BRIDGING THE GAP BETWEEN PRIVACY AND DESIGN[†]

Deirdre K. Mulligan[*]
Jennifer King[**]

ABSTRACT

This article explores the gap between privacy and design in the context of "lateral privacy"—privacy issues arising among users of a service rather than from the service provider—on social networking sites (SNSs) and other platforms by analyzing the privacy concerns lodged against the introduction of Facebook's News Feed in 2006. Our analysis reveals that the dominant theory of privacy put forth by regulators, privacy as individual control, offers little insight into the experiences of privacy violation claimed by users. More importantly, we show that this theory is ill-equipped to guide the design of SNSs and platforms to avoid similar harms in the future. A rising tide of privacy blunders on social networking sites and platforms drives the search for new regulatory approaches, and privacy regulators across the globe are increasingly demanding that the Fair Information Practice Principles, the embodiment of privacy as individual control, inform the design of technical systems through Privacy By Design. The call for Privacy By Design—the practice of embedding privacy protections into products and services at the design phase, rather than after the fact—connects to growing policymaker recognition of the power of technology to not only implement, but also to settle policy through architecture, configuration, interfaces, and default settings. We argue that regulators would do well to ensure that the concept of privacy they direct companies to embed affords the desirable forms of protection for privacy.

Ideally, there would be a widely used set of methods and tools to aid in translating privacy into design. Today, neither is true. We identify three gaps in the "informational self-determination" approach that limit its responsiveness to lateral privacy design decisions in SNSs and platforms and then explore three alternative theories of privacy that provide compelling explanations of the privacy harms exemplified in platform environments. Based on this descriptive utility, we argue that these theories provide more robust grounding for efforts by SNSs and platform developers to address lateral privacy concerns in the design of technical artifacts. Unlike FIPPs, which can be applied across contexts, these theories require privacy to be discovered, not just implemented. To bridge this discovery gap, we turn to the field of Human Computer Interaction ("HCI") and dip into the related field of Value Sensitive Design ("VSD") to identify tools and methodologies that would aid designers in discovering and ultimately embedding these contextual, socially- oriented

† This project is supported by the TRUST Center (The Team for Research in Ubiquitous Secure Technology), which receives support from the National Science Foundation (NSF award number CCF-0424422), and by the Nokia Corporation.

This material is based upon work supported by the U.S. Department of Homeland Security, under grant award #2006-CS-001-000001, and the National Institute of Standards and Technology, under grant award #60NANB1D0127, under the auspices of the Institute for Information Infrastructure Protection (I3P) research program. The I3P is managed by Dartmouth College. The views and conclusions contained in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the U.S. Department of Homeland Security, the I3P, or Dartmouth College.

* Assistant Professor, University of California, Berkeley, School of Information.

** Doctoral Candidate, University of California, Berkeley, School of Information.

understandings of privacy in technical artifacts. Finally, we provide some tentative thoughts on the form and substance of regulations that would prompt corporations to invest in these HCI approaches to privacy.

INTRODUCTION

For over thirty years the public and private sectors have been directed to protect privacy through adherence to Fair Information Practice Principles ("FIPPs"). Regional directives,[1] international instruments,[2] omnibus[3] and sectoral laws,[4] and guidance documents[5]

1 *See, e.g.*, Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31, 33 (EC); ASIA-PACIFIC ECON. COOPERATION, APEC PRIVACY FRAMEWORK (2005), *available at* http://publications.apec.org/publication-detail.php?pub_id=390.

2 *See* Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe, Jan. 28, 1981, E.T.S. 108, *available at* http://conventions.coe.int/Treaty/EN/Treaties/HTML/108.htm; *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* ORG. FOR ECON. COOPERATION & DEV. (Sept. 23, 1980), http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

3 *See* Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5 (Can.); Loi 1978-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée [Law 1978-17 of January 6, 1978 on Information Technology, Data Files and Civil Liberties], JOURNAL OFFICIEL DE LA REPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], 1978; Legge 31 dicembre 1996, n.675 (It.), *available at* http://www.garanteprivacy.it/garante/doc.jsp?ID=28335; Decreto Legislativo 30 June 2003, n.196 (It.), *available at* http://www.garanteprivacy.it/garante/docu-ment?ID=1219452 (implementing Directive 95/46/EC and the Data Protection Code).

4 While the U.S. has continued to take a largely sectoral approach to privacy, it has enacted statutes to advance FIPPs. *See, e.g.*, Right to Financial Privacy Act ("RFPA"), 12 U.S.C. §§ 3401–22 (2006) (protecting the confidentiality of personal financial records by creating a statutory Fourth Amendment protection for bank records); Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. §§ 6801, 6827 (2006) (empowering various agencies to promulgate data security regulations for financial institutions); Electronic Communications Privacy Act of 1986 ("ECPA"), 18 U.S.C. §§ 2510, 2511 (2006) (extending restrictions against wiretaps to include transmissions of electronic data by computer); Video Privacy Protection Act of 1988 ("VPPA"), 18 U.S.C. § 2710 (2006) (preventing disclosure of personally identifiable rental records of "prerecorded video cassette tapes or similar audio visual material"); Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. No. 104–91, 110 Stat. 1936 (1996) (codified as amended in scattered sections of 42 U.S.C.) (regulating the use and disclosure of "Protected Health Information" in the section 1173 under "Security Standards for Health Information" Section 2).

5 *See, e.g.*, FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 36–37 (2000) (suggesting that all consumer-oriented, personal websites that collect personal information must comply with the four widely-accepted fair information principles), *available at* http://www.ftc.gov/reports/privacy2000/privacy2000.pdf; Memorandum from Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Sec., on The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security 1 (Dec. 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf ("This

across the globe are fashioned on these principles. Until recently, adherence to FIPPs-based policies through incorporation into institutional policies and processes was viewed as largely sufficient to address privacy concerns arising from private sector data collection.

While the FIPPs model of privacy protection, and the theory of "informational self-determination"[6] on which it rests, continues to resonate with the privacy challenges in many sectors of the economy, regulators across the globe have begun to demand more of corporations, particularly corporations in the information and communication technology sectors.

The increasing importance of social networking sites ("SNSs") and platforms for a wide range of social interaction, such as communication and interaction between individuals and groups, is challenging this model of privacy protection. A rising tide of privacy blunders on social networking sites and platforms drives the search for new regulatory approaches. Many of these privacy gaffes center on the interactions between users. Frequently it is the information flows enabled by the novel technical designs of SNSs—the technical affordances or withholdings—that draw the strongest privacy objections, not the direct use of personal information by the firm itself.

These plastic, sui generis, built environments give the companies that design them a privileged role in society. As architects of the "playing fields"[7] upon which individuals, and increasingly governments and private sector entities, engage, they can erect, alter, and obliterate structural barriers[8] that afford or erode privacy through transaction costs. They can introduce novel information flows. They can enforce contractual terms with such global impact that they dwarf

---

Memorandum memorializes the Fair Information Practice Principals ("FIPPs") as the foundational principles for privacy policy and implementation at the Department of Homeland Security.").

6 The term "information self-determination" was set forth in a German court decision limiting the intrusiveness of the German Census Act of 1983. *See* Bundesverfassungsgericht [BVerfGE][Federal Constitutional Court] Dec. 15, 1983, 1 BvR 209/83 (Ger.), *translated in* 5 HUM. RTS. L.J. 94, 97 (1984).

7 David Clark et al., *Tussle in Cyberspace: Defining Tomorrow's Internet*, 13 IEEE/ACM TRANSACTIONS ON NETWORKING 462, 464 (2005) ("[T]echnologists are, in fact, creating playing fields for the tussles of society to play out in.").

8 *See* Harry Surden, *Structural Rights in Privacy,* 60 SMU L. REV. 1605, 1607 (2007) ("Structural constraints are regulators of behavior that prevent conduct through technological or physical barriers in the world. These barriers make certain conduct costly.").

national policy preferences.[9] Simply put, they have an unprecedented ability to reshape privacy norms on a global scale.

With so much at stake, regulators are reluctant to permit companies to exercise unfettered discretion over the construction of these new playing fields. Growing recognition that companies hold great sway over the related values of privacy, publicity, and identity is matched by increased desire to influence firms' architectural and policy choices. If "[t]echnology is society made durable,"[10] then society has a stake in the information flows[11] that technical designs both privilege and prevent. Regulatory focus is slowly shifting toward the design of the systems, not just the policies that govern them.

Privacy regulators across the globe are increasingly demanding that FIPPs inform the design of technical systems. In the past, FIPPs have largely been discharged through the adoption of policies and processes within the firm: privacy has been the bailiwick of lawyers. Now, under the rubric of "privacy by design," policymakers are calling on the private sector to use the distinct attributes of code to harden privacy's protection.[12] The call for privacy by design—the practice of embedding privacy protections into products and services at the design phase, rather than after the fact—connects to growing policymaker recognition of the power of technology to not only implement, but also to settle policy through architecture, configuration, interfaces, and default settings.

Exhorting companies to embed privacy into the design of their SNSs and platforms is all well and good, but before doing so regulators would do well to ensure that the concept of privacy they direct companies to embed will afford the desirable forms of protection for privacy. Ideally, there would be a widely used set of methods and tools to aid in translating privacy into design. Today, we argue, neither is true.

---

9 For example, while national policies range with respect to the desirable level of connection between online activities and identity, Facebook's real name policy may reduce the practical salience of these national policies.

10 Bruno Latour, *Technology Is Society Made Durable*, *in* A SOCIOLOGY OF MONSTERS: ESSAYS ON POWER, TECHNOLOGY AND DOMINATION 103 (John Law ed., 1991).

11 *See* Helen Nissenbaum, *Privacy As Contextual Integrity*, 79 WASH. L. REV. 119, 138–39, 155 (2004) (stating that "information appropriateness and distribution" norms derived from history, culture, law, and practice define privacy in specific social contexts and "govern key aspects such as roles, expectations, behaviors, and limits . . . .").

12 Ira S. Rubenstein, *Regulating Privacy by Design*, BERKELEY TECH. L. J. (forthcoming) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1837862.

This article explores the gap between privacy and design in the context of "lateral privacy"[13] issues on SNSs and other platforms. Our analysis reveals that the dominant theory of privacy put forth by regulators—privacy as individual control—offers little insight into the experiences of privacy violation claimed by Facebook users. More importantly, we show that this theory is ill-equipped to guide the design of SNSs and platforms to avoid similar harms in the future. While FIPPs remains quite powerful and relevant to the privacy issues arising between users and Facebook—what we will refer to as the vertical relationship—they prove less helpful in considering the decisions Facebook makes that influence data flows among Facebook users—hat we call lateral privacy issues.[14]

We begin with a description and analysis of privacy concerns lodged against Facebook's News Feed. In order to identify salient privacy issues raised by the News Feed, we explore the limits of policies and tools that foster user control over the use and disclosure of their personal information ("informational self-determination"). We identify three gaps in the "informational self-determination" approach that limit its responsiveness to lateral privacy design decisions in SNSs and platforms: inattention to technology as a regulator; exclusive focus on individuals as data subjects; and related focus on the protection of the acontextual individual as the justification for privacy. We then explore three alternative theories of privacy that provide compelling explanations of the harms flowing from the introduction of News Feeds. Based on this descriptive utility, we argue that these theories provide more robust grounding for efforts by SNSs and platform developers to address lateral privacy concerns in the design of technical artifacts. However, unlike FIPPs, which has been applied across contexts, these theories require privacy to be discovered in specific contexts prior to its implementation. To bridge this discovery gap, we turn to the field of Human Computer Interaction ("HCI") and dip into the related field of Value Sensitive Design ("VSD") to identify tools and methodologies that would aid designers in discovering and ultimately embedding these contextual, socially-oriented understandings of privacy in technical artifacts. Finally, we

---

13 In this paper, lateral privacy is defined as privacy issues arising among other users of a service, rather than from the service provider. This term was chosen to parallel the concept of coveillance or lateral surveillance. *See, e.g.*, Mark Andrejevic, *The Work of Watching One Another: Lateral Surveillance, Risk, and Governance*, 2 SURVEILLANCE & SOC'Y 479 (2005), *available at* http://www.surveillance-and-society.org/articles2(4)/lateral.pdf.

14 James Grimmelmann refers to these as "peer-produced" privacy problems. *See* James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1188 (2009).

provide some tentative thoughts on the form and substance of regulations that would prompt corporations to invest in these HCI approaches to privacy.

I. PRIVACY VIOLATIONS IN SOCIAL NETWORK SITES AND PLATFORMS

SNSs such as Facebook and MySpace support information sharing between and among their individual users. Unlike previous communication platforms, SNSs intentionally expose vast amounts of data about their users and their users' interactions and transactions. The exposure of such data is their defining feature. As boyd and Ellison state, social networks are "web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system."[15] SNSs are used not just to communicate, but to construct, explicate, and perform identity through the articulation of connections, thoughts, and acts.

These SNSs and platforms support an incredible variety of social interactions: collaborative games; membership-based groups of every kind (from alumni groups to celebrity fans); political organizing, and information seeking and sharing, to name only a few.[16] Some of these interactions are directly facilitated by the SNSs or platforms, while others are supported by platform-specific third party software. Third party applications expand the functionality of SNSs and platforms, but they also allow developers and businesses to access a vast amount of user data. Through a varied mix of technical design, policy setting, application vetting, and policing, these SNSs and platform operators attempt to control how personal information flows within, into, and out of their platforms.[17]

---

15 danah m. boyd & Nicole B. Ellison, *Social Network Sites: Definition, History, and Scholarship*, 13 J. COMPUTER-MEDIATED COMM. 1 (2007), http://jcmc.indiana.edu/vol13/issue1/boyd.ellison.html.

16 However, survey findings from the Pew Research Center note that the primary reasons people use social media are to stay in touch with family members and existing friends. *See* Aaron Smith, *Why Americans Use Social Media*, PEW RESEARCH CTR. (Nov. 14, 2011), http://pewinternet.org/Reports/2011/Why-Americans-Use-Social-Media.aspx (reporting on the results of a survey finding that adult users of social network sites "say that connections with family members and friends . . . are a primary consideration in their adoption of social media tools . . . .").

17 Various companies allow third party developers to access their platforms. *See The Developer's Guide*, ANDROID, http://developer.android.com/guide/index.html (last visited Feb. 2, 2012); *Facebook Developers*, FACEBOOK, http://developers.facebook.com/ (last visited Feb. 2, 2012); *iOS Dev Center*, APPLE, http://developer.apple.com/devcenter/ios/index.action

Increasingly, these companies are called to task for the privacy outcomes among participants enabled by their architectural and policy choices. While not unprecedented,[18] this environment presents a complex set of shifting challenges for companies, users, and policymakers concerned with privacy. For while companies are clearly responsible for ensuring their own practices for handling personal information adhere to Fair Information Practice principles reflected in data protection and privacy laws, it is less clear what those principles have to say about the information flows they architect among their users.

1. The Facebook News Feed

As of 2011, Facebook is the world's largest online social network,[19] with over 800 million users.[20] A core feature of the site is the user's ability to update a "status:" a short blurb about the user's thoughts or actions. Prior to 2006, these updates appeared only on members' profile pages and in an aggregated format called the "Mini Feed."[21] Status updates were available on a user's profile page to individuals on their friends list and in the user's networks. To view them, a friend of the user had to actively search out the user's profile page.

In 2006, Facebook introduced the News Feed.[22] News Feed transmitted status updates directly to the profile pages of the user's friends

---

(last visited Feb. 2, 2012); *MySpace Developer Center*, MYSPACE, http://developer.myspace.com/ (last visited Feb. 2, 2012); *Windows Mobile Developer Center*, MICROSOFT, http://msdn.microsoft.com/en-us/windowsmobile/bb264318 (last visited Feb. 1, 2012); and *Yahoo! Developer Network*, YAHOO!, http://developer.yahoo.com/everything.html (last visited Feb. 1, 2012).

18 Mobile platforms and SNSs are not the first to face concerns about the way their technical design choices and default settings impact user privacy, although the vast and constantly changing range of data and interactions they facilitate heighten these problems for SNSs. *See* Nissenbaum, *supra* note 11, at 121 (discussing the introduction of Radio Frequency Identification Tags); Marc Rotenberg, *Communications Privacy: Implications for Network Design*, 36 COMM. ACM 61, 63 (1993) (discussing the introduction of Caller ID).

19 Following boyd and Ellison, "We define social network sites as web-based services that allow individuals to (1) construct a public or semi-public profile within a bounded system, (2) articulate a list of other users with whom they share a connection, and (3) view and traverse their list of connections and those made by others within the system. The nature and nomenclature of these connections may vary from site to site." boyd & Ellison, *supra* note 15, at 2.

20 *Statistics*, FACEBOOK, http://www.facebook.com/press/info.php?statistics (last visited Jan. 23, 2012).

21 Ruchi Sanghvi, *Facebook Gets a Facelift*, THE FACEBOOK BLOG (Sept. 5, 2006, 4:03 AM), https://blog.facebook.com/blog.php?post=2207967130&fb_comment_id= (discussing the introduction of News Feed and Mini-Feed).

22 *Id.*

for display. The feature could not be turned off, and publication was non-selective: any "friend" on a user's friends list received the status updates. The status updates were pushed out, rather than sought out.[23]

This shift altered the access paradigm in two significant ways. First, it removed the ability of the recipient to moderate the terms of sharing. Instead of an all-you-can-eat-on-demand smorgasbord, friends found themselves at the receiving end of an always-on fire hose of status updates. Second, News Feed removed the transaction costs associated with a friend actually accessing a status update that was available as a policy matter. This merged the theoretical and actual audience for any given status update. The introduction of News Feed left Facebook users rather paradoxically feeling stalked and spammed by their so-called friends. Facebook users were upset about the heightened visibility of their actions and the sometimes-formidable demand on their attention.[24]

a. Facebook's Defense

Facebook responded to users' privacy complaints by improving the controls that allowed users to manage some of the types of information posted to the Feed.[25] However, in the mind of Facebook founder Mark Zuckerberg, the introduction of News Feed did nothing to disrupt users' privacy;[26] it maintained the status quo. The information that users chose to share with specific groups of people—friends and networks—remained available to only those groups. Fa-

23 Andrés Sanchez, *Facebook Feeding Frenzy: Resistance-through-Distance and Resistance-through-Persistence in the Societied Network*, 6 SURVEILLANCE & SOC'Y 275 (2009), *available at* http://www.surveillance-andsociety.org/ojs/index.php/journal/article/viewFile/frenzy/frenzy; Todd Simmons, The Ethics of Privacy on Facebook (Apr. 4, 2011) (unpublished MBA paper, St. Edward's University), http://todd-simmons.com/docs/MBA10_GlobalDigital_PrivacyEthics.pdf.

24 The initial shock at the change prompted a negative response from Facebook's users, with one anti-News Feed group gaining 10,000 followers in the first day of News Feed's release. Users were unhappy with the widespread distribution of activity that was previously hidden in practical obscurity, despite the fact that the information itself had not changed.

25 *See* Press Release, Facebook, Facebook Launches Additional Privacy Controls for News Feed and Mini-Feed (Sept. 8, 2006), http://www.facebook.com/press/releases.php?p=643 (describing the new privacy controls implemented in response to user feedback about the News Feed and Mini-Feed).

26 Mark Zuckerberg, *An Open Letter from Mark Zuckerberg*, THE FACEBOOK BLOG (Sept. 8, 2006, 5:48 AM), https://blog.facebook.com/blog.php?post=2208562130.

cebook had not altered[27] its users' decisions about who should have access to their personal information. Ruchi Sanghvi, the product manager for News Feed, stressed this point during News Feed's release, stating, "News Feed and Mini-Feed are a different way of looking at the news about your friends, but they do not give out any information that wasn't already visible. Your privacy settings remain the same—the people who couldn't see your info before still can't see it now."[28]

b. Users' Perspectives

Facebook users had a different perspective. For them the *mechanism* of sharing mattered. While information was still withheld or shared based on their preferences, the dynamics of sharing in the pre-News Feed environment had apparently informed users' decisions about whether to share in the first place. The transaction costs afforded by the pull environment, which required a Facebook user's friends to visit the user's page in order to view status updates, embedded an additional layer of practical privacy protection in the pre-News Feed environment.

Reducing the time and effort required to view status updates triggered two separate privacy concerns. First, the recipients of News Feed complained of being "spammed" by their friends. As summed up by one user:

> Personally, I don't have a problem with the information being there. I just have a problem with that HUGE amount of information in my face all the time. I don't care who added a new book to their favorites; if I wanted to know someone's favorite books, I read through their profile.[29]

Prior to News Feed's introduction, users with permission to view status updates maintained enormous discretion as to when and if they did so.[30] The move to a push model of distribution placed greater demands on their time and attention.

Second, the increased exposure created by the shift from a billboard to a broadcast made the experience substantively different for

---

27 Sanghvi, *supra* note 21; Mark Zuckerberg, *Calm Down. Breathe. We Hear You.*, THE FACEBOOK BLOG (Sept. 5, 2006, 10:45 PM), https://blog.facebook.com/blog.php?post=2208197130.

28 Sanghvi, *supra* note 21. We should note that the fine-grained privacy controls that now exist for News Feed posts were not available when the feature launched.

29 Enoxice, *Information Overload*, Comment to *Facebook Changes Provoke Uproar Among Users*, SLASHDOT (Sept. 5, 2006, 9:47 PM), http://slashdot.org/story/06/09/06/0112231/facebook-changes-provoke-uproar-among-users.

30 *See* Stephanie Buck, *The Evolution of Facebook Profile [PICS]*, MASHABLE (Sept. 20, 2011), http://mashable.com/2011/09/22/facebook-profile-evolution.

users posting status updates. Previously, users enjoyed a level of "practical obscurity" even from those with whom they chose to share information. While users may have granted a large number of individuals' permission to view their status updates, they knew that the transaction costs of searching and viewing their page meant that only those truly motivated to do so would actually "follow" them. With the introduction of News Feed, Facebook users faced far greater actual exposure. The transaction costs created theoretical and actual audiences: News Feed fused them. Data that previously had to be actively sought was now as a matter of course aggressively and routinely publicized to friends. In the words of a Facebook user, "Stalking is supposed to be hard."[31] News Feed made it easy.

Many experienced the News Feed as a privacy violation despite its continued deference to individuals' decisions about whether and with whom to share status updates and the consistency of the data at issue. The reduction in transaction costs rather than a change in privacy settings—or the change in mechanism of distribution, not the formal rules governing distribution—is what triggered the privacy concern.

II. UNPACKING NEWS FEED

A. News Feed and Fair Information Practice Principles

As Zuckerberg and Sanghvi rightly argued, Facebook users had affirmatively indicated a desire to share information with the set of individuals who received status updates via the News Feed.[32] They claimed that the company's actions were completely consistent with respecting users' privacy.[33] Examining Facebook's actions through the lens of information privacy as "informational self-determination," the company's position is understandable, perhaps even defensible. However, rather than attending to user claims of privacy harms, this position merely defines privacy to place them out of scope. For users, claims were not about binary choices but about expectations grounded in both policy and structural constraints, and neither were user claims about informational self-determination. Rather, they were about the dynamics of revelation in a broad, undifferentiated network of connections.

---

31 *Angry Students Lash Out at Facebook.com Privacy Changes*, FOX NEWS (Sept. 8, 2006), http://www.foxnews.com/story/0,2933,212722,00.html.

32 Zuckerberg, *supra* note 26 (discussing what he thought users would want out of Facebook); *see also* Zuckerberg, *supra* note 27.

33 Zuckerberg, *supra* note 27.

1. FIPPs and Theories of "Informational Self-Determination"

The Fair Information Practice Principles ("FIPPs") embody a rights-based framework of "informational self-determination."[34] They reflect a liberal construction of privacy that seeks to support "the claim[s] of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others,"[35] through the imposition of processes that support the individual's agency over the flow of personal information. In practice, FIPPs drive the adoption of policies and mechanisms through which "individuals can assert their own privacy interests and claims if they so wish," allowing them to define "the content of privacy rights and interests."[36] Privacy is afforded through processes that are fair and provide individuals with the capacity to make fully informed decisions about their personal information.

The Organisation for Economic Cooperation and Development ("OECD")'s *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* provide an influential statement of FIPPs.[37] The Guidelines set out eight principles that affirm the individual's right to self-determination.[38] These principles place obligations on entities

---

34 Bundesverfassungsgericht, *supra* note 6 (setting forth the term "information self-determination" in a German court decision limiting the intrusiveness of the German Census Act of 1983).

35 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

36 COLIN J. BENNETT & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 9 (2006).

37 *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, *supra* note 2.

38 The Organisation for Economic Cooperation and Development Guidelines, the most widely cited statement of FIPPs, adopted the following eight principles in 1980:

> 1. Collection Limitation Principle
> There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
> 2. Data Quality Principle
> Personal data should be relevant to the purposes for which they are to be used and, to the extent necessary for those purposes, should be accurate, complete, and kept up-to-date.
> 3. Purpose Specification Principle
> The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
> 4. Use Limitation Principle
> Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.
> 5. Security Safeguards Principle

that collect and process data, requiring: transparency about the types of information collected and the way the information will be used; limits on data collection—namely that "data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject"; provision of data subject rights to access and accuracy; and protection for collected data against breach and corruption.[39]

The FIPPs were designed for an era where big government or large corporations collected information about individuals.[40] The information might be sold or shared but was generally intended for consumption by the company or organization that collected it. The FIPPs did not anticipate a world where companies would design platforms through which individuals would share information with other individuals or with the broad public (and by default, with the platform owner). Unsurprisingly, given this history, FIPPs provides incomplete guidance to platform companies with respect to the lateral privacy issues that arise among their users.

> Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
>
> 6. Openness Principle
>
> There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
>
> 7. Individual Participation Principle
>
> An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.
>
> 8. Accountability Principle
>
> A data controller should be accountable for complying with measures, which give effect to the principles stated above.

Id.; *see also* COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 101–11 (1992) (describing the OECD principles).

39 *Id.* at 106 (quoting OECD, *supra* note 2).

40 A U.S. government advisory committee originally proposed the FIPPs in 1973 "in response to [the] growing use of automated data systems containing information about individuals." Robert Gellman, *Fair Information Practice: A Basic History, Version 1.86*, at 1 (2011), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

2. "Informational Self-determination" and News Feed

Assuming that Facebook desired to meet their users' privacy needs, the News Feed incident suggests that grounding efforts to do so in a conception of privacy as individual self-determination would have been insufficient. As noted above, Facebook defended its actions by indirect reference to the concept of "informational self-determination."[41] Facebook claimed that its practice of affording individuals an opportunity to control access to their profiles fully discharged its privacy obligations with respect to this aspect of News Feed. User complaints suggest otherwise.

The primary purpose and the use limitation principles of FIPPs are the core instantiations of the commitment to individual control. Examining News Feed under either principle would not raise an immediate flag for a lawyer or technologist. The "Purpose Specification Principle" requires corporations to specify the personal data collected and to limit its use to the fulfillment of the purposes for which the user provides it. The purpose is assessed from the perspective of the user, not the company. In the context of News Feed, users were not only informed and familiar with the information being collected, but in fact were solely responsible for its creation and contribution. Users determined the contents of status updates. Users created them for the explicit purpose of sharing with their friends (and potentially others). Users directly controlled the audience to whom they were accessible. While Facebook may be using status updates for other purposes, at least with respect to disclosures to friends and networks, Facebook was clear about the purpose and afforded users control. The "Use Limitation Principle," which generally prohibits the disclosure or use of personal information for purposes other than those initially proposed and understood by the user absent consent,[42] was clearly not implicated by News Feed either. Facebook users had determined who was authorized to access their profiles, and thus their status updates. The shift to News Feed did not disrupt their choices. If anything, it furthered their aims.

Examining Facebook's policy in isolation provides little warning about the privacy reaction News Feed would receive, precisely because the policy itself was not at issue, as it had not changed. Put another way, only a consideration that took the technical affordances as a form of regulation on par with that of policy would draw Face-

41 Zuckerberg, *supra* note 27.

42 Use for an additional purpose may lawfully occur where authorized by law.

book's attention to the additional layer of de facto privacy protection[43] offered by its earlier architecture. This sort of holistic analysis is necessary to understand the significant role that technical regulation played in users' policy choices.

Unfortunately, FIPPs do not naturally direct institutional focus toward mechanisms that implicitly or explicitly regulate information flows. While Privacy Impact Assessments ("PIA") were introduced to address the potentially disruptive effect of technology changes on privacy expectations,[44] they are generally deferential toward compliance with a stated policy. If a policy states that personal information is to be available to a given audience, a PIA will not invite an interrogation of the degree of openness. Where a tolerated privacy intrusion is magnified by a change in technology, the output of a PIA may suggest mitigations. However, where a change in technology advances a policy objective aligned with privacy—such as availability of status updates by those users who had indicated should receive them—a PIA would be unlikely to identify the change as one to be mitigated. Given that the permission structure of the shared data (status updates) remained unchanged,[45] and that, at least from the point of view of Facebook management, the intent had not shifted,[46] it is highly unlikely that PIAs or similar FIPPs-based tools would have alerted Facebook to the privacy fallout of this change.

Microsoft's "Privacy Guidelines for Developing Software Products and Services," a document "based on the core concepts" of the FIPPs,[47] reflects this focus on privacy as effectuating policy choices. It provides "guidance for creating notice and consent experiences, providing sufficient data security, maintaining data integrity, offering customer access, and supplying controls when developing software products and Web sites."[48] While these foci are all important aspects of managing the use of personal information by the corporation, they are largely irrelevant to the user complaints sparked by News Feed. Although the introduction of PIAs surely gives FIPPs more meaning

43 *See* Surden, *supra* note 8, at 1607 (explaining "latent structural constraints").

44 U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENTS: THE PRIVACY OFFICE OFFICIAL GUIDANCE (2010), *available at* http://www.dhs.gov/files/publications/gc_1209396374339.shtm#2.

45 Posts were still limited to friends and network members.

46 This is information users wanted to share; otherwise they would not have posted it.

47 *Privacy Guidelines for Developing Software Products and Services Version 3.1*, MICROSOFT CORP. 5 (Sept. 2008), http://www.microsoft.com/download/en/details.aspx?displaylang=en&*id*=16048.

48 *Id.*

in firm activities, it does not reorient the privacy analysis to any great extent.

Second, the privacy claims of recipients of status updates cannot be framed as an issue of loss of control over personal information. The recipient's information was not at issue. Thus, FIPPs frameworks' exclusive focus on informational self-determination significantly undermines their utility. Recipients' complaints were about the increased level of time and attention their Facebook friends demanded via the News Feed feature. In the role of recipients, users experienced News Feed as an intrusion on their time and attention—not a threat to their personal information. The intrusion-related privacy claims of Facebook users resonate with statutory frameworks addressing unsolicited commercial communications.[49] They protect the right to be let alone, or, at least, the right to exert some control over the level of, or conditions of, accessibility to others' communications. FIPPs focus on protecting the individual as a data subject is completely unhelpful in either explaining or addressing this privacy concern.

Finally, and perhaps most importantly, the privacy claims made by Facebook users in both roles—status updaters and recipients—suggest that users perceived the introduction of News Feed to put their relationship with others at risk. Users reacted to being "spammed" and "stalked" by their Facebook friends. Clearly, either activity puts the friend relationship at risk. Surely a friend who stalks or spams risks hasty relegation to a less favorable status.

The transaction costs that mediated sharing pre-News Feed were essential to the protection of "friend"-ship as understood on the Facebook platform. In contrast, FIPPs and other data protection models center the individual—his freedom, autonomy, and dignity—as the object of protection. From users' complaints, the object at risk appears to be, at least in part, the viability of Facebook friendships. While FIPPs based mechanisms that facilitate individual control over the sharing of information may be useful to the maintenance of friendship, protecting such relationships is neither their goal nor their justification. It is an incidental output of a model centered on the atomistic individual protecting her own interests.

Attention to FIPPs during the design process would have been of little assistance in either identifying or avoiding the privacy violations

---

49 Do-Not-Call Implementation Act of 2003, 15 U.S.C. § 6101 (2006); CAN-SPAM Act of 2003, 15 U.S.C. § 7701 (2006); Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (2006).

Facebook users claimed.[50] FIPPs focuses the privacy analysis on actors and the policies that bind them. In doing so, it diverts attention from the importance of the mechanisms through which policy choices manifest and the background against which such choices are framed. FIPPs appear ill-suited to identify or address privacy issues that arise due to gradations in accessibility caused by shifts in technology. Equally importantly, FIPPs are concerned solely with individuals as data subjects, while the complex social interaction represented by News Feed presented privacy claims for users positioned as data subjects and as recipients of communications. The orientation of FIPPs is not helpful in identifying or addressing this second set of privacy claims. Finally, FIPPs justify privacy based on the individual's autonomy, freedom, and dignity. Facebook users' privacy claims centered on the room they created for relationships among individuals. While they did not offer friendship as a justification for preferring the pre-News Feed information flows, they were concerned with the impact of the change on the category of Facebook friends as constructed under the initial rules.

B. Alternative Explanations of News Feed's Privacy Failings

If we suspend disbelief and assume that Facebook desired to meet their users' privacy requirements, our examination of News Feed complaints suggests that efforts grounded exclusively in a conception of privacy as individual self-determination are insufficient to identify the privacy issues for three inter-related reasons: they focus primarily on the role of policy in determining privacy outcomes, thereby eclipsing the role that technical artifacts play in protecting and eroding privacy; they foreclose inquiries into privacy issues unrelated to the protection of personal information, such as the right to be let alone or control access to the self; and, they center the protection of the

50 The Article 29 Working Party, established by Article 29 of Directive 95/46/EC, is comprised of the heads of EU member states' data protection authorities and is the independent EU Advisory Body on Data Protection and Privacy. In its "Opinion on Online Social Networking" it provides little concrete direction on lateral privacy issues stating, "SNS should offer privacy-friendly default settings which allow users to freely and specifically consent to access to their profile's content that is beyond their self-selected contacts in order to reduce the risk of unlawful processing by third parties." Article 29 Working Party May 2009 Opinion on Online Social Networking, at 7. In a letter to Facebook, the Working Party provided some explanation of what settings are not "privacy-friendly" writing, "Pursuant to the Data Protection Directive, the default privacy settings offered by SNS should not allow access beyond self-selected contacts and any further access should be an explicit choice by the user." Article 29 Working Party May 12, 2010 Letter to Facebook.

individual as the singular goal of privacy protection. These gaps limit FIPPs' ability to identify and solve lateral privacy issues that suffuse SNSs and platforms generally. We also believe these gaps commend other theories for our consideration.

The first limitation revealed by our analysis of News Feed directs our attention to theories that attend to the varied mechanisms of privacy protection—be it physical or code-based, social norms, or market powers. It suggests theories that focus on socio-technical systems or, at the very least, take the affordances and limitations technical artifacts provide seriously. Second, it suggests privacy theories that we will describe as capacious in that they offer more inclusive, fluid, or at least not rigidly pre-determined definitions of privacy. Privacy is implicated by many acts, not just the wresting or denial of control over personal information. Our analysis of News Feed illustrates that multiple definitions of privacy are in play in peer-to-peer interactions on SNSs, and that multiple activities can be viewed as diminishing privacy. Finally, users lamented the impact of the loss of privacy on the category of Facebook friends—including actual friends and others with whom they wish to maintain social ties, as tenuous as they may be. Theories that conceive of privacy as protecting relationships and society and not, or at least not exclusively, the individual help explain such claims. Such theories position privacy as necessary for various forms of social organization, rather than to the individual in some abstract and atomistic sense. There are several theories of privacy that exhibit these traits. Below we unpack the News Feed case to see whether the theories are as helpful in understanding privacy as our conceptual mapping suggests.

1. Alternative Theories of Privacy

We find the work of three theorists responsive to the facets of the News Feed privacy issues that are missed by a FIPPs-based approach. These theories position various contextually situated and desirable forms of social organization and activity to be the justification of privacy, thus driving consideration of the needs of multiple actors rather than only those of the data subject, and taking stock of the contributions of non-legal regulators to privacy's protection. Psychologist Irwin Altman views privacy as "an *interpersonal boundary process* by which a person or group regulates interactions with others."[51] Legal theorist

51 IRWIN ALTMAN, THE ENVIRONMENT AND SOCIAL BEHAVIOR: PRIVACY, PERSONAL SPACE, TERRITORY AND CROWDING 6 (1975).

Robert Post claims privacy tort law is best understood as socially valued protection of core individual rights that do "not simply uphold the interests of individuals against the demands of community, but instead safeguards rules of civility that in some significant measure constitute both individuals and community."[52] Philosopher Helen Nissenbaum claims privacy is achieved through adherence to contextually appropriate norms of information flow—"contextual integrity"—that support socially valued interactions within specific spheres of social life.[53] These theorists vest privacy's justification in the protection of connection and community, rather than the individual. Their work acknowledges the importance of non-legal regulators. Because their work considers privacy in the context of community, it takes a more capacious and inclusive stance on privacy's objectives and form.

a. Social Justifications for Affording Privacy

Unlike data protection and FIPPs that justify privacy in terms of its instrumental or intrinsic value for the individual, Altman, Nissenbaum, and Post justify privacy in terms of its support for interpersonal and group connection, community, the constructed and relational self, social utility, and communal solidarity. This perspective proves helpful in analyzing the News Feed case. It accounts for users as actors within a community—in Facebook's case, a socio-technical system—not merely as data subjects.

Altman provides the fullest exploration of privacy's essential role in social relationships.[54] He posits that "the concept of privacy is central to understanding environment and behavior relationships"[55] and that privacy rightly construed is "an *interpersonal boundary process* by which a person or group regulates interaction with others."[56] Focusing on the process aspect of privacy, Altman emphasizes privacy's

52 Robert Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 CALIF. L. REV. 957, 959 (1989).

53 Nissenbaum, *supra* note 11, at 138–39, 155.

54 ALTMAN, *supra* note 51, at vii ("General textbooks on environment and behavior are beginning to appear, but many cut an extremely wide swath, often treating some topics in only a superficial fashion. I have brought together research on four central issues in as comprehensive and as detailed a fashion as possible in order to provide needed conceptual handles and lend some coherence to at least part of the environment and behavior field."); *see also* Helen Nissenbaum, *Protecting Privacy in an Information Age: The Problem of Privacy in Public*, 17 LAW & PHIL. 559, 581–82 (1998), *available at* http://www.springerlink.com/content/k625w27565861919/fulltext.pdf.

55 ALTMAN, *supra* note 51, at 6.

56 *Id.*

constant redefinition across relationships, time, and sentiment, and physical and psychological terrain. Privacy is imminently fungible and a dialectic by nature that involves "a balancing of opposing forces—to be open and accessible to others and to be shut off or closed to others."[57] The dynamic and dialectic aspects of privacy defy reduction to a fixed set of protections or affordances defining a private state. Instead, it is a "process of optimization."[58] Post, too, argues that privacy is better understood as justified by the needs of community. He states that "the tort [of privacy] . . . safeguards rules of civility that in some significant measure constitute both individuals and community."[59] Post's work positions privacy tort law as a flexible mechanism that regulates boundaries between the self, groups, and others, and, in doing so, plays a key role in iteratively defining, structuring, and affirming the self and communities.

Examining the complaints of Facebook users one is struck by their concern for relationships. While Facebook users objected to being stalked and spammed, they expressed concern about the effects of inadvertent stalking and spamming on their relationships. They could position themselves on both ends of the News Feed pipe and were concerned not only about themselves but also about its potential impact on their friendships. From their perspective these new conditions put the willingness to connect at risk.

Users feared that the change in distributional norms would affect social relations. As discussed below, the distributional norm protected two privacy interests that were perceived as central to the Facebook friend relationship. The pull norm facilitated rampant sharing and rather promiscuous "friend-ing," based upon an expectation of limited actual revelation of information. While updates were available to a relatively broad audience, they remained practically obscure. The tacit understanding, expressed in user comments, was that only a limited group of their Facebook friends—their "true friends," their "close friends," or their "family"—would exert the effort necessary to scrutinize their activities and musings. This practice provided users the freedom to post relatively indiscriminately, because their friends retained ultimate control over the receipt of posts, freeing the poster from the fear of being perceived as a nuisance or an intrusion. On the recipient end, users were happy to be friend-ed because prior to the introduction of News Feed they maintained con-

57 *Id.* at 23.

58 *Id.* at 11, 25–27 (illustrating the variables involved in trying to reach an optimal level of privacy in social interactions).

59 Post, *supra* note 52, at 959.

trol over the timing and quantity of status updates they ultimately received.

As Facebook users well know, "Facebook friends," are often not *friends* in the traditional sense. As danah boyd explains, "[t]he term 'friend' in the context of social network sites is not the same as in everyday vernacular. And people know this. . . . 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."[60] A tongue-in-cheek illustration of this point is offered by the "Whopper Sacrifice" campaign that Burger King ran as a Facebook Platform application.[61] The campaign offered Facebook users who purged ten Facebook friends deemed unworthy of their weight in beef a coupon for a free Whopper.[62] Burger King dispersed many coupons.[63]

Acknowledging and setting aside objections to Facebook's appropriation of the term "friend," the introduction of News Feed put the relationship of "friend" as defined by Facebook at risk. While it is relatively easy to mock the term friend as used on Facebook, the relationship has meaning and value for members despite its variance from the common understanding of the term. News Feed removed the transaction costs that aided social sorting—an individual's friends in the vernacular sense were more likely to be consistently motivated enough to overcome the transaction costs of the pre-News Feed arrangement, while an individual's Facebook Friends were not. The pull environment thus acted as a filter, sorting friends from Facebook Friends. This was particularly important because the sharing policy lacked any sort of fine grained functionality that would allow you to selectively push out status updates depending upon their content, or to select a limited group of friends with whom to share a specific update. While it was coarse, the pull mechanism acted as a rough filter. One could go so far as to argue that the transaction cost associated with the pre-News Feed environment was constitutive of the category Facebook Friend. It likely contributed to the willingness of users to maintain a vast array of weak ties—acquaintances or other loose con-

60 danah boyd, *Facebook's "Privacy Trainwreck": Exposure, Invasion, and Drama*, APOPHENIA BLOG (Sept. 8, 2006), http://www.danah.org/papers/FacebookAndPrivacy.html.

61 *See* Jenna Wortham, *The Value of a Facebook Friend? About 37 Cents*, N.Y.TIMES BITS (Jan. 9, 2009), http://bits.blogs.nytimes.com/2009/01/09/are-facebook-friends-worth-their-weight-in-beef/ (discussing the purpose and motivation behind Burger King's "Whopper Sacrifice" campaign).

62 *Id.*

63 *Id.*

nections between individuals[64]—which research has shown are advantageous for employment opportunities and gaining "diverse perspectives and new information."[65] Prior to News Feed, one's weak ties were shielded from the minutiae of one's updates unless motivated to seek them out. The introduction of News Feed inundated users with too much information in both a quantitative and qualitative sense.

Post's conception of privacy as "rest[ing] not upon a perceived opposition between persons and social life, but rather upon their interdependence"[66] provides additional texture to this story. The privacy norms helped individuals in their role as generators and users of updates within this arguably misnamed "friend" relationship. As Ellison notes, "Before social network sites were popular, people used communication strategies like gossip and the holiday newsletter to maintain awareness of distant friends, old coworkers, and far-flung relatives. Through status updates and feeds, SNSs enable individuals to broadcast both major life changes and ephemeral activities to their broad network, allowing others to engage in lightweight social surveillance."[67] Like privacy tort law, the mechanism of information distribution and acquisition helped maintain civility. As the likelihood that one's "weak ties" would receive and view status updates increased, the actual audience extended beyond the intended audience.[68] This expansion in actual audience was experienced as a violation of norms of sharing by both parties. In response, users devised coping mechanisms, such as altering the substance of their updates or narrowing their circle of Facebook friends.[69]

---

64 Mark Granovetter, *The Strength of Weak Ties: A Network Theory Revisited*, *in* SOCIAL STRUCTURE AND NETWORK ANALYSIS 105, 105–07 (Peter V. Marsden & Nan Lin eds., 1982) (discussing the function, benefits and drawbacks of "weak ties" to the individual and the social structure generally).

65 Nicole B. Ellison et al., *Social Network Sites and Society: Current Trends and Future Possibilities*, INTERACTIONS, Jan. 2009, at 6, 7, *available at* https://www.msu.edu/~steinfie/EllisonLampeSteinfield2009.pdf.

66 Post, *supra* note 52, at 959 (offering a normative account of privacy that does not focus just on the protection of individuals, but also on protection of the community, and finding that privacy torts in the common law uphold social norms, which in turn contribute to both community and individual identity).

67 Ellison et al., *supra* note 65, at 7.

68 Researchers have found that expectancy violations by weak ties—defined as an undesired social group viewing a Facebook profile—was a predictor of user decisions to make a profile friends-only. Fred Stutzman & Jacob Kramer-Duffield, *Friends Only: Examining a Privacy-Enhancing Behavior in Facebook*, *in* CHI 2010: ACM CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (2010), *available at* http://dl.acm.org/citation.cfm?*id*=1753559.

69 *Id.*

b. Taking Technical Artifacts Seriously

Altman and Nissenbaum explicitly focus on the broad range of mechanisms that afford and define privacy in a given context: facilitating boundary regulation or constituting the contextually appropriate norms of information flow, respectively. Their theories attune privacy analysis to protections found in norms, structures and markets as well as law and policy. They draw attention to non-human actors who structure and order interactions—structuring privacy by design. While Post's focus is on law, he draws on the work of Erving Goffman whose account of the socially structured articulation of the self as a presentation before others documents the multitude of ways norms of behavior provide privacy.[70] Implicitly, Post, too, views law as only one regulating force. Collectively, these theorists draw attention to the full range of mechanisms that individuals rely upon in daily life to afford varying forms of privacy.[71]

This attention to structural privacy protections is key to understanding the reaction of Facebook users to News Feed. In Nissenbaum's theory of contextual integrity, "norms of appropriateness dictate what information about persons is appropriate, or fitting, to reveal in a particular context. Generally, these norms circumscribe the type or nature of information about various individuals that, within a given context, is allowable, expected, or even demanded to be revealed."[72] Norms of distribution, by extension, examine whether information's distribution, or flow, is consistent with context-specific norms ranging from expectations of confidentiality and discretion to entitlement and obligation to reuse or re-disseminate.[73] These shared norms—which can vary culturally, temporally, and along other dimensions—provide a set of background expectations that Nissenbaum claims define privacy in each context. When information flows are inconsistent with these norms, the resulting disruption of expectations is perceived as a privacy breach. Nissenbaum's central thesis is that there are no a priori, one-size-fits-all rules that protect privacy. Instead, she states "what bothers people, what we see as dangerous, threatening, disturbing, and annoying, what makes us indignant, resistant, unsettled, and outraged in our experience of contemporary systems and practices . . . is not that they diminish our control and

70 ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

71 Post, *supra* note 52, at 971–73 (1989).

72 Nissenbaum, *supra* note 11, at 138.

73 *Id.* at 140.

pierce our secrecy, but that they transgress context-relevant informational norms."[74]

The shift in a distributional norm—from pull to push—unsettled two expectations about how widely viewed Facebook status updates would be. The first expectation was based on a distributional norm informed not exclusively by the information's availability but rather by its availability plus the transaction costs of its discoverability. As noted above, the transaction costs associated with discovering data acted as a check on the actual audience for the average status update, effectively culling out Facebook friends. The second expectation that was violated was the relatively unobtrusive nature of one's status and other updates to one's friends—we hesitate to call them recipients because, while the information was available to them, whether they actually received it was under their control. Again, the expectation was informed by the mechanism of distribution—pull—not just permission to access the information. As noted above, the shift to News Feed literally force-fed individuals' Facebook friends a diet of daily minutiae: it was an informational assault on one's Facebook friends.

Altman's theory, which describes privacy as a "dialectic process" of boundary regulation, is perhaps the most useful in explaining the importance of qualitative shifts in accessibility brought about by technologies that reduce transaction costs.[75] In likening the process of privacy regulation to that of a cell membrane mediating the external and internal environment, Altman draws attention to the fluidity and dependency of the privacy states individuals desire and on the impact even subtle changes can have upon them. Altman posits privacy's purpose as interpersonal boundary regulation in the service of developing knowledge and defining the self, and assessing and managing the relationship between the self and others.[76]

In emphasizing the permeable membrane between the self and others, Altman's theory invites focus on the importance and breadth of *mechanisms* used to manage privacy—structures, policies, and norms. Altman, like Nissenbaum, opens our eyes to a broader interpersonal context in which individuals deploy this range of mechanisms to manage their connections to others in the complex social process that constructs privacy. From the "practical obscurity"[77] re-

74 HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 186 (2010).

75 ALTMAN, *supra* note 50, at 6.

76 *Id.*

77 U.S. Dept. of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989).

sulting from the cost associated with discovering accessible information, or deriving insights through data-mining techniques, to the norms that cause individuals to avert their gaze to things in plain sight and resist asking and responding to questions about others' private lives, Altman focuses attention on the non-legal methods that are consciously and unconsciously used to regulate access to the self.[78] In News Feed, the mechanism at issue influenced the degree of communication that regularly occurred between Facebook friends. The introduction of News Feed simultaneously increased feelings of surveillance and informational assault as the membrane separating Facebook friends became more porous and permeable.

The News Feed incident draws our attention to the dialogue between privacy and publicity, self-identity and community-identity, and connection and seclusion that permeate the process of privacy. It illustrates privacy as a fluid and intuitive practice, not the conscious, deliberative, and discrete process envisioned in theories that focus exclusively on individual control. Altman's rich description of privacy's significance in human relations and its constantly changing state root it in distinctly human processes of cyclical discovery, negotiation, and reification.

The information architecture, technical defaults, and terms of service agreements for platforms heavily inform the information sharing norms of a growing "networked public."[79] The information sharing norms of SNSs—increasingly referred to as "networked publics"—inform, challenge, and alter existing norms and create new membranes with new properties, at times inconsistent with the expectations individuals import based on past experience in non-technically-mediated environments. The interaction of the various players, the artifacts they produce, and the policies that govern them produce a "networked space"[80] just as urban planners, residents, and others

78 ALTMAN, *supra* note 51.

79 A networked public consists of "the spaces and audiences that are bound together through technological networks (i.e., the Internet, mobile networks, etc.)" and whose interactions the network mediates. danah boyd, *Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life*, *in* YOUTH, IDENTITY, AND DIGITAL MEDIA 119, 125 (David Buckingham ed., 2008) (distinguishing networked publics that provide "searchability" from other mediated publics that in turn differ from experiences of being in public in physical space because of the persistence of data, the replicability of data, and the invisibility of audience).

80 *See* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 213 (2007) ("The important question is not what kind of space cyberspace is, but what kind of space a world that includes cyberspace is and will become. Cyberspace is part of lived space, and it is through its connections to lived space that cyberspace must be comprehended and, as necessary, regulated. In particular, a theory of cyberspace and space must consider the

produce the varied range of public spaces in the physical world. While the interactions in these networked spaces may be simple extensions of familiar interactions—and therefore bring with them contextually relevant norms—in other instances they will be novel interactions with no offline parallel that require greater attention to users' understandings and constructions of context.[81]

The News Feed example confirms Altman's insight of the following:

> [D]esigners need to deal with the behaviors that users employ to achieve desired levels of interaction. . . . These questions are behavioral and focus on the user as an active, coping organism that interacts with and employs the physical environment and other behaviors in various combinations. Thus these design questions imply the theme of creating responsive environments that users can interact with and that become extensions of their behavioral repertoires.[82]

The Facebook engineers flipped a switch that greatly altered a mechanism that users intuitively relied upon to achieve a desired state of interaction. It did so without warning and initially failed to create tools for users to react, adjust, and fine tune. Rather than crafting a "responsive environment," Facebook crafted an environment and demanded users to conform.

c. Multiple Objects of Privacy Protection

The News Feed example reveals two separate perspectives on what privacy ought to protect. While not mutually exclusive, they are distinct. With respect to their status updates users expressed concern about the decrease in what is commonly known as practical obscurity. While users chose to provide their friends and networks access to their updates, they did so assuming that only a small set of those friends would exert effort to read them. Friends who received status updates raised a second variety of privacy concern. They felt bombarded and intruded upon, especially when considering the vague sense of "friend" many initially relied upon to forge these connections. Users found themselves suddenly aware of the actions of

---

rise of networked space, the emergent and contested relationship between networked space and embodied space, and the ways in which networked space alters, instantiates, and disrupts geographies of power.").

81 *See* Helen Nissenbaum, *A Contextual Approach to Privacy Online*, 140 DAEDALUS 32, 44 (2011) (discussing the challenges of "online cases without straightforward social precedents" and recommending a process that starts with an understanding of the "purposes and values" of the context, and what sort of norms will support the desired activities).

82 *See* ALTMAN, *supra* note 51, at 212 (emphasis omitted).

people with whom they had sometimes slight or even no real world personal connections.

The first privacy complaint can be framed as protesting a loss of control over personal information. However, such framing rings somewhat false given that the change in technology advanced the individual's decision to share personal information they already intended to share with others. To underscore this point, if Facebook had rolled out a new feature that made it harder for unauthorized individuals to access status updates it seems quite certain that the complaints would have been far fewer and less strident. It would be perceived as an improvement, an effort to further the user's intent not to allow access—clean and simple. Yet, here, where the technical improvement magnified the choice to share information, it was perceived as disruptive and problematic. This suggests that the relationship between the technical change and the user's policy choice—i.e., supportive or disruptive—is not itself dispositive, or predictive, of the user's perception of its impact on privacy. Or at least this seems to be the case where the change advances a choice to make information available or accessible.

While one could argue that the object that privacy is deployed to protect in this first set of complaints is "control over personal information," the terms of the objections "stalking," "watching," and "monitoring" speak more to concerns about the surveillance News Feed enabled than to concerns about access to the information itself. This complaint may be better understood as a desire to limit access to the self. While the self in this case is a digital representation, and one that is, in many instances, deliberately crafted to portray the specific self the individual desires to project into the world, it is nonetheless a manifestation of a real individual who has rights and interests concerning access to that self. In fact, one could argue that working with a concept of privacy focused on individual control over personal information is unhelpful in this instance, because the privacy analysis it triggers situates the actors and rules as the foremost objects of interrogation. This emphasis on actors shields the playing field from analysis. Yet, here the transaction costs implicit in the prior playing field—the platform without News Feed—were an essential material condition of the user's decision about whether to share or withhold status updates entirely.

This analysis aligns with other areas in which privacy protections are hotly contested. For example, the dispute at the heart of the United States v. Jones[83] case argued before the Supreme Court in 2011 is whether moving from an environment where, due to advances in technology, it is not only legal but also practically feasible for police to track the daily movements of every citizen, at ten second increments, in public places is different, as a matter of constitutional law, from an environment in which police possess the legal ability to do so but lack that technical wherewithal. In other words, does a shift in transaction cost matter in a Fourth Amendment privacy analysis? In the oral arguments, one can hear the discomfort of the Court with an outcome that fails to account for the feasibility of omnipresent police surveillance, yet the sense of some that the tool they have to work with—the Fourth Amendment—gives them no ability to account for technical change that reduces the transaction costs that independently checked the rise of widespread police surveillance irrespective of the presence or absence of Constitutional barriers to the practice. The pliability of the playing field allows those who design it to radically shift transaction costs related to the movement and processing of information.

Whether the entity shifting the field is Facebook, through disrupting mechanisms of distribution, or the police, through new methods of surveillance, the privacy responses suggest that the regulations imposed by the built environment are deeply significant for privacy. One metric against which we might consider the utility of a tool for privacy protection is how well it addresses these sorts of environmental changes. To address them well, it must not only provide a justification for penalizing certain shifts retroactively but also provide guidance to those attempting to respect privacy in their design decisions. As shown above, the formulation of privacy as individual control seems ill-suited to this task.

The second privacy claim raised by users in the role of recipients cannot be framed as a concern about loss of control. Recipients objected to new demands on their time and attention. The introduction of News Feed was an intrusion. In contrast, the theories of Altman, Nissenbaum, and Post take a capacious view on the objects protected by privacy and the mechanisms of protection. Protecting privacy in Altman's view demands that individuals and groups be able to effectively deploy a variety of mechanisms to mediate their interactions—exposure, seclusion, and connection—to others. The boun-

83 United States v. Jones, 131 S. Ct. 3064 (2011).

dary control mechanisms Altman identifies are of both input (demands for connection) and output (efforts at connection) varieties.[84] This formulation is quite helpful in considering the News Feed incident. It accounts for privacy across roles and in context. Similarly, Nissenbaum's theory of privacy as "contextual integrity"[85] finds privacy to require respect for norms of information flow—"appropriateness" and "distribution"—that facilitate socially valuable activities in various spheres of life. While affording individuals control over personal information is one means of controlling information flow, it is neither the only one nor the dominant one in many spheres. With respect to News Feed, contextual integrity requires both finer-grained individual control over actual audience as well as the ability to control the volume and frequency of intrusions on the individual's time and attention. The justification offered for both forms of control was not the protection of the individual—or their enhanced ability to enjoy freedoms or exercise rights—but the social value of the interactions that occur under those conditions.

2. New Theories to Guide Design

Individuals use Facebook and other social network sites and platforms to support and strengthen existing relationships, and to a lesser extent forge new ones, through interactions and information exchanges. Theories that emphasize privacy's role in building and sustaining relationships, delineating and defining the self in relation to others, and negotiating the interface between the self and others provide helpful explanations of the privacy fallout from News Feed. The theories above offer useful insights because they move away from the FIPPs model of users as the data subjects of corporate files. They view privacy as a product of many inputs: neither policy nor individual choice reigns supreme. For this reason, they provide a useful lens through which to examine privacy issues between users that are partially structured by the policy and technical constraints and affordances of the platforms. These theories ground privacy in a social context and conceive of privacy as a multi-dimensional, negotiated, process. They hold privacy to protect society as well as the individual—indeed, they ultimately reject constructs that pose them to be severable, at least for the purpose of considering privacy.

---

84 *See* ALTMAN, *supra* note 51, at 28 (identifying both input and output varieties of boundary control mechanisms).

85 Nissenbaum, *supra* note 11, at 138–39.

a. Re-Thinking Privacy by Design

Ideally, these theories would provide insight into design requirements that could assist platform developers in avoiding future privacy gaffes. Unfortunately, while the multi-dimensional, contextual, and fluid understandings of privacy they offer provide frameworks to understand the privacy problems facing users of social network sites and platforms, they do not provide straightforward answers as to which information flows, boundaries, or mechanisms are normatively desirable at the outset. Due to the contextually contingent understanding of privacy they propose, they cannot direct design without some additional work. For what privacy means must be derived from the context. Though we have identified useful theories, the gap between theory and design remains formidable.

For these theories to gain prescriptive power they must be coupled with design methods that elicit the contextually relevant needs and values. Figuring out what flows and boundaries should be privileged in a given context requires inquiry into the values of the context and needs of the individuals within it. If our assessment is correct and these theories of privacy should guide the design of social network sites and platforms, we must radically reconfigure the "privacy toolbox."[86]

3. Privacy as Human Process

These theories of privacy concern themselves with privacy as a *human-centered process*. As such, corporations seeking to attend to these conceptions of privacy must embrace design methods that are user-centered rather than law-centered. They must commit to processes of discovery rather than compliance. Rather than adopting legal mechanisms to distance themselves from the question of what privacy requires, platform companies must identify methods and tools that will help them unearth and understand the privacy they ought to afford. Certainly values can and should be derived from law and other positive statements of normative commitment. However, law is only one manifestation of what individuals value and require in a given context.

Unfortunately current privacy by design tools based in FIPPs manifest as a *legally-oriented process*. It is more aptly described as data protection by design, and takes privacy as commitment to a set of preor-

86 *See* BENNETT, *supra* note 38, at 153–92 (examining an array of personal data protection policy choices).

dained principles. As the European Commission states, it is a primarily a tool of compliance, "[t]he principle of 'Privacy by Design' means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal."[87] The bulk of privacy by design tools and methodologies are aimed at corporate executives and privacy officers—many of whom are lawyers, not system architects, designers, or coders.[88] They help translate legal and policy requirements for the process of system or process design. For example, requirements engineers seek to aid privacy compliance by developing frameworks and methodologies to extract privacy requirements from legal text. Such tools are explicitly aimed at compliance. They do not encourage conceptual or empirical inquiry into privacy needs, but rather seek to facilitate the process of compliance with a set of ex ante rules.

Understanding privacy as a human process requires companies to solicit and understand the context-dependent privacy expectations of affected individuals. This requires a conceptual and empirical inquiry into privacy's meaning. This form of privacy by design begins with value-centered and human-centered processes. It requires a new set of privacy experts.

Ensuring that a company accurately describes its privacy-related activities in its terms of service and provides appropriate mechanisms to capture consumer acceptance of them is a task for lawyers. Understanding the values at play and privacy requirements in a given context requires a separate set of skills. It requires research to understand and document what individuals bring to the table—their naïveté, their uninformed and ill-conceived notions of how technology works, their mental models based in prior brick and mortar interactions, and their cognitive biases, to name a few. It demands attentiveness to context and human experience, the very attributes that

---

87 *Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Approach on Personal Data Protection in the European Union*, at 12 n.30, COM (2010) 609 final (Apr. 11, 2010), *citing Communication from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions: A Comprehensive Strategy on Data Protection in the European Union*, COM (2007) 228.

88 *See* Seda Gürses, Carmela Troncoso & Claudia Diaz, Engineering Privacy by Design 2 (unpublished manuscript), *available at* http://www.cosic.esat.kuleuven.be/publications/article-1542.pdf ("However, little past experience exists in designing systems with privacy in mind, and even those are typically invisible or inaccessible to policy makers who discuss the principles of privacy by design.").

companies, through privacy notices, attempt to disavow and make irrelevant.

Although rarely included in the privacy by design discussion occurring at the regulatory level, the field of Human-Computer Interaction ("HCI") and the related and emerging field of Values Sensitive Design ("VSD") are rife with approaches for identifying human needs and values in technical systems. HCI researchers use a diverse set of methods to unearth users' privacy expectations and concerns. Based on such assessments researchers and designers select a theoretical framework to guide system design that aligns with a users' conceptions of privacy issues. Tellingly, one strand of HCI research examines privacy through the lens of "individual control"-based theories, while a second strand is motivated by Altman's theory of privacy as boundary regulation. VSD is a younger field, but shares some methodological approaches and more importantly an affinity for contextual inquiry to identify relevant values during design. We examine relevant HCI research, and highlight some VSD approaches, to illustrate the methods and tools available to assist the developers of platforms and social network sites in understanding and embedding sociality theories of privacy. Our goal is not to propose specific changes to News Feed or to social networking sites or platforms more broadly. Rather, our goal is to show the connection between the contextual understanding necessary for developers to address privacy issues and the methods and approaches of HCI and VSD.

4. Value Sensitive Design, Human-Computer Interaction, and Privacy By Design

Privacy by design, as we re-envision it, should aim to identify contextually-bound understandings of privacy, and, to design system architectures, interfaces, default settings as well as corporate policies that reflect them. Thus understood, privacy by design fits under the broad umbrella of VSD, a "theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process."[89] VSD research has focused on a broad set of values, including well being, dignity, justice, welfare, human rights, and privacy.[90] VSD is some-

89 BATYA FRIEDMAN ET AL., DEP'T OF COMPUTER SCI. & ENG'G, UNIV. OF WASH., UW CSE TECHNICAL REPORT NO. 02-12-01, VALUE SENSITIVE DESIGN: THEORY AND METHODS (2001).

90 *See* VALUE SENSITIVE DESIGN: RESEARCH LAB, INFO. SCH. AND DEP'T OF COMPUTER SCI. & ENG'G, UNIV. OF WASH., http://vsdesign.org/people.shtml (last updated June 30, 2011).

what distinct from HCI in that it "exhort[s] designers and producers to include values, purposively, in the set of criteria by which the excellence of technologies is judged"[91] regardless of whether users of a system clamor for them.

Scholars working on VSD are developing methodologies and tools to incorporate values into the design process.[92] They began with values-based criticism of artifacts and systems, but have moved to develop tools to put values into action during the design phase.[93] The goal is to facilitate the development of technological artifacts and systems that support and respect the rich, divergent, and contextually-dependent values of individuals and societies who depend on them.

VSD has deep connections to the more mature field of HCI. For over twenty years researchers in the field of HCI have uncovered privacy-specific issues in technological systems. The methods used by HCI researchers draw from over forty years of work in the field, with roots in cognitive psychology, the social sciences, and human factors research. None were developed to specifically identify privacy problems, yet they have proven effective at finding them. Through these tools and methods, privacy issues emerged through open-ended inquiries into users' concerns. Drawing upon the toolbox of methods used by HCI researchers—surveys, focus groups, qualitative interviews, experiments, and case studies, to name a few—HCI has utilized the user's perspective to successfully identify privacy problems across a broad spectrum of technologies. Some of those findings have been

---

91 Mary Flanagan, Daniel C. Howe, & Helen Nissenbaum, *Embodying Values in Technology: Theory and Practice*, *in* INFORMATION TECHNOLOGY AND MORAL PHILOSOPHY 322 (Jeroen van den Hoven & John Weckert eds. 2008).

92 For an early overview, see BATYA FRIEDMAN, VALUE-SENSITIVE DESIGN: A RESEARCH AGENDA FOR INFORMATION TECHNOLOGY (1999) (providing examples of initiatives that are intended to address social problems associated with the evolution of information technology). For specific examples of frameworks for values in design analysis, see Flanagan, Howe, & Nissenbaum, *supra* note 90, at 322 (Jeroen van den Hoven & John Weckert eds. 2008) (explaining that values may be embodied in technical systems and devices); Mary Flanagan, Daniel C. Howe, & Helen Nissenbaum, *Values at Play: Design Tradeoffs in Socially-Oriented Game Design*, *in* CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 751 (2005) (sketching a methodological framework for the consideration of values during the process of design); FRIEDMAN, *supra* note 89, at 1 (offering an overarching account of value sensitivity design); Phoebe Sengers, Kirsten Boehner, Shay David & Joseph Kaye, *Reflective Design*, *in* PROCEEDINGS OF THE 4TH DECENNIAL ACM CONFERENCE ON CRITICAL COMPUTING 49 (2005), *available at* http://epl.scu.edu/~stsvalues/readings/reflectivedesign.pdf (developing a systematic approach to including critical reflection into the practice of technology design); L. Jean Camp, *Design for Values*, *Design for Trust*, L. JEAN CAMP (Sept. 20, 2006), http://www.ljean.com/design.html.

93 Cory Knobel & Geoffrey C. Bowker, *Computing Ethics Values in Design*, 54 COMM. ACM 26, 28 (2011) (emphasizing that the value in design efforts has been under way for fifteen years).

translated into design frameworks to suggest systematic ways of identifying privacy issues, the original "privacy by design" approach.[94]

HCI work starts with people rather than formal definitions of privacy. Initially, privacy issues surfaced in examinations of the use of novel communication and collaboration tools.[95] For example, in Bellotti and Sellen's 1993 paper offering some of the first explicit privacy design guidance, the authors passed on offering a precise definition of privacy, noting that "[a]ny realistic definition of privacy cannot be static . . . . We take privacy to be a personal notion shaped by culturally determined expectations and perceptions about one's environment."[96] While HCI work continues to uncover privacy concerns through open-ended inquiries, over the past two decades, a growing body of privacy-focused HCI research has emerged to address the development of ubiquitous computing technologies and internet services such as social network sites.[97]

There are two strains of privacy-focused HCI research. Each centers on a distinct theory of privacy. Like legal scholarship, many HCI inquiries are framed around theories of privacy based on individual control over personal information. This branch is rooted in the information self-determination approach affiliated with Alan Westin and data protection. The second branch of HCI inquiry is theoretically oriented around the interpersonal, boundary-driven work of psychologist Irwin Altman (and by implication, sociologist Erving Goffman).[98]

These two orientations have led to research with two distinct foci. The first, grounded in privacy as control, "emphasizes privacy as conscious process." The second, grounded in privacy's role in develop-

---

94 *See generally* DONALD NORMAN, THE DESIGN OF EVERYDAY THINGS (1988) (providing a detailed discussion and examples of privacy frameworks, which they classify as guidelines, process frameworks, and modeling frameworks).

95 Giovanni Iachello & Jason Hong, *End-User Privacy in Human-Computer Interaction*, 1 FOUND. & TRENDS IN HUMAN-COMPUTER INTERACTION 17 (2007) (explaining that human-computer interaction research initially focused on the use of information technology to enable interpersonal communications).

96 Victoria Bellotti & Abigail Sellen, *Designing for Privacy in Ubiquitous Computing Environments*, *in* PROCEEDINGS OF THE THIRD EUROPEAN CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK 77, 78 (G. De Michelis et al., eds. 1993).

97 Others have proposed specific changes to Facebook's architecture grounded in HCI research. *See, e.g.*, Chris Peterson, Losing Face: An Environmental Analysis of Privacy on Facebook 30 (Jan. 2010) (unpublished comment), *available at* http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=cpeterson). Our task here is not to suggest particular changes based on existing research, but to suggest that HCI methods are a tool for identifying and driving privacy issues during design.

98 ALTMAN, *supra* note 51; ERVING GOFFMAN, THE PRESENTATION OF SELF IN EVERYDAY LIFE (1959).

ing the self and community, grounded in the work of Irwin Altman, emphasizes privacy as "intuitive practice."[99] The two approaches are complementary[100] and complement different areas of privacy research: examinations of notice and consent, privacy policies, ubiquitous computing technologies, and general usage of social networks or location sharing services typically are situated in the paradigm of individual control, while studies exploring more socially situated actions, such as personal disclosure on social networks or location-sharing services, are often based in boundary management. The dual approaches have "produced a wealth of tools, including analytic instruments, design guidelines, legislation, and social expectations." It has not yet led to agreement upon what tools work best.[101] Given the deep commitment to contextual solutions, it is somewhat doubtful that a set tool kit will emerge.

While a diverse set of methods are used to identify privacy issues—primarily observational studies, controlled experiments, surveys, case studies, focus groups, and qualitative interviews—the commonality that emerges across them is a focus on users. Users' goals and needs are central to all stages of the design process.[102] It is this objective of centering the analysis (both the problem specification and the solution) on users, rather than on a normative framework, that differentiates HCI-based privacy research from legal scholarship. User-centered design approaches have been used to explore privacy in a diverse set of contexts including peer-to-peer file sharing systems,[103] mobile and online photo sharing,[104] privacy settings on social net-

99 Paul Dourish & Ken Anderson, *Collective Information Practice: Exploring Privacy and Security as Social and Cultural Phenomena*, 21 HUMAN COMPUTER INTERACTION 319, 328 (2006), *available at* http://www.douri.sh/publications/2006/DourishAnderson-InfoPractices-HCIJ.pdf; Leysia Palen & Paul Dourish, *Unpacking "Privacy" for a Networked World*, *in* 5 PROCEEDINGS OF THE CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 129 (2003).

100 Scott Lederer et al., *Personal Privacy Through Understanding and Action: Five Pitfalls for Designers*, 8 PERS. UBIQUIT. COMPUTING 440, 442 (2004).

101 Iachello & Hong, *supra* note 95, at 13.

102 NORMAN, *supra* note 94.

103 *See, e.g.*, Nathaniel S. Good & Aaron Krekelberg, *Usability and Privacy: A Study of KaZaA P2P File-Sharing*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 137 (2003) (detailing how peer-to-peer network users unwittingly share private files).

104 *See, e.g.*, Shane Ahern et al., *Over-Exposed? Privacy Patterns and Considerations in Online and Mobile Photo Sharing in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 357 (2007) (focusing on how users share photos over social networks).

works,[105] information flow in RFID-enabled documents,[106] and user comprehension of legal notice and consent in software systems.[107] This context-specific approach creates detailed portraits of privacy issues across a variety of domains. The research outputs range from rich qualitative inquiries[108] to broad nationally representative opinion samples.[109]

HCI research places the user at the center of the inquiry, though the outcome of HCI research aims to represent as many germane perspectives as possible (and not simply a single "user") in order to generate a privacy model that reflects actual experiences and norms related to privacy regardless of theoretical grounding. A central aspect to this process is that, when done well, it is both iterative and empirical; researchers begin with a theory or framework that they think best captures the relationship between users and their potential privacy concerns and can refine it as appropriate after subjecting it to testing and analysis. An iterative approach can identify potential privacy mismatches between researchers and users and avoids a top-down imposition of the research organization's values on the users. Once the privacy relationship between the users, operators, and the technology is empirically modeled, then researchers can work directly with project managers and engineers to ensure it is reflected in both the system architecture and the processes for using the system.

---

105 *See, e.g.*, Zeynep Tufekci, *Can You See Me Now? Audience and Disclosure Regulation in Online Social Network Sites*, 28 BULL. OF SCI. TECH. & SOC'Y 20 (2008) (finding little connection between the desired privacy level of users and those users' actual privacy settings on social networks).

106 *See, e.g.*, Jennifer King & Aylin Selcukoglu, *Where's the Beep? A Case Study of User Misunderstandings of RFID in* 2011 IEEE INTERNATIONAL CONFERENCE ON RFID 192–99 (Apr. 2011) (exploring implementation of radio frequency identification technology in credit cards, passports, and transit passes affects user privacy concerns).

107 Nathaniel S. Good, Jens Grossklags, Deirdre K. Mulligan, & Joseph A. Konstan, *Noticing Notice: A Large-Scale Experiment on the Timing of Software License Agreements*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 607, 615 (2007); Jens Grossklags & Nathan Good, *Empirical Studies on Software Notices to Inform Policy Makers and Usability Designers*, *in* FINANCIAL CRYPTOGRAPHY AND DATA SECURITY 341–55 (Sven Dietrich and Rachna Dhamija eds., 2007).

108 Michelle Kwasny, Kelly Caine, Wendy A. Rogers & Arthur D. Fisk, *Privacy and Technology: Folk Definitions and Perspectives*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 3291–96 (2008); Judith S. Olson, Jonathan Grudin & Eric Horvitz, *Toward Understanding Preferences for Sharing and Privacy*, *in* PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1985–88 (2005).

109 Chris Hoofnagle, Jennifer King, Su Li, & Joseph Turow, *How Different Are Young Adults from Older Adults When It Comes to Information Privacy Attitudes and Policies?* 3 (U.C. Berkeley Ctr. for Law and Tech., Working Paper, 2010), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_*id*=1589864.

Unearthing users' expectations ensures that the theoretical framework chosen to guide system design captures users' conceptions of privacy. For example, had Facebook used contextual integrity theory to analyze News Feed's previously existing norms of information flow, their designers might have anticipated many of their users' complaints and designed the changes with these norms in mind, allowing those who wished to broadcast their Feed far and wide to do so while respecting the concerns of others. Nissenbaum, from the VSD perspective, would have contextually grounded the review of status updates. While Facebook is somewhat sui generis, its purpose is to promote social interaction among friends. Thus the proper question to ask would be what sorts of information flows are necessary to support friendship. Such an inquiry would have invited reflection on the differences between the vernacular category friend and the Facebook category Friend. It may have revealed some tension between broad friending which is beneficial to both Facebook and users and dissemination models that eliminate the transaction costs that sorted vernacular friends from Facebook friends. Two HCI-specific methods could have surfaced this potential problem: a study examining users' motivations for using the (Mini) Feed and their expected audience and testing of the proposed changes with a broad population of users. While the eventual result might have in fact been the News Feed as we know it in 2011—a push mechanism but with the ability to select among friends on both the sending and receiving ends—a deliberative approach centered on user needs and values could have saved the company from months of backlash by proactively identifying concerns and incorporating features similar to those they later retrofitted. A complementary argument can be made with respect to boundary regulation; if Facebook had been interested in exploring whether their existing architecture supported the lines users drew (or wanted to draw) between their public profiles and their respective audiences, they could have conducted a qualitative study to identify how and why their user population utilized profile privacy settings. Had the company subjected its privacy settings to an analysis within this framework prior to making their much-derided architectural changes in December 2009,[110] when the profile defaults were changed to expose more information, the company might have realized then that the site's network structure was insufficient for supporting com-

110 Zuckerberg, *supra* note 26 (describing the company's 2009 "simplification," after which user information was available to "friends, friends of . . . friends, or everyone," rather than only within certain networks).

plex boundary management. This case was not one of accident but of deliberate choice on the part of founder Mark Zuckerberg, who has stated that having more than one identity—"a different image for your work friends or co-workers and for the other people that you know"—demonstrates "a lack of integrity."[111] Zuckerberg attempted to prioritize his values in the site design. His values apparently conflicted with those of many Facebook users. If Facebook had understood that Zuckerberg's opinion on this issue was not universal, they might have avoided user protests and post-launch modifications. Perhaps they would have worked with a privacy model that supported more granular options for sharing profile data and facilitated the maintenance of multiple identities.[112]

The theories we have identified as useful for understanding lateral privacy concerns in SNSs and platforms, due to their deeply contextual and human-centered orientation, require processes of discovery, not just implementation. HCI and VSD provide uniquely helpful methods to aid in the discovery process as well as implementation. Contextual integrity, for example, calls attention to existing norms and information flows. At a minimum, researchers employing this framework should appreciate the "radical heterogeneity"[113] of online experience and its interconnection to offline experiences, and therefore view efforts to export rules across contexts skeptically. Researchers should explore and document users' extant privacy definitions and expectations and test whether proposed architectures and designs support or violate these definitions. To the extent that the system under inquiry involves social interactions, researchers and designers should pay special attention to the social relationships their system enables, and whether users have the tools necessary to maintain the boundaries that regulate their sense of privacy in accordance with their expectations.

While HCI has a track record of success in identifying privacy concerns, it lacks a cohesive, prescriptive method to guide subsequent inquiries. This is partially because privacy research in HCI is in

---

111 Kim-Mai Cutler, *Why Mark Zuckerberg Needs to Come Clean About His Views on Privacy*, VENTUREBEAT (May 13, 2010), http://venturebeat.com/2010/05/13/zuckerberg-privacy/ (quoting DAVID KIRKPATRICK, THE FACEBOOK EFFECT 199 (2010)).

112 *See also* Mark Zuckerberg, *Making Control Simple*, The FACEBOOK BLOG (May 26, 2010, 1:55 PM), http://blog.facebook.com/blog.php?post=391922327130 (explaining the changes to Facebook's privacy settings intended to make Facebook privacy simpler to control).

113 *See* Nissenbaum, *supra* note 81, at 37, 41 ("As long as public discourse about privacy online takes the marketplace and commerce as proxies for the whole, conceptions of privacy will be inadequate. We need to take full account of the radical heterogeneity of online activity and practice.").

its early adolescence. Iachello and Hong characterize the state of the field as "unorganized and dispersed" and suggest that "understanding privacy requires HCI practitioners to expand their field of view from traditional HCI domains such as social psychology and cognitive science, to a broader picture which includes economics and law."[114] However, even when mature, the context-dependent nature of HCI privacy inquiry suggests that it will never be tightly prescriptive. HCI privacy inquiry is not amenable to off-the-shelf decisional tools or paper processes. The HCI professional's value is in part the judgment to ascertain what method is appropriate for a given situation.

V. NEW REGULATORY DIRECTIONS

We have argued that corporations should embrace definitions of privacy that are contextual and contingent, and adopt HCI and related VSD methodologies to construct these definitions and drive their implementation in design. These tools are appropriate because they seek to discover privacy, rather than dictate or assume it.

The steady stream of privacy blunders stemming from a lack of attention or actual disregard for users' privacy expectations suggest that companies have not adopted HCI-focused approaches, or, if they have, that that HCI input has been devalued. Given that Facebook, Google, Apple, Microsoft, Twitter, and other companies employ significant numbers of HCI researchers, it is likely that such privacy failures can be attributed to both lack of adoption of HCI methods and disregard for HCI-based insight when in tension with other business goals.

The release of Google Buzz offers a glimpse into one privacy incident that might have been avoided if an HCI-grounded inquiry had been used to understand the privacy expectations of users and inform design. Google typically offers beta releases of its products and uses feedback during this period to work out glitches, including privacy glitches. Unlike other products that reportedly are tested by a group of family and friends as well as employees, Buzz skipped this limited external testing.[115] Instead, it underwent only internal employee testing known colloquially as "dogfooding."[116] This process failed to

---

114 Iachello & Hong, *supra* note 95, at 114–15.

115 Jonathan Fildes, *Google Admits Buzz Social Network Testing Flaws*, BBC NEWS (Feb. 16, 2010), http://news.bbc.co.uk/2/hi/technology/8517613.stm.

116 *See generally* Warren Harrison, *Eating Your Own Dog Food*, IEEE SOFTWARE, May & June 2006, at 5–7 ("[T]he software industry has adopted the phrase to mean that a company uses its own products.").

identify the privacy problems that the public noted upon launch.[117] After Buzz launched, a former Google designer who worked on the product released a widely viewed presentation on the future of social networks, which indirectly critiqued many of the privacy problems raised by Buzz.[118] Thus, even Google, an engineering organization employing hundreds of user experience researchers, was apparently deaf to their recommendations, resulting in a flurry of privacy blunders,[119] a class-action lawsuit, and ultimately a settlement with the Federal Trade Commission ("FTC").[120] Ironically, the designer subsequently left the company for Facebook, noting that "Google is an engineering company, and as a researcher or designer, it's very difficult to have your voice heard at a strategic level . . . . Google values technology, not social science."[121] Companies may run roughshod

117 *See* Fildes, *supra* note 112 (describing the series of changes made to Google Buzz after consumer backlash concerning the privacy settings). HCI researchers identify several reasons dogfooding is an insufficient replacement for user testing. First, it is difficult for employees to step out of evaluator mode—a mode of rational, reflective process—and into user mode—dominated by a subjective relation to objects, an experiential mode. *See* Elizabeth F. Churchill, *The (Anti)Social Net*, INTERACTIONS, Sept. & Oct. 2010, at 23, *available at* http://doi.acm.org/10.1145/1836216.1836222 ("Geeks, computer scientists, and mathematicians who love networks are not good people to assess your social-networking products . . . because we operate simultaneously in user and evaluator mode . . . ."). Second, employees at technology companies tend to be expert users, while the population as a whole is not. Generalizing based on test results from the expert population is dangerous. It is true that even expert users misunderstand the privacy implications of settings. *See* MICHELLE MADEJSKI, MARITZA JOHNSON, & STEVEN M. BELLOVIN, COLUMBIA UNIV. COMPUTER SCI., TECHNICAL REPORT NO. CUCS-010-11, THE FAILURE OF ONLINE SOCIAL NETWORK PRIVACY SETTINGS 7–11 (2011), *available at* https://mice.cs.columbia.edu/getTechreport.php?techreportID=1459 (showing that even their study's sample pool, college students who are expert Facebook users, did not understand how to protect their privacy). Non-experts, however, have a greater tendency to engage in over-sharing that results in problematic "misclosures." Kwasny, *supra* note 105, at 2393. In addition, many employees of social network sites are enthralled with networks qua networks: they are not "people" persons.

118 *See* Paul Adams, *The Real Life Social Network*, (Jul. 1 2010), http://www.slideshare.net/padday/the-real-life-social-network-v2 (cautioning companies that failing to safeguard private information will lead to a decrease in consumer trust and criticizing companies for difficult to understand privacy settings).

119 Alma Whitten, *An Update on Buzz*, THE OFFICIAL GOOGLE BLOG (Mar. 30, 2011, 7:30 AM), http://googleblog.blogspot.com/2011/03/update-on-buzz.html (admitting that Google Buzz fell short of standards for transparency and user control).

120 Press Release, Federal Trade Commission, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm ("Google Inc. has agreed to settle Federal Trade Commission charges that it used deceptive tactics and violated its own privacy promises to consumers when it launched its social network, Google Buzz, in 2010.").

121 Paul Adams, *Why I Left Google. What Happened to My Book. What I Work on at Facebook*, THINK OUTSIDE IN (July 12, 2011), http://www.thinkoutsidein.com/blog/2011/07/why-i-left-google-what-happened-to-my-book-what-i-work-on-at-facebook/.

over decisions that protect users privacy when they are in tension with other factors.

A key question is therefore what might regulators do to prompt the adoption of HCI and VSD methodologies to identify and respond to privacy issues in the design of SNSs and platforms. Two conditions set out in recent FTC settlements could, if appropriately fueled, drive corporate privacy activities in this direction.

First, the two recent settlements require companies to establish a comprehensive privacy program ("CPP"). Per the agreements, a CPP must include specific processes aimed at identifying "reasonably foreseeable, material [privacy] risks"[122] in "product design, [and] development"[123] and to design, implement, and iteratively monitor, test, and improve "reasonable privacy controls and procedures."[124] The activities called for under the "comprehensive privacy program" appear uniquely aligned with HCI approaches.

Second, the decision in a separate settlement to constrain the acceptance of pro forma disclosures of deviant information flows is dispositive of the fairness of a surveillance practice. The FTC rejected a company's effort to egregiously violate users' privacy by engaging in widespread monitoring of all their online activities based on a buried disclosure in their terms of service—despite the fact that the company's notice was detailed and alarming.[125] The implication of the order is that companies have an obligation to attend to consumers' understandings of the normal rules of engagement during online interactions and that if they want to deviate and capture novel information they must "clearly and prominently disclose" and gain consent through a mechanism other than the End-User License Agreement ("EULA"), Privacy Policy, or Terms of Service ("TOS").[126] By limiting the ability of companies to unilaterally define consumers' expectations, the FTC is shifting away from a contract-based regime toward a more tort-based regime focused on fairness—an approach imminent-

122 Agreement Containing Consent Order at § III, para. B, *In re* Google Inc., No. 102-3136 (F.T.C. 2011), *available at* http://www.ftc.gov/os/caselist/1023136/110330googlebuzzagreeorder.pdf [hereinafter Google Order].

123 *Id.*

124 *Id.* at § III, para. C.

125 *In re* Sears Holding Mgmt. Corp., Docket No. C-4264 (issued Aug. 31, 2009) (complaint), *available at* http://www.ftc.gov/os/caselist/0823099/090604searscmpt.pdf.

126 Sears Order § I. The order in the Google case contains a similar provision requiring separate notice and consent procedures for disclosures of a Google user's information. Google Order, *supra* note 124, at § II.

ly consistent with the FTC's enabling statute and in line with a series of settlements in security cases based on allegations of unfairness.[127]

Corporate lawyers have complained that the shift from an analysis of the adequacy of notices to an assessment of the milieu in which the interaction occurs provides inadequate guidance to companies and invites endless Monday morning quarterbacking by the FTC and advocates.[128] There is some truth to this; however an alternative outcome could be greater corporate reliance on HCI professionals to understand users' expectations and ensure that deviations are justifiable and clearly spelled out.

Taken together, these settlements set the stage for HCI-based approaches. However, they will not take root on their own. While there is some evidence that at least a subset of corporations were using a contextually-driven, consumer expectations-oriented definition of privacy to inform corporate privacy activities, and that this approach emerged in part due to the activities of the FTC,[129] the requirements of these orders set the stage for more attention to consumer expectations. With these recent actions the FTC posits that privacy is not exclusively the product of a contractual agreement. Implicitly, this precludes using a single or consistent notice—or approach—across a range of services or practices, because doing so fails to acknowledge privacy's contextual tether. The clauses strongly suggest that corpo-

---

127 In a series of actions, the Commission has brought unfairness claims against companies for breaches of data security despite the fact that they had not made representations regarding data security. *See, e.g.*, *In re* Vision I Props., L.L.C., 139 F.T.C. 296 (2005) (alleging unfairness rather than deception); *In re* BJ's Wholesale Club, Inc., 140 F.T.C. 465 (2005) (alleging unfairness where no statements were made about security); *see also* Andrew B. Serwin, *The FTC's Increased Focus on Protecting Personal Information: An Overview of Enforcement and Guidance* (Nov. 22, 2008), *available at* http://ssrn.com/abstract=1305669 (discussing the impact of FTC actions on the data security obligations of corporations).

128 *See, e.g.*, Alan Charles Raul et al., *End of the Notice Paradigm?: FTC's Proposed* Sears *Settlement Casts Doubt On the Sufficiency of Disclosures in Privacy Policies and User Agreements*, 8 PRIVACY & SEC. L. REP. 1070, 1070–71 (2009) ("Heretofore, the FTC had emphasized that it was not engaged in a game of 'Gotcha' with online business. The *Sears* settlement, on the other hand, could easily have caught the respondent company by surprise—especially since Sears was unquestionably providing something of value to the participating consumers in exchange for their reduced privacy (i.e., paying them cash) . . . If this decision is finalized in its current form, and if the Commissioners indicate that the erstwhile notice paradigm is legally insufficient to protect consumers, then the FTC should publish clear rules for how they expect companies to communicate online with their consumers."); *see also* Michael D. Scott, *The FTC, the Unfairness Doctrine and Data Security Breach Litigation: Has the Commission Gone Too Far?* (Aug. 20, 2007), *available at* http://ssrn.com/abstract=1012232 (discussing and criticizing the FTC's data security cases under the unfairness doctrine on a similar basis).

129 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247 (2011).

rations should pay greater attention to their customers' intuitive understanding of the data flows in the technical environment. The contours of the "comprehensive privacy program" set out in the Google Order clearly require activities to understand privacy from the users' perspective. Designing, implementing, testing, and monitoring "reasonable privacy controls and procedures" requires interaction with users. Surely some relevant users of privacy controls will be inside the company; however, just as surely some privacy controls will be provided to consumers themselves and assessing the reasonableness of such controls, monitoring them, and testing them all require interactions with users. The Google Buzz consent decree seemingly indicates that the FTC will be pushing firms to develop processes that embed privacy into corporate practice and technical design.[130]

Taken together these settlements could begin to steer the law toward HCI inquiry. Understanding privacy protection as a process of iterative assessment of privacy risks and responsive design may drive corporations to embrace HCI methods and tools. However, given the predominance of lawyers and notice and consent-based privacy approaches, greater direction and encouragement will likely be required to drive their adoption.

In the absence of new legal authority, the FTC could choose among several options for advancing the use of HCI methods by firms. The FTC has begun to issue guidance in the wake of the Google Buzz settlement by urging companies to "bake privacy in" and "consider it from the get go."[131] Through workshops and reports it could provide important exposure to HCI research methods.

In the past, the FTC has devoted substantial effort to support the production of a shared knowledge base, the exchange of ideas between practitioners and researchers, and the sharing of best practices on significant consumer protection issues, including privacy. For example, the issues of "online profiling" and "behavioral advertising" have been the subject of numerous FTC workshops over the past decade.[132] To assist the business community in implementing legally

130 Press Release, Federal Trade Comm'n, FTC Charges Deceptive Privacy Practices in Google's Rollout of Its Buzz Social Network (Mar. 30, 2011), *available at* http://www.ftc.gov/opa/2011/03/google.shtm.

131 Lesley Fair, *The FTC's Settlement with Google: Part 4*, FEDERAL TRADE COMM'N BUREAU OF CONSUMER PROTECTION BUSINESS CTR. (Apr. 14, 2011, 5:53 PM), http://business.ftc.gov/blog/2011/04/ftcs-settlement-google-part-4.

132 *See, e.g.*, FTC Workshop, Monitoring Software on Your PC: Spyware, Adware, and Other Software (Apr. 19, 2004), *available at* http://www.ftc.gov/bcp/workshops/spyware/index.shtm; FTC Workshop, The Information Marketplace: Merging and Exchanging Consumer Data (Mar. 13, 2001), *available at* http://www.ftc.gov/bcp/

mandated financial privacy notices, the FTC cooperated with the other eight regulatory agencies responsible for implementation of the privacy provisions of the Gram Leach Bliley Act to host a workshop on effective notices.[133] The workshop brought the expertise of academic and professional experts in the communication field to the attention of regulated entities for the purpose of providing guidance and methods for effective notices.[134] Similar public workshops were held to examine "negative options."[135] Again, academic and professional experts were brought in to discuss the issues. Ultimately a staff report based on the FTC's law enforcement actions and the workshop was issued setting out principles for avoiding deception in negative options.[136] The FTC could pursue a similar path with privacy issues in social network sites and platforms. The privacy by design requirement found in the recent preliminary FTC staff report on "Protecting Consumer Privacy in an Era of Rapid Change"[137] can be viewed as an early step in this direction. Follow-up workshops that explore the use of HCI techniques could be quite beneficial to platform and social network site developers who will find incomplete guidance, at best, in existing privacy by design approaches. Convening experts from the fields of VSD and HCI to discuss their approaches could begin to generate industry interest in a more robust privacy by design toolbox.

---

workshops/infomktplace/index.shtml; FTC Town Hall, Ehavioral Advertising: Tracking, Targeting & Technology (Nov. 1–2, 2007), *available at* http://www.ftc.gov/bcp/workshops/ehavioral/index.shtml.

133 See Press Release, Federal Trade Commission, Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices, Fed. Trade Comm'n (Dec. 4, 2001), *available at* http://www.ftc.gov/bcp/workshops/glb/index.shtml (describing a workshop educating individuals about changes in privacy rules after the GLB Act).

134 See Agenda, Interagency Public Workshop: Get Noticed: Effective Financial Privacy Notices, Fed. Trade Comm'n (Dec. 4, 2001), *available at* http://www.ftc.gov/bcp/workshops/glb/agenda.htm (explaining that the aim of one panel was to "provide guidance in communicating complex information to consumers. . . [and] discuss various tools that may assist financial institutions in crafting understandable privacy notices" with panelists including Deborah S. Bosley, Ph.D., Director of the University Writing Programs at the University of North Carolina at Charlotte, Mark Hochhauser, Ph.D., Readability Consultant, and Alan Levy, Ph.D., Senior Scientist, Consumer Studies Team, Center for Food Safety and Applied Nutrition, Food and Drug Administration).

135 FED. TRADE COMM'N, NEGATIVE OPTIONS: A REPORT BY THE STAFF OF THE FTC DIVISION OF ENFORCEMENT i–ii, iv (Jan. 2009), *available at* http://www.ftc.gov/os/2009/02/P064202negativeoptionreport.pdf

136 *See id.* at i. ("On January 25, 2007, the Federal Trade Commission hosted a workshop that brought together industry representatives, consumer groups, and members of the academic community to discuss negative option marketing.").

137 FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: A PROPOSED FRAMEWORK FOR BUSINESSES AND POLICYMAKERS (Dec. 2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf.

The FTC could raise the pressure and attempt to use its soft law powers to encourage companies in the platform and social network site businesses to establish a set of self-regulatory guidelines on how to use HCI in their privacy work. Ideally, such guidelines would require companies to use HCI methods to identify and address privacy issues. The development of the Network Advertising Initiative guidelines[138] provides an example of a self-regulatory code that developed in response to ongoing scrutiny by the FTC.[139] Given the relentless barrage of privacy complaints and increasing regulatory scrutiny companies such as Google, Facebook, Apple, Microsoft, and Twitter are facing, they may find it useful to collaborate on a process-oriented set of guidelines for considering privacy issues. Such agreement might be quite advantageous in navigating the regulatory chaos. By agreeing on process-based guidelines they would retain ample room to make distinct choices about the design, defaults, and policies they put in place. The value of adherence to a self-regulatory code for a business varies greatly depending upon the extent to which it disrupts business practices, its strength, public perception of its legitimacy, and the willingness of relevant regulators to endorse it. In an area of emerging regulatory requirements, self-regulatory codes offer industry an opportunity to proactively shape the legal landscape. Given that privacy is ambiguous, and likely to remain that way, and that regulators are rolling out new requirements to address it during all phases of business and product development but have not yet clarified exactly what is expected, the timing of an effort to clarify what

---

138 NETWORK ADVERTISING INITIATIVE, SELF-REGULATORY PRINCIPLES FOR ONLINE PREFERENCE MARKETING BY NETWORK ADVERTISERS (2000), *available at* http://www.ftc.gov/os/2000/07/NAI%207-10%20Final.pdf (guiding business practices with respect to online advertisement).

139 An FTC workshop, and media and advocate scrutiny, led to the adoption of an initial set of guidelines by ten companies: 24/7 Media; AdForce; AdKnowledge; Adsmart; DoubleClick; Engage; Flycast; MatchLogic; NetGravity; and Real Media. *See Comments of the Network Advertising Initiative, Testimony at the Public Workshop on Online Profiling*, FED. TRADE COMM'N (Nov. 8, 1999), http://www.ftc.gov/bcp/workshops/profiling/comments/nai.htm (describing the Network's motivation for drafting the guidelines). In the wake of ongoing FTC focus, including complaints and investigations, a broader group of companies adopted a revised set of principles. For the most recent NAI Code, see NETWORK ADVER. INITIATIVE, 2008 NAI PRINCIPLES: THE NETWORK ADVERTISING INITIATIVE'S SELF-REGULATORY CODE OF CONDUCT (2008), *available at* http://www.networkadvertising.org/networks/2008%20NAI%20Principles_final%20for%20Website.pdf. For a discussion of the FTC workshop and overview of the FTC's early activities, see FED. TRADE COMM'N, ONLINE PROFILING: A REPORT TO CONGRESS (2000), *available at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf. For an update on recent FTC activities, see FED. TRADE COMM'N, SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING (2009), *available at* http://www.ftc.gov/os/2009/02/P085400behavadreport.pdf.

sort of design processes are appropriate to address privacy may be ripe and beneficial.

The stage is set for HCI and VSD research and design to take its place in the regulatory landscape. The FTC would do well to use its convening skills to begin to solidify the relationship between its direction to companies and this emerging field.

CONCLUSION

> [A]general principle is that we should attempt to design *responsive environments*, which permit easy alternation between a state of separateness and a state of togetherness. If privacy has a shifting dialectic quality, then, ideally, we should offer people environments that can be responsive to their shifting desires for contact or absence of contact with others . . . . The logic of our framework calls for more use of changeable environments so as to permit a greater responsiveness to changing needs for privacy.[140]

Irwin Altman's words endure. The plasticity of SNSs and platforms that support a growing percentage of human interaction makes them arguably more relevant and more pressing. Society wants privacy expectations reflected in the information flows afforded by these built environments. Yet the absence of a sound theoretical framework is problematic for corporations that lack guidance and find their decisions subjected to heavy hindsight criticism. It prevents privacy professionals within firms from systematizing approaches across the firm. It is equally problematic for regulators whose actions can be portrayed as unjustified and unsupported.[141]

Privacy by design is an exceedingly important regulatory initiative. Artifacts matter and ought to assist in protecting social values including privacy. However, building the right "privacy" into design is critical, and today regulators are working with an extremely cramped definition of privacy. Individual control may be the touchstone of data protection, but it is not the touchstone of privacy protection.

It is time to think of the internet as more than the latest marketing database. It is the public square, the private living room, the café, and the schoolyard. Privacy must relate to the varied nature of these environments and the activities that occur within them. Privacy is

---

140 ALTMAN, *supra* note 36, at 207–08.

141 *See, e.g.*, Alan Charles Raul et al., *End of the Notice Paradigm?: FTC's Proposed Sears Settlement Casts Doubt On the Sufficiency of Disclosures in Privacy Policies and User Agreements*, 8 PRIVACY & SEC. L. REP. 1070, 1070 (2009) (criticizing an FTC settlement with a national retailer regarding its failure to adequately disclose the scope of consumer personal information being collected by marketing research software).

contextual and fluid. It is individual and social. It is justified, challenged, and negotiated.

Privacy so-defined requires processes of discovery to precede design. HCI and VSD offer tools for unearthing relevant conceptions of privacy. Corporations need a reason to adopt them. Recent activity at the FTC provides an opening to connect the HCI and VSD community of researchers and practitioners to the regulatory endeavor. The FTC has an opportunity to facilitate the development of a new set of privacy professionals within firms: HCI and VSD researchers and designers. Doing so would breathe life into the call for privacy by design, animating privacy, and emboldening design.