen "sense of audience." He tailored his voice to the situation, adapting his style, content, anecdotes, and rhetoric depending on whether he was addressing primarily white or black audiences.

In the late 1960s Carmichael was invited to appear upon 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 Whitewater Hotel than at a gathering in Detroit),[106] on television he was speaking to one massive and 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, all because the broad reach of broadcast media caused him to lose his voice.[107]

The story of Stokely Carmichael demonstrates how difficult it is to respect norms of appropriateness when the audience is invisible.[108] danah boyd notes that in "unmediated spaces, it is common to have a sense for who is present and can witness a particular performance,"[109] but no such feedback exists on Facebook. Similarly, Professor Jonathan Zit-

---

106 Compare, for example, two speeches he gave in the mid-1960's on the subject of integration. Carmichael told a white audience in Wisconsin that "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." Not long after, he told a black audience in Detroit that "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]." See Brockeriede and Scott.

107 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 the audience to which he was speaking. He told the white audience in Wisconsin that "Negroes are dependent on, and at the discretion of, forces and institutions within the white society which have little interest in representing us honestly." He told the black audience in Detroit much the same thing but in a very different way: "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." See Brockeriede and Scott.

108 The story of Stokely Carmichael as an example of dangers of invisible audiences was inspired by similar treatments in the work of Joshua Meyrowitz and danah boyd.

109 See boyd, "Taken Out of Context" at 34.

train has described the Internet as having a certain "autistic" quality in that it doesn't convey a sense of who one mingles with at any given time in any given space.[110]

Invisible Audiences are another technological fiction of Facebook because users are artificially unaware of who they are performing for. Facebook designs its environment such that users don't know who has looked at their profile or which data were accessed. Facebook users 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 them or what they are looking for. Eventually, they forget its a false mirror at all, feel as if they were alone, and return to picking their noses. boyd describes how the inability to perceive audiences on Facebook keeps users from realizing their *faux pas*:

> *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.*[111]

In the physical world people can see their audiences and situate themselves accordingly. On Facebook, even if audiences are *known* consciously, they aren't *salient* viscerally, and so users may sometimes disclose information to too many people. 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 fame or fortune but because they watch with unseen eyes, obscure norms of appropriateness, and cause contexts to collide.

---

110 See Zittrain, "Berkman Book Release: The Future of the Internet And How To Stop It."; also Zittrain. "A Neighborhood Watch in Cyberspace.": "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."

111 *Id* at 38.

2.8: Strange Disclosure Defaults

In the physical world it takes a great deal of effort to share information. 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. In the physical world, data is dead weight, and only through conscious action does it move around.

These properties inform norms of distribution. When an individual relocates to a new town, they don't expect that merely moving there means all other residents now know everything about them. In populated areas like cities, even the most gregarious of individuals may never encounter more than a relative handful of individuals, much less learn their life story. Dead weight data creates strong norms that information is mostly immobile and never travels far from those who know it.

The dynamics of Facebook are completely different. The registration page for Facebook allows users to join "networks." These networks were originally college campuses but have since grown to include high schools, companies, and 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 them.

These Strange Sharing Defaults are technological fictions because the do not accord with lived experience and user expectations. No one thinks that moving to Boston means pushing all their information at every other resident, but joining the Boston network on Facebook does exactly that, despite the fact that "doing things on the basis of 'networks' doesn't help draw socially meaningful lines."[112] The fact that a student and their parent and professor all live in Amherst 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. Furthermore, the

112 Personal correspondence with James Grimmelmann.

global publishing default of photos and videos completely disrespects any norm of distribution. Even if it were possible to share one's multimedia with every person in the entire world it seems unlikely that people would *want* to do so.

Facebook is designed with disclosure in mind.[113] 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.

Part 3: Reconstructing Collapsed Contexts

What Should Be Done

3.1: Why Facebook Should Care

These technological fictions are key deficiencies in the privacy architecture of Facebook. They rob users of the architectural cues they rely up on to situate themselves and keep contexts apart. Perhaps unsurprisingly, 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 is produced by users sharing data. There's no point in targeting ads when users don't share any useful demographic information. 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

---

113 See "Facebook | Free Flow of Information on the Internet." The mission statement of the group has changed considerably since 2006: it now mostly serves as a clearinghouse for news about net neutrality and other issues with content regulation. When it was launched, however, Zuckerberg indicated that it was an explicit principle guiding Facebook. "About a week ago I created a group called Free Flow of Information on the Internet, because that's what I believe in – helping people share information with the people they want to share it with." See Zuckerberg, "Facebook | An Open Letter from Mark Zuckerberg." This explanation, of course, is about as vague and safe as a politician's self-professed love of mother, country, and apple pie. The *implementation* of this principle, with defaults that do not seem to respect any norms of distribution that I can find, tell a slightly different story.

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.

Recall the discussion of "privacy events" from Section 1.6. 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, more people will share, until they share too much, experience an "ick" moment, and immediately clamp down on their disclosure to compensate. 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[114] and everybody wins.[115] If altruism or concern for their users can't make Facebook care about their privacy problems, maybe old-fashioned self-interest ought to make them explore ways to help users maintain contextual integrity and practice privacy.

---

114 Going back to the profit models, then, the correct linear relationship is not that sharing is positively related to how easy it is for the user to share, but rather that sharing is positively related to how much the user trusts Facebook. Surveys bear out this relationship between trust and disclosure. In "Privacy in Electronic Commerce and the Economics of Immediate Gratification" Acquisti cites a 2006 study that showed online shopping would have been 24% higher in 2006 if websites had done more to assure their users that their privacy and security would be protected on their site.

115 Unless, of course, users are tricked into what James Grimmelmann has called 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.

3.2: Why Law Won't Work

The year was 1890, and the lawyer Samuel Warren was in a churlish mood. The cause of his anger is unclear. Some contend he was furious when the news media hounded the wedding of his daughter.[116] Others argue he was incensed by a series of articles chronicling his lavish dinner parties.[117] Whatever the reason, Warren was outraged. He felt very strongly that some right of his had been violated by lascivious voyeurs in the press and public. However, he was not quite sure what the right consisted of, what it protected, or what remedies it prescribed. Warren summoned his law school friend and business partner Louis Brandeis, with whom he had recently penned a series of articles about the law of ponds.[118] Eager to leave behind such stagnant subjects for fresher waters, Brandeis signed on, and they soon published "The Right To Privacy,"[119] which became one of the founding pillars of privacy law in the United States.[120]

Brandeis and Warren believed the law was changing. This change, they argued, extended the law to protect more than just mere boring standbys like life, liberty, and property. Instead, the law had come to recognize that "[t]he intense intellectual and emotional life, and the heightening of sensations which came with the advance of civilization, made it clear [that] only a part of the pain, pleasure, and profit of life lay in physical things."[121] Laws prohibiting assault, nuisance, defamation, and the theft of intellectual property had all arisen to protect these intangible accoutrements of an enjoyable life.[122]

According to Warren and Brandeis, these laws all flowed from the same source: a fundamental right "to be let alone," which they called "privacy," a right necessary for sanity and happiness in an increasingly claustrophobic world:

> *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*

116 See Prosser at 383.
117 See Solove, The Future of Reputation at 109.
118 *Id* at 110.
119 See Warren and Brandeis.
120 See Solove, The Future of Reputation at 110.
121 See Warren and Brandeis.
122 *Id.*

> *individual... invasions upon his privacy [subject] him to mental pain and distress, far greater than could be inflicted by mere bodily injury.*[123]

Just as printing facilitated libel and the theft of intellectual property, Warren and Brandeis explained, so too did perfidious modern technologies enable the destruction of privacy.[124] This, they wrote, was unacceptable, for "[the] individual is entitled to decide whether that which is his shall be given to the public."[125] The common law had long secured the right of the individual to be free from the unreasonable intrusions of government. Without similar protection against the prurience of private citizens, Warren and Brandeis contended, the courts would "close the front entrance to constituted authority [but] open wide the back door to idle [curiosity.]"[126] Warren and Brandeis sparked a privacy revolution. Even a century later, their central thesis that privacy protects the right to be let alone constitutes the conceptual core of all modern privacy law.

This story - that new technologies create new privacy problems - seems awfully familiar to digital natives. It is tempting to think that Warren and Brandeis have insights for the digital age that could help users protect their privacy on Facebook. However, in this case appearances are misleading. The privacy problems of Facebook aren't intrusions upon seclusion, and the right to be let alone doesn't suggest any helpful solutions for users.

According to most legal scholars, privacy law in America has evolved to protect secrecy, as "[t]here can be no privacy in that which is already public."[127] 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."[128]This strict dichotomy between public and private makes an awful lot

---

123 *Id.*

124 *Id.* "Instantaneous photographs and a newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "what is whispered in the closet shall be proclaimed from the house-tops...The press is overstepping in every direction the obvious bounds of propriety and of decency...Even gossip apparently harmless, when widely and persistently circulated, is potent for evil."

125 *Id.*

126 *Id.*

127 See Solove, The Future of Reputation at 161.

128 See Friedrich at 105. Furthermore, existing case law seems to suggest that any information posted to Facebook, no matter its privacy settings, can no longer be considered private as a matter of law under the third party doctrine. See for example *Couch v. U.S* at 335: "there can be little expectation of privacy where records are handed to an accountant."; *Miller v. U.S.* at 449: "The depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."

of sense if one is chiefly concerned with retaining the "essential solitude" championed by Warren and Brandeis. When the most immediate privacy problem is keeping reporters out of one's house and away from one's personal life, the right to seclusion seems sufficient to solve the problem.[129]

But the privacy violations felt by Facebook users are different. The seclusion regime only works inasmuch as the individual is interested in secluding themselves, but Facebook users don't retreat from the complexity of advancing civilization, they *embrace* it. As James Grimmelmann writes, "the first task of technology law is always to understand how people actually use the technology,"[130] and no one on Facebook is *trying* to keep information secret. That's not the *point* of Facebook.

Furthermore, using law to fix Facebook would inevitably entail attempts to legislate contextual integrity, and it's not clear how such regulation would work. Would a legal solution try to prevent promiscuous or decontextualized Friending, perhaps by regulating who may friend whom? This cannot work: regulators are even worse than Facebook at defining social relations, and requiring users to consult the Department of Friendship before connecting on Facebook seems unreasonable at best. Would a law require certain technologies or architectures of any social network site? Such a law would surely stifle innovation, as no startup could survive if they were required to build a complex privacy architecture before they could even admit alpha testers, and no one can define a "social network site" anyway. Would a law accept that unwanted exposure is inevitable and instead try to constrain the use of that information after the fact, perhaps by prohibiting employers from firing employees for information found on Facebook? Surely such a law would infringe upon the freedoms of the employer, and in any case the "ick" moment would have already occurred, not been forestalled.

Privacy law simply can't restore contextual integrity to Facebook because it cannot comprehend the violations or suggest how they might be solved. Warren and Brandeis rooted the right to privacy deep in the soil of seclusion, and it cannot be easily transplanted to these problems.

---

129 Or, as Solove wrote on page 109 of The Future of Reputation, "Warren and Brandeis looked into the future and foresaw the paparazzi."

130 See Grimmelmann, "Saving Facebook" at 2.

Privacy law is not well equipped to solve problems of contextual integrity partly because, as a product of the physical world, it *presumes* certain architectural properties. It isn't possible to seclude oneself if spaces and times aren't separated, if Friendships are flat, and if audiences are invisible. Trying to use the seclusion regime to solve the contextual breakdown on Facebook is like trying to use a shield as a scalpel: it's just not the right tool for the job.

3.3: Why Markets Won't Work

Markets are another 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 the costs to their privacy outweigh the benefits of that technology. No laws prohibit the building of glass houses because the market's aversion to constant surveillance does the job just fine. Devout cyberlibertarians might argue that if users really care about privacy they will simply stop using Facebook or jump ship 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 the invisible hand will reconstruct contexts on its own.

Faith in market solutions, like faith in legal solutions, is predicated on certain premises. Just as law presumes a desired end-state of seclusion, markets presume the classical economic dogma that individuals make choices (including those affecting their privacy) according to their rational self-interest. As such, economists who study privacy and decision making 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."[131] In English, this means that individuals fully understand the implications of their practices on their present or future privacy by instantly calculating the equilibrium of the payoffs or consequences of disclosure and behaving accordingly. According to classical economists, privacy practices are just market transactions, driven by rational cost-benefit analyses. There is even an equation that supposedly models the tradeoffs of "privacy transactions":[132]

---

131 See Acquisti and Grossklags at 1.

132 See Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification" at 2. If the equation doesn't make any sense, that's fine, because it shouldn't. For a complete explanation of each variable and how it "should" work, refer to the paper.

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

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."[133] 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."[134] 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 intent and the objective affect of users.[135]

Acquisti found that privacy transactions in electronic media are often characterized by *incomplete information* and *bounded rationality*. It is difficult for users to accurately appraise the risk of unwanted exposure since Invisible Audiences keep them from perceiving who they are exposing themselves to. Furthermore, most of the costs of protecting privacy (i.e., spending much time changing privacy preferences) are immediate and salient, whereas most of the payoffs (i.e., not having contexts collapse) are only felt *ex post facto*. 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 actual subjective valuation of privacy.[136] 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 such as identity theft" and thus regularly underinsure themselves.[137] All of these biases would seem to explain the otherwise counterintuitive finding that the strength of Facebook privacy settings

133 See Ariely.

134 See Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification" at 1.

135 Including, for example, the tensions described in Section 1.6.

136 *Id* at 3.

137 *Id* at 4. For additional insights on hyperbolic discounting and other behavioral biases, see Gilbert.

isn't predicted by articulated user concern for privacy but rather by whether a user has recently experienced an "ick" moment or privacy event.[138]

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 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.[139] 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."[140] 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. Acquisti and Gross detected widespread optimism bias in the social practices of Facebook users.[141]

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 the best choice for them and instead just stick with the default option. The default exerts tremendous power even over decisions normally considered very personal and important. For instance, a study of Iowa residents showed that even though 97% of respondents favored organ donation in the event

---

138 Personal correspondence with Professor Ian Brown. While there appears to be very few studies that have explicitly investigated the nature, rate of occurrence, and affect of privacy events, some preliminary data and anecdotal practices seem to be support the conclusion. Acquisti and Gross, for instance, found in "Imagined Communities" that a statistically significant number of users from their cohort changed privacy settings after having specific privacy problems and permissive privacy defaults described to them. Rachel and Jess from the case studies probably 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 for once outweigh the costs. This is, of course, understandable - but it is by no means rational.

139 See Thaler and Sunstein, Nudge at 32.

140 See Acquisti, "Privacy in Electronic Commerce and the Economics of Immediate Gratification" at 4. A classic example of the "associated risk" bias is smoking, as smokers often don't grasp that the harm of long term smoking is greater than the sum of cigarettes smoked.

141 See Acquisti and Gross, "Imagined Communities" at 13, figure 9. When asked what others use Facebook for, users routinely respond with "making themselves more popular" or "finding dates." However, they universally deny that *they* use Facebook for these purposes.

fort to check the box on their drivers licenses.[142] 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. Now, only 12% checked the box, while the rest "chose" to donate their organs.[143] The effect is international: compare the 12% rate of organ donation in Germany (where citizens opt-in) to the 99% donation rate in Austria (where citizens opt-out).[144]

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. According to Facebook Chief Privacy Officer Chris Kelly, only 20% of Facebook users ever change their privacy settings.[145] Gross and Acquisti found that almost a fifth of Facebook users think they have no control over who can read their Facebook profile.[146] 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.[147] Ethnographers, including danah boyd, have found that Facebook users often struggle to change the defaults in practice. 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*

142 See Thaler and Sunstein, Nudge at 177.
143 *Id* at 178.
144 *Id.*
145 See Stross.
146 See Acquisti and Gross, "Imagined Communities" at 16. It should be noted that Gross and Acquisti dispute Kelly's numbers: their study found that only a vanishingly small 1.2% of users ever touched their privacy settings. However, I did not include this number, largely because Gross and Acquisti were writing very early on in the process and that specific data is no longer good. It would not surprise me, however, if the true number were somewhere between 2% and 20%.
147 See "Sophos ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves."

> *it yet'. The result is that she sees the private information for [many Londoners] but not that of her schoolmates*.[148]

Additionally, Acquisti and Gross 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*.[149]

These data suggest that Facebook privacy practices are driven by anything but rational consideration. Instead, users routinely, systemically, and predictably underestimate privacy risks and thus underinsure against them, often only 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 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[150] it would not receive accurate privacy signals. Inaccurate privacy signals create a feedback gap and cause market failures.[151]

Faith in market solutions also presupposes a competitive market. 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,

---

148 See Livingstone at 406.

149 See Acquisti and Gross, "Imagined Communities" at 11.

150 Which it doesn't seem to be. See Wortham: although 1.2 million users have indicated displeasure with the 2009 redesign Facebook shows no signs of changing it, despite the fact that a vote of less than 600,000 was sufficient to switch privacy policies.

151 Or, as Grimmelmann explains in "Saving Facebook" at 31, "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. Where a well-functioning market would need 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 non-users —the people who've suffered a privacy loss aren't in a position to negotiate effectively."

as danah boyd notes, by "where [their] friends are."[152] Social networks, in other words, are characterized by increasing returns.[153] 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 is reached and it makes social sense to join. Thus, any potential competitor to Facebook faces the crippling disadvantage of *not being Facebook*. The mere proliferation of other social network sites like mySpace or LinkedIn doesn't necessarily solve the anticompetitive question. No one uses mySpace or LinkedIn or Facebook for the same social purposes, just as no one rents a taxi when the social situation demands a limousine. Social network sites provide complementary social services, not substitute social goods.

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,"[154] and further discourages competition. 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.[155] Many users find Facebook socially indispensable, meaning they "will put up with a bad deal rather than make the effort of replicating all their personal data and 'friends" connections elsewhere.[156] 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.[157] The best predictor of whether one joined Facebook was not concern for privacy but age,[158] which points to the existence of a network effect overriding users' personal privacy preferences.[159]

Cognitive biases prevent most users from accurately expressing their privacy preferences and instead provide misleading signals to the market. Furthermore, even if users could overcome these biases, the anticompetitive character of Facebook means they don't

---

152 See boyd, "Taken Out of Context."
153 See Arthur.
154 See Edwards and Brown at 23.
155 See Ellison et al, "Building Social Capital."
156 See Edwards and Brown at 23.
157 *Id.*
158 *Id.*
159 *Id* 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."

have much of a choice beyond deactivating their profile. The market has yet to provide a solution to Facebook privacy problems. These are but a few reasons to suspect that it can't.

3.4: Why Code Could Work

Privacy law is designed to deal with a different problem. Predictable irrationalities and anticompetitive effects lead markets astray. If the collapse of contexts is a problem of architecture, however, code could help provide some solutions.

Code is law.[160] More specifically, "code does the work of law, but does it in an architectural way."[161] As a form of architecture, 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."[162] The design of Facebook doesn't afford privacy practices because its technological fictions make it difficult for users to respect norms of distribution and appropriateness and consequently difficult to maintain contextual integrity.

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. Technological architectures, unlike laws of nature (and often those of man), can be easily changed. Lessig wrote that "we don't 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."[163] The same might be said of Facebook.

This architectural approach raises immediate objections. After all the discussion about norms and social cues it seems a bit counterfactual to describe privacy as something "built." Privacy is lived and practiced, not constructed. When people practice contextual integrity they respect the norms incident to their immediate social situation. They don't try to

---

160 See Lessig, Code 2.0.

161 See Grimmelmann, "Regulation by Software" at 1721; See also Rotenberg, "Fair Information Practices and the Architecture of Privacy" at 1: "[the] power of code as law (or "architecture as policy)..."; and Ethan Katsh, *Software Worlds and the First Amendment* at 355: "Yet, changing software is not simply changing what is on the surface. If a comparison to the physical world is necessary, one might say that the software designer is the architect, the builder, and the contractor, as well as the interior decorator. Software determines structure as well as appearance."

162 See Norman, Things That Make Us Smart, at 243. See also Kranzberg's First Law, which reads "Technology is neither good, nor bad; nor is it neutral." Kranzberg, "Technology and History:'Kranzberg's Laws." at 545.

163 See Lessig. "Reading the Constitution in Cyberspace" at 888.

develop comprehensive rules that could describe any social situation they might ever encounter in the future.

Many leading scholars of social networks have sharply criticized existing code-based solutions for this reason. James Grimmelmann argues that privacy controls are not sufficient to protect privacy, explaining that:

> *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.*[164]

Clay Shirky also argues believe that the arms race for ever-more-granular privacy controls is a fool's errand. He scoffs at the RELATIONSHIP project - an attempt to create a machine-readable taxonomy of social relations - and dismisses the idea that technical settings could ever accurately reflect actual contexts:

> *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.*[165]

danah boyd completes the chorus, chiming in to say that technical permissions lists cannot meaningfully recreate social relationships:

> *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*

---

164 See Grimmelmann, "Saving Facebook" at 36

165 See Shirky, "RELATIONSHIP: A vocabulary for describing relationships between people."

> *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.*[166]

These critiques are largely accurate.[167] Current technical controls, while powerful, are too unwieldy and difficult for their users to actually use. James Grimmelmann is right to point out that it is "deeply alien to the human mind to manage privacy using rigid *ex ante* rules."[168]

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 technical controls is partially due to insufficient privacy settings and partially due to a deficient privacy architecture. The former failure has (rightly) received much attention while the latter has been largely neglected.

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 "technical control" on privacy in speech, and in the physical world it works just fine.

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. Second, respecting norms of distribution presumes that one *can* change the volume of one's voice and *can* raise or lower volume to reach more or less people as desired. These properties are presumed because they are integral to the architecture of the physical world.

Of course, Facebook *doesn't* afford these practices. 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

---

166 Personal correspondence with boyd.

167 Of course, there are some ways that users repurpose code to practice privacy. Recall the way some users change their names or searchability or ages to keep from being discovered.

168 See Grimmelman, "Saving Facebook" at 36.

difficult to set *ex ante* rules, but also because Facebook's design withholds from users the environmental and social cues 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.

Privacy practices cannot be analyzed apart from the environment wherein they occur,[169] and the Facebook environment, as currently architected, is set against privacy practices.[170] 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 has many advantages as a solution. For example, it is easier to implement, self-enacting, and universal when compared to law.[171] 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.

Grimmelmann, Shirky, boyd, and others are right to be skeptical of the technical control arms race. 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 a better privacy environment. Code can

---

169 Recall Altman's "people-environment unit" from Section 2.4.

170 I allude here to Lessig's proposition in "Reading the Constitution in Cyberspace" 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."

171 See Edwards and Brown at 20: "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."

make it easier for users to respect norms of distribution and appropriateness by making information flow intuitively throughout Facebook. That code could help solve this problem is not particularly surprising: after all, the problem of privacy on Facebook is architectural in character, and architectural problems demand architectural solutions.

Creating an Environment That Privileges Privacy

3.5: Some Guiding Principles For Usable Privacy

The problem of privacy on Facebook is a collapse of contexts. The present privacy architecture of Facebook enabled the collapse. A different design might help reconstruct contexts. Still, it is extraordinarily difficult to design good privacy architectures. Different sites require different solutions depending on different uses: the sort of privacy architecture 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 can be attributed to this tension between user expectations and the actual dynamics of the design, the most obvious solution is to redesign the system so that it respects user norms of distribution and enables differentiated disclosure. Such respect requires that users have the tools to protect their privacy *and* that they operate within an environment that provides them the sort of architectural cues that inform their privacy practices in the physical world.

Enacting these principles would help "transform difficult tasks into easy ones"[172] and enable users to more easily practice privacy on Facebook. The following sections revisits the technological fictions identified in Section 2 and describe some ways in which they might

172 *Id.*

be designed to better respect user norms of distribution such that "the user can figure out what to do, and the user can tell what is going on."[173]

3.6: The Wisdom of Friends: Loosely Typed Privacy Clusters

Section 2.6 described 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."[174] Launched in March 2008, the Friends List feature allows users to create groups of their Friends. Clicking on 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 choose to give the "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.[175]

The use of Friends Lists as a method to maintain social contexts is an essential weapon in the privacy practitioner's arsenal. It can empower users to restore robustness and

---

173 See Norman, The Design of Everyday Things at 188.

174 While Facebook did not respond to requests for data on the adoption and use of Friends Lists, anecdotal evidence and informal surveys strongly support the conclusion that almost no users know that Friends Lists exist and even fewer use the feature.

175 In addition to the author, who has argued for this functionality and use since the launch of the Friends List, Professor Lorrie Cranor and her graduate student Aaron Shelmire of Carnegie-Mellon University have argued in favor of it. See for instance Shelmire's unpublished "Social Networks and the Professional/Private Life Boundary," on file with the author. See also Hong 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."

complexity to formerly Flat Friendships. However, it does give rise to two serious objections. First, the entire idea of using Friends Lists as privacy tools seems to conflict with Grimmelmann, Shirky, and boyd's observations about the inability of technical settings to capture social complexities. Second, if Facebook already has this feature, it seems strange that so few members employ it as a means to practice privacy.

Grimmelmann, Shirky, and boyd are absolutely correct that more granularity does not equal more practicable privacy. Technical controls are no match for social complexity, and no Friends List could ever accurately represent the actual social relations between users. Even if the technical controls of Facebook provided users the ability to finely discriminate their disclosure, trying to implement the controls would impose unbearable and insurmountable cognitive costs in actual use.[176]

However, users don't need Friends Lists to perfectly recreate each social relationshipsin order to use them to help practice privacy. Users simply need Friends Lists to help them define broad social contexts and respect the associated norms of appropriateness. After all, when one goes to a bar with five friends, one doesn't feel the need to behave in five different ways at the same time just because one doubtlessly has different relationships with each of those friends. In other words, for the purposes of privacy it doesn't necessarily matter whether Friends Lists precisely describe social relations. Instead, what really matters is whether members can use the Friends List feature to create "privacy clusters" and differentiate their disclosure according to broad situational contexts.

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.[177] Users could differentiate their disclosure by individual, by custom-made groups, by a "Team" mode dictated by the application, or to share

---

176 See Hong at 98: "A consensus is slowly building in the research community that privacy-sensitive applications cannot make all data transfers explicit, nor require users to track them all. The related UIs and interaction patterns would simply be too complex and unwieldy."

177 See Lai and Patil, "Who Gets to Know What When: Configuring Privacy Permissions in an Awareness Application."

"globally" with the entire network. 70% of users managed their permissions at the group level.[178] 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 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"...Defining permissions at group level appears to provide the flexibility needed to appropriately manage the balance between awareness and privacy without undue burden.*[179]

A similar study conducted by Olson and company discovered such "clusters" within user contacts.[180] 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.*[181]

According to the *Economist*, Cameron Marlow - Facebook's resident sociologist - claims that users have "core networks" that bear a striking resemblance to the concentric circles of trust discovered by Lai, Patil, Olson, and others:

> *Thus an average man—one with 120 friends—generally responds to the postings of only seven of those friends by leaving comments on the posting individual's photos, status messages or "wall". An average woman is slightly more sociable, responding to ten. When it comes to two-*

178 *Id* at 104
179 *Id* at 106, 108
180 See Olson et al, "A study of preferences for sharing and privacy."
181 See Hong at 29.

> *way communication such as e-mails or chats, the average man interacts with only four people and the average woman with six. Among those Facebook users with 500 friends, these numbers are somewhat higher, but not hugely so. Men leave comments for 17 friends, women for 26. Men communicate with ten, women with 16.*[182]

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 underutilized. This discrepancy between the theoretical utility of the Friends List and the actual use 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.[183] The Friends List feature was introduced in March 2008 as a way for users to organize their Friends into different social groups, not necessarily into different privacy clusters. For example, selecting a "College" list filters a user's feed such that only updates from Friends who attended the same college will show up. While this is a useful social tool, 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 do have an epiphany and realize that they can use Friends Lists to manage their privacy, Facebook does not facilitate the privacy process. When users create a new Friends List, they are instantly confronted 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 gigantic list of one's every Friend and try to recreate privacy clusters out of whole cloth on the spot with zero situational or social guidance.

---

182 See "Primates on Facebook." According to the *Economist*, Marlow's findings are in line with other sociological finds that suggest humans tend to have a "social circle" of weak ties (famously pegged by Dunbar at 120 people) and then a "core network" of far fewer that they feel they can truly confide in.

183 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?

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."[184] Facebook could very easily relaunch the Lists - or something like them - and advertise them as a way to separate out privacy clusters. Instead of publicizing them as social filters, it could 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.

Facebook could also help users overcome cognitive barriers by making it easier for users to recreate social contexts online. It could, for instance, perform basic network analysis on a user's Friends network to inform them of what clusters may already exist, and perhaps to create default Friends Lists for them automatically to help them along.[185] 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, whom 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.[186]

Donald Norman, the famed industrial designer and applied psychologist, believed that designers should harness "knowledge in the world" to produce more usable designs. For example, Norman argued, it is foolish to design a door with a handle if the door is meant to be pushed, as the handle would send a counterfactual signal to the user to "pull." A better solution, according to Norman, is to equip the door with a flat panel, since a flat panel intuitively affords pushing. Designing for intuitive use takes knowledge out of the head ("I know I must push this door, as I remember that I have had to push it before, and as the sign

---

184 Personal correspondence with James Grimmelmann.

185 Lai and Patil also argue for this 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." See also boyd, "Faceted/ID."

186 It should be noted that Facebook already uses this knowledge to aggressively push new Groups, Friends, Applications, or Pages at users via the "Suggestions" feature at http://www.facebook.com/find-friends/?expand=pymk&ref=hpb.

tells me to push") and puts it in the world ("I know I must push this door, because it has a flat panel, and that means push.") The difference between knowledge in the head and knowledge in the world, wrote Norman, is "fundamental to design."[187]

On Facebook, the world is the network. 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 amount of data it has collected about user social networks. It could push the Friends List feature as a way to manage privacy and inspire users to utilize it to preserve social contexts.[188] It could smooth out existing problems with its privacy preferences. Instead of requiring users to navigate a labyrinthine process to access privacy preferences it could make them easier to access and smooth out existing problems with their implementation.[189]

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

---

187 See Norman, The Design of Everyday Things 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."

188 Lai and Patil agree, finding at 108 that: "Our findings provide strong support for providing grouping functionality in awareness systems for *more than contact list organization*." (emphasis added)

189 For example, no matter what privacy preferences are set for individual Videos, Facebook only respects the global settings of the Video application, which prevents users from discriminating disclosure in all but the most hamfisted of manners. I discovered this myself after posting a video to Facebook. The video was set to be accessed by one specific Friends List. When someone outside of the Friends List - indeed, someone who was not a Friend of mine at all - commented on the video, he contacted Facebook for support. After a dozen or so emails were exchanged, it was determined that the *global* preferences for the Video application were set to "share to Friends and Friends of Friends" overrode the video-specific "share to [x] Friends List" setting. When I expressed my displeasure and requested that his preferences be respected, Facebook's support staff responded by writing "Unfortunately, the specific functionality you are requesting is not currently available. You can either restrict all of your videos or none of them, according to the Application Privacy settings. Sorry for the inconvenience." Thus does poor design thwart the most determined practitioners of privacy. The entire email chain is on file and available upon request, especially if Facebook were to request it so that they might fix a tiresome and inexcusable bug.

do this because the separation of spaces allowed him to distinguish between audiences.[190] Television, 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, it could help rebuild the walls that once kept social context apart and be invaluable to the practice of privacy.

3.7: Restoring a Sense of Place: Feedback, Salience, and Visibility

Even if Facebook users are assiduously aware of their audience (or, more likely, imagine an audience for which they are performing)[191] they still lack the necessary feedback to practice their privacy. 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.*[192]

The gulf of Evaluation on Facebook is caused by the disconnect between the a user's imagined audience and a 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 could access content not intended for them, or that their intended audience did not match their actual audiences:

---

190 See Meyrowitz 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]."

191 See boyd, "Taken Out of Context" at 35. "When performing in networked publics, people are forced to contend with invisible audiences and engage in acts of impression management even when they have no idea how their performances are being perceived. Performing for imagined or partial audiences can help people handle the invisible nature of their audience. These practices became a part of life in networked publics, as those who contributed tried to find a way to locate their acts."

192 See Norman, The Design of Everyday Things at 50-51. Norman also identifies as "gulf of Execution," which he identifies as "[the] difference between the intentions and the allowable actions." Insufficient privacy controls are a gulf of Execution.

> *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 because they lack the control that they think they have.*[193]

Section 2.6 described how the problem of privacy on Facebook is enabled not only by insufficient privacy controls but also by a lack of the architectural cues users need to situate themselves and guide privacy practices. The absences of feedback, visibility, and salience are key deficiencies in the Facebook privacy environment. Facebook should build these cues back into its architecture by taking steps to make users more aware of their situation, their audience, and their information.

One step would be to map the privacy settings more closely to the content. Standard practices tend to segregate privacy preferences from the data they govern. This creates a gulf of Evaluation as users don't connect abstract access privileges to concrete personal data. danah boyd argues that privacy settings should be attached to the data they control:

> *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?*[194]

Another software tool that might help users bridge the gulf of Evaluation is the technology of "privacy mirrors" introduced by Mynatt and Nguyen. According to them, the real enemy of privacy practices in ubiquitous computing is not Big Brother but "interfaces

---

193 See boyd, "Putting Privacy Settings in the Context of Use." 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.

194 *Id.*

that do not give people the needed tools of awareness and control to comprehend and shape the behavior of the system."[195] According to Hong, just as real mirrors are used to police self-presentation in the physical world, "privacy mirrors provide useful feedback to users by reflecting what the system currently knows about them."[196]

Facebook recently implemented an embryonic privacy mirror known as the ViewAs function.[197] 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 developed enough to really tell users everything they need to know. The ViewAs function only allows users to look at their own profile page while wearing the "mask" of another user. Once a user clicks into the "Video" or "Photos" sections of the site, the mask disappears, and they are left wondering who can really see what. Furthermore, many users are completely unaware of the ViewAs function. It needs to be made more powerful and accessible before it achieves its true promise.

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 this sort of access feedback on user privacy.[198] 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.[199] In one condi-

---

195 See Mynatt and Nguyen at 1.

196 See Hong at 82.

197 It 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 wear the "mask" of.

198 See Cranor et al, "Who's Viewed You."; "Understanding and Capturing People's Privacy Preferences In a People-Finder Application."

199 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.

tion, 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 crucial to accurate privacy settings, as were tools that enhanced the salience of access:

> *[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. 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.*[200]

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. On their own, users generally had 59% accuracy with their initial rule set and 65% with the revised rules. When assisted by an automated case-based reasoning program that compared past decisions to present revisions, however, the accuracy skyrocketed to 82%.[201]

Cranor's findings also supports one of the key theoretical claims made in Section 3.1: 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.[202] Cranor concludes that:

---

200 See Cranor et al, "Who's Viewed You."

201 *Id.*

202 *Id* at 7.

> *[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 policies. Providing feedback to users about when and by whom they have been queried tends to make them more comfortable about sharing location information.*[203]

The most powerful privacy controls in the world aren't worth much if users lack the architectural cues that they rely on to situate them in a context or to inform them of the dynamics of disclosure. Gulfs of Evaluation prevent users from accurately appraising the effect of their settings and impair privacy. In order to create a better privacy architecture, Facebook should design an environment that provides users with social clarity and more accurate and salient feedback. Any environment that lacks these cues robs users of the necessary architectural conditions for the successful practice of privacy.

3.8: 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. This dynamic is completely counterintuitive and in no way respect user norms of distribution. danah boyd attributes many common privacy violations to the Strange Sharing Defaults that make a picture float around Facebook without its owner having any idea of who can view it.[204]

To be sure, defaults can be changed, but they rarely are,[205] leading Brown and Edwards to argue that defaults *disempower* users.[206] 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."[207] 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.

---

203 *Id* at 9.

204 See boyd, "Putting Privacy Settings in the Context of Use."

205 Again, according to Facebook CPO Chris Kelly, only 20% of users ever touch their privacy settings. See Stross.

206 See Edwards and Brown at 22.

207 See Kesan and Shah, "Setting Software Defaults" at 596.

The power of the default, however, is a tool, not a moral agent with an active 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."[208] 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.[209] The cognitive biases that drive users to discount privacy perils would still have been in play at the negotiating table and caused them to misapprehend the risks and enjoy the benefits of an open network until after they suffered a privacy event. Though the "would have wanted" standard is a good rule of thumb, it isn't appropriate for these circumstances.

Instead, *defaults should be modeled after the norms of distribution*. 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, the current defaults say that when a user joins the Boston network they intend to share every bit of their profile information with every member of that network even if they have never met and will never meet. No one expects this. It does not accord with norms of distribution. 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. They should 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

208 *Id* at 618.

209 See Edwards and Brown at 22.

them before they moved on to networking."[210] 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."[211] While Grimmelmann is substantively correct he is perhaps too dismissive of the merits of the idea. After all, even if Facebook users immediately turn off the privacy settings, at least they become informed that there *are* privacy settings and have to learn how to use them in order to shut them off.[212] Donald Norman might call this a "forcing function."[213] Like a dead man's switch, the affirmative effort required to turn off privacy settings can only have a beneficial educational effect.

Other forcing functions could be employed to consistently "nudge"[214] users into better privacy practices, as Cranor found when popup alerts informed and assisted users.[215] For instance, suppose user A is friends with user B. B has recently joined a company network for a company at which user A may someday want to work. This may change what A wants to share with B, especially if by default any friends of B can see any pictures of A. Facebook, of course, is aware of these changes in the network. Facebook might automatically prompt user A with a notice informing them 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 a "libertarian paternalistic"[216] approach to facilitating 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 the Boston network. Nobody is forced to have a private profile. However, if the defaults respect

---

210 *Id.*

211 See Grimmelmann, "Saving Facebook" at 37.

212 Recall from Section Section 2.8 that as much as a fifth of Facebook users don't even realize there *are* privacy settings.

213 See Norman, The Design of Everyday Things at 131.

214 See Thaler and Sunstein's Nudge.

215 See Cranor et al., "Who's Viewed You?"

216 See Thaler and Sunstein, "Libertarian Paternalism is Not an Oxymoron," also Nudge.

norms of distribution, than they also natively support user privacy practices. The power of the default can afford privacy rather than impairing it.

3.9 The Caveats of Code

Of course, the mere fact that an aspect of Facebook's design impairs contextual integrity is not sufficient cause to eliminate it. The ability to search may aid the collapse of contexts, for instance, but what use would Facebook be if no one could find their friends?[217] Automatic recording may harm contextual integrity, but what would Facebook be without semipermanent profile information? Few would give up their cellphones simply because they conflict with the norms about when and where one can be contacted. It isn't in anyone's interest to automatically eschew new technologies because they don't respect old norms. That's the point of progress.

However, neither is it in anyone's interest to simply assume that new technologies are worth their cost, or that the present design is at equilibrium. Facebook makes Friendship flat because it *chooses* to do so, not because of any law of nature or man saying that it must. Facebook's technological fictions may serve a utility, but they may also impede the practice of contextual integrity. The role of designers should be to implement systems that strike a balance between privacy interests and social dynamics. Two technologies that should be so evaluated are the existing News Feed and a hypothetical Viewer Tracking system.

During the first two years of Facebook any user who wanted to view content posted by a Friend had to manually access the their profile. Students would spend hours reading and rereading all of their Friend's profiles, looking for new photos, groups, or interests, a practice endearingly nicknamed "Facebook Stalking." This dynamic was largely in line with user norms of distribution, because generally in the physical world, people have to actively seek out information about other people.

---

217 When the forums of the popular comedy site SomethingAwful.com disabled their search functionality, it simultaneously angered the thousands of users who could no longer find content easily and relieved thousands more who were all too delighted to let intemperate past posts sink slowly into obscurity.

In September 2006 Facebook launched a feature called the "News Feed."[218] News Feed publishes all updates made by a user's Friends and to the user's home page. It was the same information, accessible to the same people, but now, instead of the users having to "pull" it from profiles, it was "pushed" to them by the News Feed. Users were outraged, and nearly 20% of all Facebook members joined a single group opposing the News Feed.[219]

Facebook (and many classical privacy scholars) was bewildered by the uproar over News Feed and the claims of violated privacy. Mark Zuckerberg told users to "calm down [and] breathe":

> *We didn't take away any privacy options. [Your privacy options remain the same.] The privacy rules haven't changed. None of your information is visible to anyone who couldn't see it before the changes. If you turned off your wall to non-friends, no one who is not your friend will be able to see a post on your wall. Your friends can still see it; it hasn't changed. Secret groups and secret events remain secret from other people. Pokes and messages remain as private interactions. Nothing you do is being broadcast; rather, it is being shared with people who care about what you do—your friends. This is information people used to dig for on a daily basis, nicely reorganized and summarized so people can learn about the people they care about."*[220]

Zuckerberg missed the point by about a mile. As James Grimmelmann explains:

> *The information wasn't exposed to the wrong people, wasn't particularly sensitive, and wasn't sent to a more public place. Instead, Facebook changed how profile update information flowed from users to their contacts. Pull (you visit my profile to check on me) and push (my activities are sent to you automatically) are socially different, so switching between them implicates privacy values.*[221]

While it's true that News Feed didn't change what information was accessible by which people, it changed the *dynamics* of the disclosure. It ran against the norm of distribution that makes people expect their information will circulate "close" to them. danah boyd likened the reaction to the News Feed to the sense of embarrassment one feels when,

---

218 See "Facebook | Timeline."

219 boyd, "Facebook's Privacy Trainwreck."

220 Zuckerberg, "Calm down. Breathe. We hear you."

221 See Grimmelmman, "Saving Facebook" at 24.

while screaming to be heard at a party, the music suddenly drops and everyone there can suddenly hear what one was saying.[222] Additionally, the News Feed cripples the ability of users to control what information is being pushed to them, in stark contrast with norms prescribing the right of the individual to choose what speech they'd like to receive.[223]

The obvious solution, from the standpoint of promoting contextual integrity, is to remove the News Feed entirely. Once the dynamics of disclosure return to a "pull" model, some of the beneficent inefficiency that previously protected privacy will return, and norms of distribution will be respected. At the same time, the News Feed provides some serious utility by informing users of updates made by people outside their "core networks" that they'd otherwise never check up on, a utility that may even serve broader democratic ideals.[224] Still, users are very vocal that it is not a perfect system. It should be redesigned and recalibrated to better balance social dynamics with privacy interests.

A similar social dilemma plagues any hypothetical feedback system. The research conducted by Cranor and her team at Carnegie Mellon would seem to support the introduction of a "Who's Viewed You" system that would notify users whenever a Friend accessed

---

222 See boyd, "Thinking Through Facebook's Privacy Trainwreck.": "Imagine that you are screaming to be heard in a loud environment when suddenly the music stops and everyone hears the end of your sentence. Most likely, they will turn to stare at you and you will turn beet red (unless exposure does not bother you). When the music was still chirping away, you were speaking loudly in a room full of people. You felt (and were) protected by the acoustics and you made a judgment about how loudly you should speak based on your understanding of the architecture of the environment...privacy is not simply about zeros and ones, it is about how people experience their relationship with others and with information. Privacy is a sense of control over information, the context where sharing takes place, and the audience who can gain access."

223 This harm is more like an intrusion or a limitation on personal autonomy, not contextual integrity, so I will not deal with it in the body of the text. Furthermore, the feature is so new that it is still to early to fairly judge its impact. However, I believe it may introduce a new sort of privacy problem to Facebook: the problem of "too much information", or "TMI." There may be instances in which one user wishes to remain Friends with another but also wants to limit the amount of information being pushed at him or her by that user. For example, one college student I know described a similar experience after he broke up with his girlfriend. They were still friendly, and he did not want to terminate the Facebook Friendship. However, he was deluged by her photo updates in the News Feed and the Highlight Feed, many of which featured pictures of her on dates or hooking up with other men. This understandably upset him, so he tried to limit both feeds such that her photo updates were eliminated. To his amazement, he found that the News Feed only allowed him to see everything or nothing she posted, rather than discriminating by content, and that the Highlight Feed could not be modified at all! There was nothing he could do, short of deFriending her, that would keep these photos from being pushed at him. This potentially could comprise a new sort of privacy problem that is more amenable to the tort of intrusion upon seclusion, because the harm derives from being unable to sequester oneself away from information one does not wish to receive. Suffice it to say that it is both a privacy problem and an architectural nigthmare. As an aside, I cannot imagine why Facebook does not allow this functionality. This particular student of whom I speak is certainly not alone in his concern. As of April 25 2009, many thousands of requests for the ability to modify the Highlights Feed have been filed on the Facebook website to no avail. See http://www.facebook.com/help.php?hq=highlights&ref=hq.

224 For more about the dangers that echo chambers and self-selecting core networks may pose to democracy, see Sunstein.

their profile and inform the user what content their Friend viewed. 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. It seems like a no-brainer.

And yet, such a Viewer Tracking system would undoubtably clash with strong social norms on Facebook. "Facebook Stalking", to one degree or another, remains an accepted practice. Most users know that sometimes Friends of theirs - whether out of an earnest interest or a lascivious intent - will occasionally linger on their profiles, flip casually through their photos, and browse through their interests. However, if this activity were shone under the bright 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.

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 should create a serious, deliberative discussions that weigh 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. There is zero evidence that such discussions are currently taking place within Facebook or without. That needs to change.

There may be instances in which code cannot fix the problem. Grimmelmann has estimated that technical controls alone can never solve more than 80% of the privacy violations experienced on Facebook,[225] an estimation that is remarkably in line with Cranor's finding that even machine-aided user rules rarely surpass 80% accuracy when determining user disclosure.[226] This is probably accurate. Code can never recapture robust relationships, and any privacy will necessarily be loosely typed and not airtight.

---

225 Personal correspondence with James Grimmelmann.

226 See Cranor et al., ""Understanding and Capturing People's Privacy Preferences In a People-Finder Application" at 4.

However, 80% of privacy problems prevented is significantly better than the status quo, where the vast majority of users never touch the default privacy settings, can't comprehend their privacy environment or its architectural cues, and are privacy trainwrecks waiting to happen. Code can't provide airtight privacy protection, but it can certainly comparatively improve the situation by making it easier for users to understand and interact with their Friends on Facebook in ways that maintain contextual integrity and preserve privacy.

Conclusion: Saving Face

In a 1995 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 doesn't socialize with any of George's friends and is thus outside their "world," but he fears that if his fiancee 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!*
>
> *JERRY: I didn't know...about the worlds!*
>
> *GEORGE: You couldn't figure out the "World's Theory" for yourself? It's just common sense. Anybody knows ya gotta keep your worlds apart! [You're] all killing independent George! Worlds are colliding!*[227]

George isn't concerned about his "privacy" as it is normally understood, which is to say he isn't worried about some secret information being ripped from his private life and exposed to a ravenous and voyeuristic public. He isn't going to suffer an intrusion upon his seclusion, a public disclosure of a private fact, or any of the other common privacy violations recognized by law and society. Instead, he worries that the walls separating "Independent

227 See "The Pool Guy" from *Seinfeld*.

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. The worlds that had collided become separate again.

On Facebook, it's not so simple. While the properties of the physical world 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.

This is a problem for users, and it is a problem of privacy. But unlike many privacy problems, this is not one that law or markets can solve. This is a job for code. Code cannot solve every privacy problem. Technological skepticism is justified. However, there are concrete steps that can be taken to build a better privacy architecture on Facebook. There are specific things that can be done to design an environment that makes privacy practices easier and more intuitive to accomplish. Providing users with the technological tools and architectural cues needed to practice privacy is the first step to helping them contextualize, situate, and define themselves on Facebook. And in a world where drinking buddies hang with grandmothers, it is the first step to saving face.

BIBLIOGRAPHY

The following is a record of all sources consulted at any point during the research for this thesis, regardless of whether they were cited in the body of the text. Refer to footnotes for specific citations. All web addresses are accurate as of May 2009.

- All personal correspondence is on file with the author and available upon request at cpeterson@umasslegal.org
- Abril, Patricia. "A mySpace of One's Own: On Privacy and Social Networks." 6 Nw. J. Tech. & Intell. Prop. 73, 2007.
- Acquisti, Alessandro. "Privacy in Electronic Commerce and the Economics of Immediate Gratification." *Proceedings of the ACM Electronic Commerce Conference (ACM EC)*. ACM. 21-29, 2004. Available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-gratification.pdf.
- Acquisti, Alessandro and Jens Grossklags. "Privacy and Rationality in Individual Decision Making." IEEE Security and Privacy, 3(1), 26-33, 2005. Available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti.pdf.
- Acquisti, Alessandro and Ralph Gross. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." *Proceedings of Privacy Enhancing Technologies Workshop (PET)*, Lecture Notes in Computer Science. Ed. Springer, Volume 4258, p. 36-58, 2006. Available at http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf.
- Acquisti, Alessandro and Ralph Gross. "Privacy and Information Revelation in Online Social Networks: The Facebook Case." *11th Colloquium for Information Systems Security Education (CISSE)*. Boston, 2007. Available at http://www.heinz.cmu.edu/~acquisti/papers/privacy-facebook-gross-acquisti.pdf.
- Altman, Irwin. The Environment and Social Behavior. Belmont: Wadsworth Publishing Co, 1975.
- Ariely, Dan. "Predictably Irrational: The Hidden Forces That Shape Our Decisions." New York: HarperCollins, 2008.
- Aristotle. "The Nichomachean Ethics." Aristotle in 23 Volumes. Vol. 19, book 8. Translated by H. Rackham. Cambridge: Harvard University Press, 1934.
- Arrington, Michael. "85% of College Students Use Facebook." TechCrunch. September 7 2005. Available at http://www.techcrunch.com/2005/09/07/85-of-college-students-use-facebook/.
- Arthur, W. Brian. Increasing Returns and Path Dependence in the Economy. Ann Arbor: University of Michigan Press, 1997.
- Brandenberg, Carly. "The Newest Way to Screen Job Applicants: A Social Networker's Nightmare." 60 Fed. Comm. L.J. 597, 2008.
- Beardsley, Elizabeth. "Privacy, Autonomy, and Selective Disclosure." NOMOS XIII. Ed. Pennock and Chapman. Atherton Press, 1971. p. 65.
- Beaver, Doug. "10 Billion Photos." Facebook Engineering Blog. October 14th 2008. Available at http://www.facebook.com/note.php?note_id=30695603919.

- boyd, danah. "Facebook's Privacy Trainwreck: Exposure, Invasion, and Social Convergence." Convergence, Volume 14, p. 13-20, 2008. Sage Publications. Public draft at http://www.danah.org/papers/FacebookAndPrivacy.html.
- boyd, danah. "Faceted/Id: Managing Representation in a Digital World." Unpublished MIT master's thesis. August 2002. Available at http://www.danah.org/papers/Thesis.FacetedIdentity.pdf.
- boyd, danah. "Friends, friendsters, and top 8: Writing community into being on social network sites." FirstMonday. Volume 11, Number 12, 2006. Available at http://www.firstmonday.org/issues/issue11_12/boyd/.
- boyd, danah. "My Friends, MySpace: American Youth Socialization on Social Network Sites." The Berkman Center For Internet and Society. Produced June 2007. Available at http://cyber.law.harvard.edu/interactive/events/luncheon/2007/06/boyd.
- boyd, danah. "Putting Privacy Settings in the Context of Use (in Facebook and elsewhere)." Apophenia Blog. Posted October 22 2008. Accessed October 24 2008. Available at http://www.zephoria.org/thoughts/archives/2008/10/22/putting_privacy.html.
- danah boyd. "Reflections on Friendster, Trust and Intimacy." *Ubiquitous Computing (Ubicomp 2003), Workshop application for the Intimate Ubiquitous Computing Workshop*. Seattle, WA, October 12-15, 2003. Available at http://www.danah.org/papers/Ubicomp2003WorkshopApp2.pdf.
- boyd, danah. "Sociable Technology and Democracy." Extreme Democracy. Ed Lebkowsky and Ratcliffe. 2005. Available at http://www.danah.org/papers/ExtremeDemocracy.pdf.
- boyd, danah. "Social Network Sites: Public, Private, or What?" The Knowledge Tree. May 2007. Available at http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-network-sites-public-private-or-what/.
- boyd, danah. "Taken Out of Context: American Teen Sociality In Networked Publics." PhD Dissertation, University of California-Berkeley, School of Information, 2008. Available at http://www.danah.org/papers/TakenOutOfContext.pdf.
- boyd, danah. "The Significance of Social Software." BlogTalks Reloaded. Social Software - Research & Cases. Ed. Burg and Schmidt. Norderstedt: Books on Demand. Available at http://www.danah.org/papers/BlogTalksReloaded.pdf.
- boyd, danah. "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life." *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume.* Ed. Buckingham. Cambridge, MA: MIT Press 2007. Available at http://www.danah.org/papers/WhyYouthHeart.pdf.
- boyd, danah and Jeffrey Heer. "Profiles as Conversation: Networked Identity Performance on Friendster." *In Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39), Persistent Conversation Track.* Kauai, HI: IEEE Computer Society. January 4 - 7, 2006. Available at http://www.danah.org/papers/HICSS2006.pdf.
- boyd, danah and Nicole Ellison. "Social network sites: Definition, history, and scholarship." Journal of Computer-Mediated Communication. Volume 13, article 11, 2007. Available at http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.
- Brockriede, Wayne and Robert L. Scott. "Stokely Carmichael: Two Speeches on Black Power." Language, Communication, and Rhetoric in Black America. Ed. Smith. New York: Harper and Row, 1972.

- Chapman, John W. "Personality and Privacy." NOMOS XIII. Ed. Pennock and Chapman. Atherton Press, 1971. p. 235.
- Cohen, Jodi. "Cop snares college pals in own Web." Chicago Tribune (Chicago, IL) (August 3, 2006): NA. General OneFile. Gale. Univ Mass Amherst. Accessed April 9 2009. http://find.galegroup.com/itx/start.do?prodId=ITOF.
- Colurso. "Making connections Freshmen start college with pre-assembled crews gathered from a variety of places." Birmingham News. LIFESTYLE; Pg. 1E Vol. 118 No. 138. August 21 2005.
- *Couch v. U.S*, 409 U.S. 322. 1973
- Cranor, Lorrie, Jason Hong, 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*. ACM, New York, NY. p. 2003-2012, 2009. DOI= http://doi.acm.org/10.1145/1518701.1519005. Available at http://www.cs.cmu.edu/~sadeh/Publications/Privacy/CHI2009.pdf.
- Cranor, Lorrie, Alessandro Acquisti et al. "What's It To You? A Survey of Online Privacy Concerns and Risks." NET Institute Working Paper No. 06-29. Available at http://ssrn.com/abstract=941708.
- Cranor, Lorrie, Jason Hong, et al. "Understanding and Capturing People's Privacy Policies in a People Finder Application." Journal of Personal and Ubiquitous Computing. Ed. Springer. 2008. Available at http://www.cs.cmu.edu/~jasonh/publications/puc2008-peoplefinder-final.pdf.
- Edwards, Lilian and Ian Brown. "Data Control and Social Networking: Irreconcilable Ideas?" Harboring Data: Information Security, Law and the Corporation, Ed. Matwyshyn. Stanford University Press, forthcoming 2009. This thesis refers to a draft of the chapter, provided by Ian Brown and available at http://ssrn.com/abstract=1148732.
- Ellison, Nicole et al. "The Benefits of Facebook "Friends:" Social Capital and College Students' Use of Online Social Network Sites." Journal of Computer-Mediated Communication, Volume 12, Issue 4, article 1, 2007. Available at http://jcmc.indiana.edu/vol12/issue4/ellison.html.
- *Ettore v. Philco Television Broadcasting Co*., 229 F.2d 481 (3d Cir. 1956)
- "Facebook | Free Flow of Information on the Internet." Facebook.com. Accessed April 26 2009. Available at http://www.facebook.com/group.php?gid=2208601394&ref=ts.
- "Facebook | Timeline." Facebook. Accessed May 2009. Available at http://www.facebook.com/press/info.php?timeline.
- "Facebook Remark Teenager Is Fired." BBC. February 27 2009. Available at http://news.bbc.co.uk/2/hi/uk_news/england/essex/7914415.stm.
- Fahey, Tony. "Privacy and the Family: Conceptual and Empirical Reflections." Sociology. 29, p. 687, 1995. DOI: 10.1177/0038038595029004008. Available at http://soc.sagepub.com/cgi/content/abstract/29/4/687.
- Fried, Charles. "Privacy." 77 YLJ 475, 1968.
- Friedrich, Carl J. "Secrecy vs. Privacy, The Democratic Dilemma." NOMOS XIII. Ed. Pennock and Chapman. Atherton Press, 1971. p. 105.

- Gentile, Carmen. "Student Fights Record of 'Cyberbullying.'" New York Times. February 8 2009, page A20. Also available at http://www.nytimes.com/2009/02/08/us/08cyberbully.html.
- Gilbert, Dan. "How we are deceived by our own miscalculations of the future." TED. Filmed July 2005. Available at http://www.ted.com/index.php/talks/dan_gilbert_researches_happiness.html.
- Grimmelmann, James. "Accidental Privacy Spills." Journal of Internet Law, July 2008; NYLS Legal Studies Research Paper No. 07/08-35. Available at http://ssrn.com/abstract=1147195.
- Grimmelmann, James. "Regulation by Software." 114 Yale L.J. 1719, 2005.
- Grimmelmann, James. "Saving Facebook." Iowa Law Review, vol. 95, forthcoming in 2009. This thesis refers to a draft of the article, entitled "Facebook and the Social Dynamics of Privacy" and available at http://ssrn.com/abstract=1262822.
- Grossklags, Jens et al. "E-privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior." *Proceedings of EC'01: Third ACM Conference on Electronic Commerce*, ACM, Tampa, p. 38-47, 2001. Available at: http://people.ischool.berkeley.edu/~jensg/research/paper/grossklags_e-Privacy.pdf.
- Gruden, Jonathan. "Desituating Action: Digital Representation of Context." Human Computer Interaction. Volume 16, Issue 2, p. 269-286, 2001. Part of the Microsoft HCI Research Paper series. Available at http://research.microsoft.com/en-us/um/redmond/groups/coet/grudin/hci-contextaware.pdf.
- Hodge, Matthew. "The Fourth Amendment and Privacy Issues on the 'New' Internet: Facebook.com and MySpace.com." 31 S. Ill. U. L. J. 95, 2006.
- Hoffman, Claire. "The Battle for Facebook." Rolling Stone. June 26 2008. Available at http://www.rollingstone.com/news/story/21129674/the_battle_for_facebook.
- Hong, Jason and Giovanni Iachello. "End-User Privacy in Human–Computer Interaction." Foundations and Trends in Human–Computer Interaction. Vol. 1, No. 1, p. 1–137, 2007. DOI: 10.1561/1100000004.
- Kaplan, Katharine. "FaceMash Creator Survives Ad Board." The Harvard Crimson. November 19 2003. Available at http://www.thecrimson.com/article.aspx?ref=350143.
- Katsh, Ethan. Law In A Digital World. Oxford: Oxford University Press, 1995.
- Katsh, Ethan. "Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace." U Chi Legal F 335, 1996.
- Kesan, Jay and Rajiv Shah. "Setting Software Defaults: Perspectives from Law, Computer Science, and Behavioral Economics." 82 Notre Dame L. Rev. 583, 2006. Available at http://ssrn.com/abstract=906816.
- Kramer, Nicole and Stephen Winter. "Impression Management 2.0 The Relationship of Self-Esteem, Extraversion, Self-Efficacy,and Self-Presentation Within Social Networking Sites." Journal of Media Psychology. Volume 20, Issue 3, p 96-106. DOI10.1027/1864-1105.20.3.96
- Kranzberg. "Technology and History:'Kranzberg's Laws." Technology and Culture. Vol. 27, No. 3,p. 544-560, 1986.

- Krebs. "Court Rules Against Teacher in MySpace 'Drunken Pirate' Case." The Washington Post. December 3 2008. Available at http://voices.washingtonpost.com/securityfix/2008/12/court_rules_against_teacher_in.html.
- Lash, Devon. "Site Used To Aid Investigation." The Daily Collegian. November 10 2005. Available at http://www.collegian.psu.edu/archive/2005/11/11-10-05tdc/11-10-05dnews-09.asp
- "Legal Fiction." Black's Law Dictionary. 5th Edition. West Publishing, St. Paul, Minnesota, 1979.
- Lessig, Lawrence. Code: Version 2.0. New York: Basic Books, 2006.
- Lessig, Lawrence. "Reading the Constitution in Cyberspace." 45 Emory L.J. 869, 1996. Available at http://ssrn.com/abstract=41681.
- Lessig, Lawrence. "The Architecture of Privacy." 1 Vand. J. Ent. L. & Prac. 56, 1999. Available at http://cyber.law.harvard.edu/works/lessig/architecture_priv.pdf.
- Lewis, Kevin et al. "Tastes, ties, and time: A new social network dataset using Facebook.com." Social Networks. Volume 30, Issue 4, p.330-342, 2008. Available at http://dx.doi.org/10.1016/j.socnet.2008.07.002.
- Levy, "The Ladettes Who Glorify Their Shameful Drunken Antics on Facebook." The Daily Mail. November 5 2007. Available at http://www.dailymail.co.uk/news/article-491668/The-ladettes-glorify-shameful-drunken-antics-Facebook.html.
- Livingstone, Sonia. "Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self- expression." New Media & Society. Volume 10, p. 393-411, 2008. DOI: 10.1177/1461444808089415.
- Mayer, Adalbert and Steven Puller. "The old boy (and girl) network: Social network formation on university campuses." Journal of Public Economics. Volume 92, p 329 – 347, 2008.
- Meyrowitz, Joshua. No Sense of Place: The Impact of Electronic Media on Social Behavior. New York and Oxford: Oxford University Press, 1985.
- *Miller v. U.S.*, 425 U.S. 435, 1976.
- Mynatt, Elizabeth and 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.
- Nissenbaum, Helen. "Privacy as Contextual Integrity." 79 Wash. L. Rev. 119, 2004. Available at http://ssrn.com/abstract=534622.
- Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." Law and Philosophy, Vol 17, 559-596, 1998. Available at http://ssrn.com/abstract=139144.
- Norman, Donald. The Design of Everyday Things. New York: Basic Books, 1988.
- Norman, Donald. Things That Make Us Smart. Reading, UK: Addison-Wesley, 1993,

- Olson, J.S., et al. "A study of preferences for sharing and privacy." *Proceedings: CHI '05 Extended Abstracts on Human Factors in Computing Systems (Portland, OR, USA, April 02 - 07, 2005).* Available at http://research.microsoft.com/en-us/um/people/horvitz/privacy_chi2005.pdf.

- O'Neill, Nick. "Facebook Demographics." AllFacebook. January 14th 2009. Available at http://www.allfacebook.com/2009/01/facebook-demographics-country-saturation/.

- Palen, Leysia and Paul Dourish. "Unpacking 'Privacy' for a Networked World." *CHI Letters (Human Factors in Computing Systems: CHI 2003),* vol. 5, no. 1, pp. 129–136, 2003.

- Patil, Sameer and Jennifer Lai. "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).* ACM. p. 101-110, 2005. DOI= http://doi.acm.org/10.1145/1054972.1054987

- Peterson, Chris. "High School Facebook." The Virginia Informer. October 2005. Available at http://web.wm.edu/so/virginiainformer/archives/oct2005/highschoolfacebook.php

- "Primates on Facebook." The Economist. February 26 2009. Available at http://www.economist.com/science/displaystory.cfm?story_id=13176775.

- Prosser, William. "Privacy." 48 Cal. L. Rev 383, 1960. Available at http://www.jstor.org/stable/3478805.

- Rachels, James. "Why Privacy Is Important." Philosophy and Public Affairs. Vol 4 No 4, p. 323-333, 1975. Available at http://www.jstor.org/stable/2265077.

- Reidenberg, Joel. "Lex Informatica: The Formulation of Information Policy Rules Through Technology." 76 Tex. L. Rev. 553, 1997.

- "Respectfully Quoted." Library of Congress. Available online at http://www.credoreference.com.silk.library.umass.edu.

- Rosen, Jeffrey. "Privacy in Public Places." 12 Cardozo Stud. L. & Lit. 167, 2000.

- Rosen, Jeffrey. "The Unwanted Gaze: The Destruction of Privacy in America." New York: Random House, 2000.

- Rotenberg, Marc. "Fair Information Practices and the Architecture of Privacy." 2001 Stan. Tech. L. Rev. 1, 2001.

- Samuelson, Robert J. "A Web of Exhibitionists." The Washington Post. September 20th 2006. Available at: http://www.washingtonpost.com/wp-dyn/content/article/2006/09/19/AR2006091901439.html

- Schweitzer, Sarah. "Fisher College expels student over website entries." The Boston Globe. October 6 2005. Available at http://www.boston.com/news/local/articles/2005/10/06/fisher_college_expels_student_over_website_entries/.

- Shea, Danny and Matthew Feinstein. "An open letter to Mark Zuckerberg." The Daily Princetonian. March 9 2006. Available at http://www.dailyprincetonian.com/2006/03/09/14810/.

- Shelmire, Aaron. "Social Networks and the Professional/Private Life Boundary." Unpublished graduate research paper conducted for Dr. Lorrie Cranor at Carnegie Mellon University, 2008. On file with author.

- Shirky, Clay. "Here Comes Everybody: The Power of Organizing Without Organizations." New York: Penguin Group, 2008.
- Shirky. "Interview for AOL Switched." AOL Switched. Interview by Benjamin Chertoff, 2007. Available at http://video.aol.com/video-detail/benjamin-chertoff-switched-shirky/1153013873.
- Shirky, Clay. "RELATIONSHIP: A vocabulary for describing relationships between people." Many2Many. Posted March 16 2004. Accessed October 8 2008. Available at http://many.corante.com/archives/2004/03/16/relationship_a_vocabulary_for_describing_relationships_between_people.php.
- "Sophos ID Probe Shows 41% of Users Happy to Reveal All to Potential Identity Thieves." SOPHOS. Posted August 14 2007. Available at http://www.sophos.com/pressoffice/news/articles/2007/08/facebook.html.
- Solove, Daniel J. "A Taxonomy of Privacy." 154 U. Pa. L. Rev. 477, 2006. Available at http://ssrn.com/abstract=667622.
- Solove, Daniel J. "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy." 44 San Diego L. Rev. 745, 2007. Available at http://ssrn.com/abstract=998565.
- Solove, Daniel J. The Future of Reputation: Gossip, Rumor, and Privacy on the Internet. New Haven and London: Yale University Press, 2008. Also available at http://docs.law.gwu.edu/facweb/dsolove/Future-of-Reputation/text.htm.
- Stone, Brad. "Is Facebook Growing Up Too Fast?" New York Times. March 29 2009. Available at http://www.nytimes.com/2009/03/29/technology/internet/29face.html?_r=1&ref=technology&pagewanted=print.
- Strahilevitz, Lior. "A Social Networks Theory of Privacy." 72 U. Chi. L. Rev. 919, 2005. Available at http://ssrn.com/abstract=629283.
- Stross, Randall. "When Everyone's a Friend, Is Anything Private?" The New York Times. March 7 2009. Available at http://www.nytimes.com/2009/03/08/business/08digi.html.
- Stumpf et al. "Toward harnessing user feedback for machine learning." *Proceedings of the 12th international Conference on intelligent User interfaces (Honolulu, Hawaii, USA, January 28 - 31, 2007). IUI '07*. ACM, New York, NY, 82-91. DOI= http://doi.acm.org/10.1145/1216295.1216316. Available at http://portal.acm.org/citation.cfm?doid=1216295.1216316.
- Sunstein, Cass. Republic.com 2.0: Revenge of the Blogs. Princeton and Oxford: Princeton University Press, 2007.
- Tabak, Alan. "Hundreds Register for New Facebook Website." The Harvard Crimson. February 9 2004. Available at http://www.thecrimson.com/article.aspx?ref=357292.
- Thaler, Richard and Cass Sunstein. "Libertarian Paternalism Is Not an Oxymoron." 70 U. Chi. L. Rev. 1159, 2003.
- Thaler, Richard and Cass Sunstein. Nudge: Improving Decisions About Health, Wealth, and Happiness. New Haven and London: Yale University Press, 2008.
- "The Pool Guy." *Seinfeld*. Episode 118. Originally aired on November 16 1995. Written by David Mandel. Script available at http://www.seinfeldscripts.com/ThePoolGuy.html. "Independent George" sketch available at http://www.youtube.com/watch?v=SxuYdzs4SS8.

- Tien, Lee. "Architectural Regulation and the Evolution of Social Norms." International Journal of Communications Law & Policy. Issue 9, 2004.
- Tufecki, Zeynep. "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. DOI:10.1177/0270467607311484.
- Warren, Samuel and Louis Brandeis. "The Right to Privacy." 4 Harv. L. Rev. 193, 1890.
- Wortham, Jenna. "Facebookers Approve New Policy, but Still Hate Redesign." New York Times Bits Blog. April 24 2009. Available at http://bits.blogs.nytimes.com/2009/04/24/facebookers-approve-new-policy-still-hate-redesign/.
- Wu, Tim. "The International Privacy Regime." Securing Privacy In The Internet Age. Ed. Radin and Chander. Palo Alto: Stanford University Press, 2005. Available at http://ssrn.com/abstract=630961.
- Zittrain, Jonathan. "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
- Zittrain, Jonathan. "Berkman Book Release: The Future of the Internet And How To Stop It." Harvard Law School. April 2008. Available at http://cyber.law.harvard.edu/interactive/events/2008/04/zittrain.
- Zittrain, Jonathan. "Facebook's Privacy Storm." futureoftheinternet.org. Posted February 18th 2009. Accessed February 19th 2009. Available at http://futureoftheinternet.org/facebooks-privacy-storm.
- Zittrain, Jonathan. The Future of the Internet - And How To Stop It. New Haven and London: Yale University Press, 2008.
- Zittrain, Jonathan. "What The Publisher Can Teach The Patient: Intellectual Property and Privacy in an Era of Trusted Privication." 52 Stan. L. Rev. 1201. Available at http://ssrn.com/abstract=214468.
- Zittrain, Jonathan and Peter Thiel. "Can Monopolies Save The Internet?" The Berkman Center for Internet and Society. Debate between Professor Jonathan Zittrain and Peter Thiel. Filmed April 2009. Available at http://bigthink.com/berkmancenter/can-monopolies-save-the-internet.
- Zuckerberg, Mark, "An Open Letter from Mark Zuckerberg." Facebook. September 8 2006. Available at http://blog.facebook.com/blog.php?post=2208562130.
- Zuckerberg, Mark. "Calm down. Breathe. We hear you." Facebook. September 6 2006. Available at http://blog.facebook.com/blog.php?post=2208197130.