The Silicon Flatirons Roundtable Series on Entrepreneurship, Innovation and Public Policy
Report No. 6*

The Social, Ethical, and Legal Implications of Social Networking

John Bergmayer, Rapporteur

Executive Summary

The roundtable debated several issues related to social software, focusing on:

- The pros and cons of social software as a replacement for or adjunct to real-life social interactions;
- The way that the debate over social software is influenced by sensational media accounts;
- Whether online networks (considered by themselves or in conjunction with the Internet as a whole) display features of complex and self-emergent systems;
- What "privacy" really means in an age of widespread sharing, and what can replace a simplistic division between "public" and "private";
- Reputational and other harms that can arise from social software;
- Whether the solutions to various "privacy" issues should be regulatory or left to emerge spontaneously, and whether the architecture of social software determines what kinds of solutions are possible;
- Examples of such solutions.

Overview

On January 22, 2009, the Silicon Flatirons Center for Law, Technology, and Entrepreneurship held a roundtable discussion on social networking issues at the ATLAS Building on the University of Colorado campus in Boulder, Colorado. This roundtable brought together a diverse group of participants, ranging from academics to venture capitalists to practicing lawyers to entrepreneurs. A full list of attendees and their affiliations can be found in the appendix accompanying this report.

---

* The Silicon Flatirons Roundtable Series on Entrepreneurship, Innovation and Public Policy is sponsored by Brad Feld, Managing Director of the Foundry Group. This discussion on "The Social, Ethical, and Legal Implications of Social Networking" followed earlier ones on (1) The Unintended Consequences of Sarbanes-Oxley, (2) Rethinking Software Patents, (3) The Entrepreneurial University, (4) The Private Equity Boom, and (5) The Promise and Limits of Social Entrepreneurship. The reports from those discussions can be found at http://www.silicon-flatirons.org/publications.php?id=report.

The roundtable, which began with an overview by Phil Weiser, Silicon Flatirons' Founder and Executive Director, who underscored the basic ground rules of the discussion—no one would be quoted without permission and that the discussion would be "off the record" until this report was published. Nonetheless, the regular refrain—repeated by several participants—that "in the Internet world, privacy is irrelevant" suggested a possible tension in having a private discussion about social networking technologies and the implications for privacy and personal reputation. That tension became pronounced when Robert Reich, Founder of OneRiot and the Organizer of the New Technology Meetup, asked the assembled group if they realized that Micah Baldwin, the Founder and CEO of Current Wisdom, was Twittering throughout the discussion—in effect, broadcasting the comments made by participants in real-time.

To many of the assembled participants, the news that one of those in attendance was relaying the conversation in real-time struck them as a blatant violation of the ground rules. To others, the news was a perfect metaphor for social networking and the challenges of controlling one's reputation in the Internet age, where the sharing of information is easy and nearly impossible to contain. To that end, we are all now in the position faced by the "Star Wars kid"—someone made famous by the posting of his (unintentionally) humorous video which led to massive taunting.[1] Micah, in his defense, suggested that he had not attributed any of the comments to individuals while engaging in his usual practice of sharing his thoughts with those who followed him on Twitter.

The challenge posed by the ubiquitous use of social networking, or "Web 2.0," technologies like Twitter, Facebook, and YouTube is that they allow the broadcasting of information that was not intended to be shared, cannot easily be corrected, and is stored (and available via a simple Google search) for years or decades. The privacy concerns related to this phenomenon dominated the discussion of the implications of social networking despite Weiser's attempt to highlight other critical issues, such as the impact of such technologies on the workplace, government, and politics as well as what competition policy issues arise in this context. Consequently, this report will mostly explore the themes related to privacy.

The principal takeaway from the discussion was that policymakers need to develop a more sophisticated understanding of the proper uses of personal information that takes into account the full complexities of human relationships and accounts for the fact that a use that may be appropriate in one context may not be appropriate in another. There was less agreement as to what those proper uses actually are. While "privacy" remains a driving concern relating to the growth of social networks, perhaps the key privacy challenge is defining what, in fact, privacy is. While there were numerous viewpoints represented on various topics related to the challenges of protecting privacy in the Internet era, the discussants were in agreement that the issue of privacy is not susceptible to easy answers.

[1] *See* Wikipedia, Star Wars Kid, http://en.wikipedia.org/wiki/Star_Wars_kid.

The Roundtable

Social networking is one of the most notable recent developments in the evolution of the Internet, with the use of social networking sites growing among all demographic groups.[2] The roundtable was convened in order for the Colorado business, legal, and academic community to discuss the social, political, and policy implications of the rise of social networking. While commercially-oriented sites oriented to a general audience such as Facebook, Myspace, and Twitter were the focus of the discussion, related trends such as online collaboration (e.g., Wikipedia and open source software) and the effect of the blogosphere were also discussed.

Introductory Remarks

Professor Weiser set out a roadmap for the roundtable, suggesting that the discussants focus on how social networking has (1) influenced our understanding of the nature of reputation and privacy; (2) affected the nature of community, discourse, and political deliberation; and (3) heightened concerns about the ownership of data, network effects, and consumer lock-in. Before opening up the roundtable, he turned over the discussion to John Gastil, and then Dan Kahan, who gave their thoughts on the topic and summarized some of their research.

John Gastil, Professor of Communications at the University of Washington, offered a nuanced take on the nature of social software and online collaboration, pointing out both benefits and hazards. Gastil pointed out instances where online collaboration has been clearly successful, such as Wikipedia, open source software, and the use of tools such as Twitter and Facebook in the 2008 presidential election. Wikipedia and open source software, for instance, demonstrate the good results that can result from communities of experts. Social networking technology has had cultural benefits, as well. People with minority tastes are able to connect with each other, and even meet up in the real world. Star Trek conventions, for instance, were difficult to organize and publicize in the 1970s, but today, like-minded people can find each other very easily.

Gastil also emphasized the deficiencies of purely online movements, observing that the transformative nature of social campaigns such as the feminist movement has yet to be matched by anything seen online. The downside of social networking sites is potential loss of intimacy, as people replace physical interaction with its online counterpart. He said that people's networks of close, in-person friends (and not just online "friends") are smaller today than they were twenty years ago. Additionally, he stated that the availability of government records online, ready to be analyzed by distributed teams of volunteers who connect through social networking sites, is often touted as a benefit of the Internet age that could lead to better governance. However, he observed that a wealth of information does necessarily lead to an abundance of wisdom. By what standards, he asked, do you judge a "transparent" government that releases many unedited records online? Very few people may be equipped to put such information to use. He also cited

---

[2] Amanda Lenhart, Adults and Social Network Websites, http://www.pewinternet.org/pdfs/pip_adult_social_networking_data_memo_final.pdf (describing the increased use of social networks by adults).

the "echo chamber" effect found in the blogosphere,[3] and worried that government might come to rely too heavily on "crowd-sourced" received wisdom, avoiding accountability for tough choices.

Online movements, such as the "netroots" who first mobilized in support of the candidacy of Howard Dean[4] (and later Barack Obama), tend to be focused on limited ends, and can dissipate when their initial motivation ends. By contrast, because traditional social movements involved in-person organizing and activism, they tended to be more personally transformative, and the movements, though perhaps initially formed for limited ends, continued to grow, transform, and change lives. It has yet to be shown that online political engagement has the potential to be as transformative as the feminist or civil rights movements. In sum, Gastil is aware of the promise of online collaboration, but cautions us as to the hazards of replacing face-to-face communication with interactions that are primarily mediated by technology.[5]

Dan Kahan, a Professor at Yale Law School, offered a different take than Gastil, placing the advent of social networking in a more optimistic light. He began by noting that, in his view, much of the debate about social networking reflects both confusion and alarmism. In particular, he suggested, the debate is confused insofar as words such as "privacy" are used to refer to distinct ideas and concerns. Much controversy, for instance, surrounds the commercial use of data that people have voluntarily disclosed and made "public." There is also widespread concern about the way that the Internet facilitates malicious behavior, such as harassment and rumor-mongering. Here, the underlying bad acts are not new; the concern is that the Internet facilitates these kinds of communication as well as the "good" kinds that Gastil noted earlier. In other words, for good and ill, the Internet makes *existing* kinds of actions and behaviors more efficient; it does not necessarily bring something new to the world. Merchants have always sought to learn about their customers, but today Amazon can gather precise data and, consequently, make useful book recommendations. In other words, consumers might have amorphous fears about such data being gathered, but they have concrete gains. He also stressed that much of the debate suffers from excessive attention to rare events, such as instances of child predation.[6] Unusual events

---

[3] *See* Eszter Hargittai, Jason Gallo, & Matthew Kane, *Cross-Ideological Discussions Among Conservative and Liberal Bloggers*, 134 PUBLIC CHOICE 67, 67 ("[w]e find that widely read political bloggers are much more likely to link to others who share their political views"), *available at* http://www.springerlink.com/content/p7m41t21344130t7/fulltext.pdf; Emily Eakin, *Study Finds a Nation of Polarized Readers*, N.Y. TIMES, Mar. 13, 2004, at B9 (describing research showing that people's book-buying habits on large Internet bookstores are similarly ideologically polarized).

[4] The term "netroots," meaning both a grassroots campaign conducted primarily through the Internet, and the participants in such a campaign, was first coined in 2004 by political strategist Jerome Armstrong. *See* Netroots for Dean in 2004, MyDD.com, *archived page available at* http://web.archive.org/web/20030223172938/www.mydd.com/archives/000319.html.

[5] For a recent study on the changes in people's face-to-face interactions brought about by new technology, see Aric Sigman, *Well Connected? The Biological Implications of "Social Networking"*, 56 BIOLOGIST 14 (2009), *available at* http://www.iob.org/userfiles/Sigman_press.pdf.

[6] Mike Musgrove, *Challenging Assumptions about Online Predators*, WASH. POST, Jan. 25, 2009, at F1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2009/01/24/AR2009012400182.html

tend to receive excessive attention, with the reliance on an "availability heuristic"[7] distorting our perception of emerging technology and sometimes leading to bad public policy.

Kahan then moved onto the more theoretical reasons why he is more optimistic than Gastil as to the transformative potential of social networking and online collaboration. He suggested that the lessons of network theory and emergent systems generally provide a basis for believing that order can indeed emerge from chaos. He explained that rules governing spontaneous self-ordering are manifested in systems as diverse as cellular biology, ecosystems, and macroeconomic behavior. Although individual actors in some systems do not attempt to order themselves in a way that serves a greater good, higher-level order can nevertheless emerge from their actions. Other examples of how high-level, emergent order can evolve from simple interactions could include the flocking or schooling behavior of birds and fish,[8] or the complex patterns that emerge from systems of cellular automata governed by only a few simple rules.[9] Kahan thus posited that, if we view social networks and other communities as instances of systems governed by known principles of network theory, we can make some predictions, including that traditional and formalistic versions ordered deliberation will become obsolete. Along those lines, Kahan suggested that social networks might be to traditional democracy what blogging and the Internet generally have been to publishing: low-cost, disruptive technologies that call into question the viability of the models they replace.

In sum, Kahan is more optimistic than Gastil because he feels that networks tend to develop rules and patterns out of undirected individual actions that serve the needs of the system as a whole. By contrast, Gastil fears that online social networks may never develop the positive features of the traditional social networks they displace.

Clarifying "Privacy"

Professor Weiser then opened up the roundtable to general discussion. Though many topics were broached, many of the issues raised involved one key theme: the need, first noted by John Gastil, for a more nuanced and granular theory of information usage to replace the simplistic dichotomy between "public" and "private." Other topics discussed tied into this broader theme in some way. The way the discussion focused on this theme rather than the roadmap suggested by Professor Weiser could itself be viewed as an example of the ungovernable, yet self-ordering nature of social interactions stressed by Dan Kahan.

Niel Robertson of Instinct Ventures stated the fundamental issue very clearly: uses of information that might be appropriate in one context, or by one person or organization, might not

---

[7] *See generally* Amos Tversky & Daniel Kahneman, *Availability: A Heuristic for Judging Frequency and Probability*, 5 COGNITIVE PSYCHOLOGY 207 (1973), *abridgment available at* http://psych.colorado.edu/~vanboven/teaching/p7536_heurbias/p7536_readings/tversky_kahn_1973.pdf.

[8] For an entertaining look at some of these phenomena, see Steven Strogatz, TED Talk: How Things in Nature Tend to Sync Up, http://www.ted.com/index.php/talks/steven_strogatz_on_sync.html (video presenting ideas from his book SYNC: THE EMERGING SCIENCE OF SPONTANEOUS ORDER (2003)).

[9] *See* STEPHAN WOLFRAM, A NEW KIND OF SCIENCE 2 (2002) ("despite the simplicity of their rules, the behavior of [cellular automata is] often far from simple . . . some of the simplest programs that I looked at had behavior as complex as anything I had ever seen.").

be appropriate in another context or by someone else.[10] James Clark of Room 214 articulated this same point slightly differently, suggesting that the important issue is what is done with data, by whom, and for what purpose, and not whether data should be pigeonholed as "public" or "private." This is not merely a suggestion that we move past an either/or public/private distinction on information to a spectrum from public to private. Rather, a more multidimensional understanding is needed. For instance, there may be "private" information you would share with your accountant, but not with your closest of friends. You may be willing to discuss politics with one group of acquaintances, but not with another. In fact, as Professor James Grimmelmann has written, many privacy concerns are in fact peer-produced.[11] Users are concerned, not only with what platform owners such as Facebook will do with their information, but also with what their friends will do with it. Sometimes users are comfortable with some kinds of information being "public," as long as it is not too readily available. This common-sense understanding of the complex nature of human relationships is too often lacking in discussions of information use policies, which, it was generally agreed by the discussants, have suffered from overly simplistic concepts. As will be discussed below, Phil Gordon suggested that what may be necessary is a set of flexible *information practices*.

Privacy Expectations

Dan Kahan raised several relevant points with regard to the debate over privacy. First, he noted that, in the context of data mining, much information is made "public" that people have never consciously elected to make public. For instance, Google tracks the searches its users make in order that it may target ads and sell marketing data to advertisers more effectively. Whether users view these uses of information as appropriate will depend on how thoroughly they understand what data are being collected, by whom, and for what purpose. Some users still do not understand the extent to which data about them are collected online. In the aggregate, this inadvertently revealed information can reveal much about particular users, or about demographic groups. Significantly, Twitter, a company that has been criticized for not having a revenue model,[12] has recently announced its intention to sell "analytics," or information about its users concerns and interests.[13] This shows that data mining has become a business plan. Neither is it limited to the business sector—the federal government increasingly relies this technique.[14] Indeed, many of those—including Kahan—who expressed comfort with Google and other Internet companies' use of monitoring user behavior reacted quite differently when asked, by Professor Paul Ohm, whether they felt differently when the government was the entity collecting the data.

---

[10] For an analysis of the complexities of drawing the boundaries between public and private, see danah boyd, *Social Network Sites: Public, Private, or What?*, KNOWLEDGE TREE, Issue 13, 2007, http://kt.flexiblelearning.net.au/tkt2007/edition-13/social-network-sites-public-private-or-what/

[11] James Grimmelmann, *Facebook and the Social Dynamics of Privacy*, 94 IOWA L. REV. (forthcoming 2009), *draft available at* http://james.grimmelmann.net/publications.

[12] *E.g.*, Sam Gustin, *Twitter's Business Model? Well, Ummmm...*, WIRED, Aug. 4, 2008, http://www.wired.com/techbiz/people/news/2008/08/portfolio_0804.

[13] Taylor Buley, *Twitter's Analytical Business Plan*, FORBES, Feb. 15, 2009, http://www.forbes.com/2009/02/14/Twitter-analytics-business-technology-ebiz_0215_Twitter.html

[14] Arshad Mohammed & Sara Kehaulani Goo, *Government Increasingly Turning to Data Mining*, WASH. POST, June 15, 2006, at D3.

Kahan had noted that people feel that their "privacy" is violated when information they had made public is used in ways they did not anticipate, such as for commercial purposes. This feeling, however, is not limited to unanticipated commercial use. Here, the example of Facebook's News Feed is instructive. This feature allows each Facebook user to see, among other things, all the changes her friends have recently made to their profiles in one simple, combined view. For example, if someone changed his relationship status from "single" to "engaged"—or from "in a relationship" to "single"—many of his Facebook friends, who might not otherwise know of the change, would be made aware of it on account of this feature. When Facebook introduced the news feed, there was widespread criticism that Facebook had disregarded its users' privacy.[15] Of course, users had already made the information "public"; a user's friends could already view his profile and see what relationship status was indicated. Users who object to making this kind of information public can always leave it blank. Furthermore, the information, as well as a user's profile, is only available to people the user has actively chosen to be "friends" with. Here, the objection was not so much that Facebook made information "public" that otherwise was not already available, but that it provided a tool that made it much easier for Facebook friends to keep tabs on each other. Over time, as people became accustomed to the feature, most users appear to have concluded that its benefits outweighed its costs, and it is now Facebook's most popular feature. The example of the Facebook News Feed points to two important considerations that must be a part of a more nuanced theory of information usage: (1) that people are concerned with how accessible even "public" data are, and are sometimes comfortable with having information available to those interested enough to seek it out, but not necessarily with having it broadcast, and (2) that people's expectations affect what uses they see as appropriate, and what level of availability they are comfortable with.

The idea that people's expectations affect how they view what uses are appropriate was emphasized by Phil Weiser, who pointed out that, despite their apparent technological similarities, he has a friend who hates blogs but enjoys Facebook. JB Holston, CEO and President of NewsGator, replied that this demonstrates how the analogies people form to help them situate new technologies can affect how they perceive them. Blogging is viewed as a platform for publishing, while Twitter and Facebook are more conversational. Different people might be averse to one platform and not the other based on what they perceive it as similar to—and, in turn, platforms can affect the way they are perceived by the affordances they provide.[16]

---

[15] For an overview of the Facebook News Feed controversy, including its later popularity, see Ellen McGirt, *Facebook's Mark Zuckerberg: Hacker. Dropout. CEO.*, FAST COMPANY, Dec. 19, 2007, http://www.fastcompany.com/magazine/115/open_features-hacker-dropout-ceo.html. Facebook has created other controversies relating to privacy and the control of users' data. *See, e.g.*, Eric Eldon, *Facebook Reverts to Old Terms of Service, Working on New Version That "Everybody Can Understand"*, VENTUREBEAT, Feb. 17, 2009, http://venturebeat.com/2009/02/17/facebook-reverts-to-old-terms-of-service-working-on-a-better-new-version/ (describing how Facebook instituted, and then withdrew terms of service that appeared to grant it intellectual property rights over user's data); Ellen Nakashima, *Feeling Betrayed, Facebook Users Force Site to Honor Their Privacy*, WASH. POST, Nov. 30, 2007, at A1 (describing the furor over Facebook's "beacon" program, which posted to Facebook details of transactions Facebook users conducted at other sites).

[16] *See* DONALD A. NORMAN, THE DESIGN OF EVERYDAY THINGS 9 (first paperback ed. 2002) ("the term *affordance* refers to the perceived and actual properties of the thing, primarily those fundamental

How different people's expectations can affect what uses of information they see as public, and which as private, was emphasized by the revelation that Micah Baldwin was posting his thoughts on the ongoing discussion to Twitter as the roundtable progressed. Discussants familiar with Twitter seemed to have no objection to this (and some were following his comments on Twitter in real time); others, however, noting that the roundtable was labeled a "private" event, hinted that such behavior might be inappropriate. In any event, it was generally agreed that the incident demonstrated some of the ambiguity surrounding different people's understanding of which uses of information are appropriate, and which are not.

Is Privacy Dead?

Baldwin suggested that we simply move on from privacy concerns. Paraphrasing Scott McNealy, he stated that "Privacy is dead, deal with it."[17] Moreover, he suggested that privacy considerations, if taken too seriously, could cripple the Internet, whose purpose is to enable communication and not protect people's outdated sensibilities. As an example, he offered his own life, where he shares many personal details about himself online. There was agreement from some of the discussants who suggested that if there is information a person would not be comfortable sharing with anyone—a romantic partner, a loan officer, or a potential employer—then that person should not make that information available online, anywhere. To expect that information could be contained once put online, these discussants argued, was unrealistic. Additionally, as Robert Reich observed, traditional methods of protecting information (intellectual property laws, licensing agreements and other forms of contracting) are premised on a world where the sharing of data is hard. By contrast, today, sharing is easy. Traditional means of enforcement, such as bringing private lawsuits, are available only to well-heeled parties. Even if an individual consumer had a valid cause of action,[18] the high cost of enforcing small stakes effectively stacks the deck against the little guy. Where the existing regime is premised on a concentrated interest able to police the marketplace itself, the problem today is that of a highly diffuse interest.

Another dynamic discussed at the roundtable is the extent to which people are starting to realize that once information is available online, any privacy protection is surrendered and to conform their behavior accordingly. JB Holston related that, afraid of having pictures of them drinking showing up on social networking sites and getting them in trouble, some young people at parties have darkened "shot rooms" where alcohol can be consumed without fear that photographic evidence will show up online. He wonders if this demonstrates that people are

---

properties that determine just how the thing could possibly be used"); Derek Wenmoth, Digital Lemmings, Derek's Blog, Oct. 15, 2008, http://blog.core-ed.net/derek/2008/10/digital-lemmings.html (how Twitter's affordances lend it to being used as a "back-chat" tool during conferences).

[17] In early 1999, McNealy, in response to a question about whether Sun had built privacy safeguards into some of its new technologies, responded that privacy issues were a "red herring" and that "[y]ou have zero privacy anyway. Get over it." Toby Lester, *The Reinvention of Privacy*, THE ATLANTIC, Mar. 2001, at 27-39, *available at* http://www.theatlantic.com/doc/200103/lester.

[18] Of course, the legal theory that a person would try to rely on to claim ownership of personal information such as a purchasing history or Internet click stream is not at all clear. Copyright, for instance, does not protect factual information, only creative expression. *See, e.g.*, Feist Publ'ns v. Rural Tel. Serv., 499 U.S. 340 (1991).

becoming afraid of the consequences of the widespread dissemination of personal information that social networks enable. Dan Kahan suggested that issues of fear are likely to be limited to transitional generations just becoming familiar with new technologies, but Phil Weiser observed that fear can be a good thing if what you are doing is, in fact, dangerous.

Matt Galligan, founder of Social Thing, observed that technology has simply removed the concept of privacy through obscurity. Any information that is made public, he argued, is available to anyone who looks for it quite easily. He argues that the example of the "Star Wars kid"[19] shows that this is not necessarily a good thing. This goofy video, which in the past may have subjected its creator to some teasing at his school, became a worldwide phenomenon, and one that the Star Wars kid has had trouble living down. Galligan suggests that, while privacy through obscurity is dead, its passing is to be mourned. Today, something is only as private as those you communicate it to choose to keep it, since there are no barriers to the widespread dissemination of information. Kahan countered, however, that examples like the Star Wars kid are rare and extreme, suggesting that we should look to the costs and benefits of new communications methods as a whole and not base our opinions on a few outlying cases.

Phil Weiser pointed out that if everything is public, the ability to have "intimate" information which is only shared with certain people is lost. Jud Valeski countered that social networks have given rise to a kind of "ambient intimacy"[20] whereby it is easy to keep track of the comings and goings of dozens of different people. In this sense, following people on Twitter is like having them as your roommate.

Professor Paul Ohm stated that the example of the Star Wars kid frightened him, because he sees himself in the Star Wars kid. Who among us, he suggests, has not done embarrassing things best forgotten? He raised a number of points relevant to the discussion of the need for a more sophisticated understanding of "privacy." He observed, for example, that the issue of privacy tends to bring out the paternalist in people who can otherwise be thought of as civil libertarians. Many of the people who call most loudly for restrictive regulations regarding what can be done with personal information tend to otherwise be very laissez-faire when it comes to, e.g., matters of free speech.

Related to Ohm's point about government use of data and to the concept that information that is meant to be private should simply be kept private, Robert Reich noted that the military is quite good at keeping some kinds of data confidential. It does this by keeping private data private: behind lock and key and not exposed to public networks. He also suggested that too much of the discussion of privacy, and the use of personal information more generally, is tied to the specific architectures of existing technologies and not to the underlying issues.

---

[19] *See* Vanessa Hua, *Spread of Jokes on the Internet About Real People Raises Privacy, Legal Issues*, S.F. CHRON., Sep. 8, 2003, at E1.

[20] *See* Clive Thompson, *I'm So Totally, Digitally Close to You*, N.Y. TIMES, Sep. 5, 2008, (Magazine), at MM42, *available at* http://www.nytimes.com/2008/09/07/magazine/07awareness-t.html.

Coping with "Threats"

Uses of personal information obtained through social networking sites that could be characterized, from the user's perspective, as threatening, weighed heavily on the minds of many discussants. Many instances of online harassment were discussed. In addition to the example of the Star Wars kid, Phil Weiser mentioned Autoadmit, an anonymous message board for law students that at times infamously devolved into attacks on other student's personalities and appearances, and which spawned several lawsuits.[21] The fact that social networking sites can work to turbo-charge gossip and rumor was cited by several discussants. Recently, the micro- and photo-blogging platform Tumblr caused controversy when it issued, and then quickly retracted, a policy banning accounts that were solely designed to criticize other users.[22]

Despite their relative rarity[23] (a point emphasized by Kahan), online threats to children remained an area of concern to many discussants. The age of a user is likely one of the factors that should play into a comprehensive data use theory. In the meantime, social networking sites continue to take actions designed to eliminate potential threats,[24] however unlikely those threats might be. Bullying behavior, which was briefly discussed,[25] is, of course, nothing new. Nevertheless, there may be some ways for social networking platform owners to make architectural decisions that make bullying more difficult and thus can protect users without compromising the nature of the experience.[26]

Phil Gordon, an attorney whose practice touches on the use of personal information by businesses, brought pragmatic insights to the discussion informed by his experience. He noted that the widespread availability personal information on the Internet can seriously harm people's career prospects. He pointed out that approximately 25% of employers and human resource departments now make use of information about potential employees gathered from social networking sites and the Internet at large. This number, he notes, will likely reach 100% as employers come to rely on the kinds of personal information that can be gathered so quickly and at little cost, and which often reveals much more about a job applicant than a résumé and an

---

[21] *See* Anna Badkhen, *Web Can Ruin Reputation with the Stroke of a Key*, S.F. CHRON., May 6, 2007, at A1.

[22] Eric Krangel, *Tumblr Ditches Anonyblogger Ban Amidst User Revolt*, BUSINESS INSIDER, Feb. 18, 2009, http://www.businessinsider.com/tumblr-ditches-anonyblogger-ban-amidst-user-revolt-2009-2.

[23] For a comprehensive evaluation of the risks children face online, see INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY & ONLINE TECHNOLOGIES 4 (2008), http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/ISTTF_Final_Report-Executive_Summary.pdf ("The Literature Review shows that the risks minors face online are complex and multifaceted and are in most cases not significantly different than those they face offline, and that as they get older, minors themselves contribute to some of the problems.")

[24] Jenna Wortham, *MySpace Turns Over 90,000 Names of Registered Sex Offenders*, N.Y. TIMES, Feb. 4, 2009, at B4.

[25] *See* Deborah Gage, *Web 2.0 Defamation Lawsuits Multiply*, S.F. CHRON., Feb. 9, 2009, at A1; Dan Slater, Student Cyberbullying & the Law: Part III, WSJ Law Blog, Feb. 9, 2009, http://blogs.wsj.com/law/2009/02/09/student-cyberbullying-the-law-part-iii.

[26] For example, the proposals outlined in a recent European Union pact signed onto by major social networking sites. *See* Constant Brand, *Social Networks Join Pact Against Cyberbullying*, MSNBC, Feb. 10, 2009, http://www.msnbc.msn.com/id/29120870.

interview. (This flow of information is a two-way street, however—some employers are finding out that their internal personnel decisions can become public quickly as laid-off employees with nothing to lose discuss their situations on social networking sites.[27]) He explained further that no laws currently concern what uses employers can make of information they gather about their potential and current employees.

In terms of how to approach privacy, Gordon suggested that what is needed is not an absolutist conception of privacy in the Brandeisian sense of "the right to be let alone,"[28] but a set of "information practices." As an example, he suggested that private companies should be required to disclose precisely what uses they intend to make of people's personal information and then be held to those disclosures.[29] This suggests that the current regime of voluntary "privacy policies," often couched in very general terms, is not sufficient. Employers should not be forbidden from accessing publicly available information about current and potential employees, but they could be required to disclose what kinds of information they intend to gather, and to what use it will be put. Widespread disclosure of the various uses to which personal information is put could affect how people use social networking sites. Similarly, sophisticated employers may come to realize that how a person behaves in his personal life may not necessarily reflect on his performance as an employee. He observed that people have a right to a private life, and their behavior in their personal life, as incompletely revealed on social networking sites, should not be used against them in unfair ways. Rob Johnson shared this concern, pointing out that context is important and that people should not rush to judge others based on the small pieces of their lives that may be found online. The Star Wars kid, for example, had a past and has a future, and shouldn't forever have to be judged based on one moment of his life.

Architectural Responses

It was noted that the foundational architectural choices made by the developers of social software can influence how those systems are used. In his book CODE (AND OTHER LAWS OF CYBERSPACE), Lawrence Lessig made famous the proposition that "code is law" (i.e., software engineering choices can have consequences at least as profound as any legal regime). In CODE, Lessig related the poisoning effect anonymity had on a discussion board used in conjunction with a class he was teaching—indeed, he lamented that the unease generated by some anonymous attacks spilled over to the regular sessions of his classes.[30] Todd Vernon, CEO of Lijit, agreed with this concern, stating that in his view anonymity encourages abusive behavior. Nonetheless, it remains an open question whether norms concerning basic architectural choices, such as whether to allow anonymity, can emerge spontaneously from social networks (as Dan Kahan

---

[27] *See* Corporate Executive Board, 2009 Recession Briefing, http://now.eloqua.com/e/es.aspx?s=693&e=255401263fe54b94aa609c0c0f70e962.

[28] Samuel Warren & Lois D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("the right to life has come to mean the right to enjoy life—the right to be let alone").

[29] BUSINESS FORUM FOR CONSUMER PRIVACY, A NEW APPROACH TO PROTECT PRIVACY IN THE EVOLVING DIGITAL ECONOMY: A CONCEPT FOR DISCISSION (2009), https://www.privacyassociation.org/images/stories/pdfs/a%20new%20approach%20to%20protecting%20privacy%20-%20final.pdf.

[30] LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 78-82 (1999).

might suggest), or whether those basic choices must be imposed from outside the network.[31] Indeed, it was suggested that anonymity could undermine the potential of trust networks, discussed below, to provide a solution to issues relating to online behavior and information use. By contrast, John Gastil stated that nominal group technique[32] teaches us that anonymity and accountability can not only coexist, but flourish together.

In reflecting on the key challenges of protecting privacy in the Internet environment, John Bennett discussed how transitive trust networks could work to solve many of the issues people have with the proper scope of information usage. Trust, he argued, is a moderator of privacy. Some people and organizations have earned and deserve our trust, while others have not. It is thus reasonable, he explained, to hold different people to different standards of personal data use based on our level of trust in them. In the world of computer science, a transitive trust network is one where, if Party A trusts Party B, and Party B trusts Party C, it is inferred that Party A trusts Party C to some degree. (Distrust, similarly, would be transitive.) A properly functioning trust network would allow users to set degrees of information access, and perhaps rules for information use, for individuals and organizations based on the level of trust the user bestows on him. The transitive nature of the network frees the user from having to set trust levels for each other user and allows strangers to be given a default level of trust based on the extent that people he trusts trust that stranger. A transitive trust network could thus be an architectural solution to the problem of how to determine what kinds of information use you allow different people and classes of people on social networks.

Michele Jackson, Chair of CU-Boulder's Department of Communications, similarly brought up an architectural point, reminding us of the virtues of *forgetting*. Traditionally, people could move on from events as they receded into the past and were superseded by more recent events, or were gradually forgotten. If worst came to worst, people could move to a new community and start afresh. The Internet works against this dynamic: it is a global community that people may find it impossible to escape, and it tends to record all events, even minor embarrassing ones, for posterity. She suggested that Internet data be given a half life, so that events from peoples' pasts do not continue to follow them for the rest of their lives.

Discussants then focused on the implementation problems behind some of the architectural methods that were proposed. Clayton Lewis, of CU's Computer Science Department, for instance, described the difficulties in dealing with trust issues on a new roommate finder service. Matt Galligan observed that whether recent or old data are preferred depends on the context. For instance, older, authoritative information might be preferable to

---

[31] Among those calling for regulations to be imposed on Internet platform owners are Nancy Kim, a professor of law at California Western School of Law, who has argued that website operators should be liable in some cases for harassment that occurs on their sites, Nancy Kim, *Imposing Tort Liability on Websites for Cyber-Harassment*, 118 YALE L.J. POCKET PART 115 (2008), http://thepocketpart.org/2008/12/15/kim.html, and who has also called for software-based "architectural restraints" such as cooling-off periods before comments are posted to deal with problems of Internet harassment, Drake Bennett, *Time for a Muzzle*, BOSTON GLOBE, Feb. 15, 2009, at C1, *available at* http://www.boston.com/bostonglobe/ideas/articles/2009/02/15/time_for_a_muzzle.

[32] *See generally* André L. Delbecq & Andrew H. Van de Ven, *A Group Process Model for Problem Identification and Program Planning*, 7 J. OF APPLIED BEHAVIOR SCIENCE 466 (1971).

someone researching the civil war, but more recent information might be preferable to someone tracking the career of a celebrity. How, then, can an automated system know which kind of information to "forget" or devalue? Robert Reich noted that automated systems can have a hard time keeping up with reality—citing the example of some searches for "Obama" coming up with results appropriate for "Bush." For any research task, there's a long tail of irrelevant data.

Jason Mendelson, Managing Director at the Foundry Group, observed that many corporations choose to work around trust issues by implementing internal social networking systems, in essence piggybacking on the existing trust system of the workplace. Todd Vernon, CEO of Lijit, noted that the architecture of commercial social networks works against their utility to users and doubted that commercially-oriented networks could be viable in the long term. Facebook, for instance, would prefer if you were "friends" with as many people as possible, and MySpace wants you to be "friends" with Pepsi. Jason Mendelson also noted that all automated reputation systems suffer from first mover problems. A responsible eBay seller, by sheer bad luck, might have a bad transaction and receive negative feedback on it. An established seller with a lot of good feedback would probably not be harmed by just one piece of negative feedback. But a new seller might not be able to bounce back from that first piece of bad feedback. Michele Jackson countered that this exact kind of scenario is the kind of situation that a half-life for data is intended to correct.

The unanswered question regarding the architectural features of social networking such as anonymity and trust systems is whether ideal architectures can spontaneously emerge from the undirected interactions of the users of networks themselves, or whether they must be imposed from the outside. While Niel Robertson argued that regulatory and architectural choices must precede self-organization and emergence, John Gastil countered that *all* features of networks can and should emerge from the unmanaged interactions of their participants. In either case, as Christine Bevc of CU's Natural Hazards Center pointed out, the opportunity to watch new communities being formed, and new social norms, rules, and laws emerge, is fascinating from a sociological point of view. At the same time, the knowledge that sociologists have gained from looking at other emerging communities and networks can deepen our understanding of the dynamics currently working in social networking sites.

Conclusion

Just as the "[m]odern privacy law arose, in part, out of a concern over an earlier transformative technology: the Kodak 'snap camera,'"[33] the rise of social networking software calls for, at least, a reanalysis of the fundamental concepts of "public" and "private." A more rigorous understanding of these concepts will allow the discussion over what kinds of uses of personal information are acceptable, and what are not, more closely track the complex views that users actually have on these subjects. The spirited discussion at the roundtable, however, suggests that a consensus on the future of privacy will not be easy to obtain.

[33] Bennett, supra note 31.

Appendix: Roundtable Attendees

Chris Achatz	*CU Law Student*
Meg Ambrose	*ATLAS Student*
Micah Baldwin	*Lijit*
John Bergmayer	*CU Law Student/Reporter*
Ashlie Beringer	*Gibson Dunn*
Brad Bernthal	*University of Colorado Law School*
John Bennett	*ATLAS*
Christine Bevc	*CU Natural Hazards Center*
James Clark	*Room 214*
David Cohen	*TechStars*
John Conley	*Governor's Office of Information Technology*
Kylie Crandal	*CU Law Student*
Matt Galligan	*Social Thing*
John Gastil	*University of Washington*
Phil Gordon	*Littler Mendelson*
Tracy Gray	*Hogan & Hartson*
Dirk Grunwald	*University of Colorado*
Gabe Hamilton	*StickyVote by InnoVoter, Inc*
Janet Eaton	*Harris Umbria*
J.B. Holston	*NewsGator*
Michele Jackson	*University of Colorado*
Rob Johnson	*EventVue*
Dan Kahan	*Yale University*
Nidhi Kakkar	*CU ITP Student*
Tom Keller	*Intense Debate*
Walter Knapp	*Lijit*
Clayton Lewis	*University of Colorado*
Mike Locatis	*Governor's Office of Information Technology*
Jason Mendelson	*Foundry*
Ben Oelsner	*Kendall Koenig & Oelsner*
Paul Ohm	*University of Colorado*
Julie Penner	*CU MBA/JD Student*
Lisa Reeves	*Vista*
Jill Rennert	*Silicon Flatirons*
Niel Robertson	*Instinct Ventures*
Brandon Sandberg	*CU Law Student*
Doug Sicker	*University of Colorado*
Jud Valeski	*Gnip*
Jill Van Matre	*ATLAS*
Todd Vernon	*Lijit*
Phil Weiser	*University of Colorado Law School*
Michael Zeisser	*Liberty Media*
Robert Reich	*One Riot*