*Cyber-surveillance in Everyday Life * May 12-15, 2011 * University of Toronto*

# Reconfiguring the House of Mirrors: Narrowing Digitally Mediated Surveillance on Facebook[1]

Deborah G. Johnson
University of Virginia

Priscilla M. Regan
George Mason University

## Introduction

In ongoing and previous work, we develop a house of mirrors metaphor to shed light on digitally-mediated systems of accountability involving transparency and surveillance. Facebook is framed as an accountability system alongside campaign finance disclosure, Secure Flight, user tracking by Google, and the American Red Cross blood donation system. The house of mirrors metaphor provides a framework for understanding the movement and transformation of personal information that takes place in these systems and the normative implications. In a house of mirrors the subject is viewed as fragmented, split into selected parts, with some parts exaggerated and others shrouded. In the case of Facebook, users select a subset of information about themselves, highlighting and shading certain dimensions of their selves. Facebook then transmits this data—like images in parallel mirrors, infinitely multiplied—not only to "friends" and "friends of friends," but also to marketers who target users based on their selected activities, interests and expressed tastes.

Although the house of mirrors metaphor can be used broadly to understand digitally-mediated systems, our central concern in this paper is to address the tension between privacy and the display of personal information that seems to be inherent in social networking sites. We focus exclusively on Facebook and we ask in particular how the house of mirrors might be reconfigured to limit and mitigate surveillance. We ask whether revising and refining privacy notices effectively controls the movement of personal information within a hall of mirrors. Will imposing technical controls or standards over the flow of information is an effective mechanism? Will government regulations over the revelation, collection and exchanges of information be necessary? Or is there some other leverage point to limit surveillance that is revealed by the house of mirrors metaphor? The focus of our analysis extends beyond traditional studies of policy tools as it specifically examines the processes in socio-technically configured halls of mirrors.

We begin with a brief summary of the house of mirrors metaphor and how it applies to Facebook. Next we explore how relationships and accounts of an individual are rendered in the Facebook house of mirrors. Finally we provide an analysis of how the mirrors might be reconfigured to better protect the privacy of Facebook users.

[1] This research is supported by a grant, "Technology and Democracy: Surveillance and Transparency as Sociotechnical Systems of Accountability" (SES-0823363), from the National Science Foundation. The grant has funded discussion and collaboration among a team of researchers composed of the authors and Roberto Armengol, Siva Vaidhyanathan, Kent Wayland, Alfred Weaver and Kathleen Weston – all at the University of Virginia.

**House of Mirrors**[2]

Both surveillance and transparency involve revelation of information for purposes of accountability; that is, in both types of systems there are watchers, watched, and accounts of the watched. Most importantly in both types of systems, the revelation of information is in tension with the privacy of the watched. Whether the revelation of information is controlled by the watched, as is typically the case in transparency, or controlled by the watcher, as in surveillance, the information becomes available to those who can use it for purposes unbeknownst to the watched. This tension arises regardless of the medium in which the information is collected and used, but it is exacerbated and reconfigured in an electronic medium. Understanding of the nature of the electronic medium is, then, essential to understanding the tension and how it can be managed or navigated.

Conceptually, 'surveillance' and 'transparency' are overly simplistic notions for understanding electronic or digitally-mediated systems. 'Surveillance' suggests direct observation and accurate information about the watched flowing to watchers. 'Transparency' suggests that those who are watched simply remove the shrouds and reveal what they are doing. Yet, even a cursory examination of digitally-mediated systems suggests that transparency systems are far from transparent and surveillance systems are far from direct or accurate observations of individuals. By contrast, the house of mirrors metaphor captures the complexities of digitally-mediated systems of accountability and the processes by which information and, ultimately, the watched are rendered. The house of mirrors metaphor is a heuristic device to tease out the myriad ways that information is transformed and repurposed in the electronic medium. Indeed, a house of mirror analysis indicates that we ought to be cautious in presuming that digitally-mediated transparency and surveillance are suitable forms of accountability for democratic institutions.

A house of mirrors is full of reflection, refraction, multiplication of images, and unpredictable perspectives; a person standing in a house of mirrors sees aspects of her body seemingly distorted, that is, elongated, shortened, exaggerated, and fragmented. A house of mirrors is a complex of imagery, with bouncing, highlighting, and shading of images that produce a surprising experience. An individual sees an image of himself out of whack with his own sense of self. Importantly, the distortion is far from random; it is the result of the way the mirrors have been made, the placement of the mirrors in the architecture of a building, the lighting, the expectations that individuals have when they enter which in turn have been shaped by the representations encountered before entering, and so on. A proliferation of images are created with some emphasizing this aspect and some that aspect of a person, some quite fine-tuned and some wide-angled, and with some in bright light and some in shade or near dark. No image is complete and no image is a completely accurate representation of the person.

The house of mirrors metaphor suggests that there are at least four types of processes at work in digitally-mediated accountability systems. First there is an *entry* point at which data about an individual is entered either by the individual or someone else. The entered

[2] For more complete discussion of the house of mirrors metaphor, see: Deborah Johnson, Priscilla M. Regan and Kent Wayland, "Campaign Disclosure, Privacy and Transparency," *William & Mary Bill of Rights Journal* (forthcoming). For application of the house of mirrors metaphor to Facebook, see: Priscilla M. Regan and Kent Wayland, "Facebook Funhouse: Notes on Personal Transparency and Peer Surveillance," Prepared for Conference Presentation at: A Global Surveillance Society? City University London, April 13-15, 2010.

data constitutes an initial image or representation of an individual. Next, the entry representation may *bounce* as the initial representation moves to different places, is multiplies, and becomes accessible to different viewers. As the initial image bounces, aspects of the person are *highlighted or shaded* in ways that depend on where the initial representation has gone, e.g., to a mirror that elongates or shrinks different components. Finally, the person exits the house of mirrors with a different sense of how they look; their companions in the house may also have a new picture of how the individual looks. We refer to this stage as *rendering*. The individual has been rendered in a particular way that results from the house of mirrors.

The four stages can be used to understand what happens in Facebook. Individuals (users) enter the house of mirrors when they create a Facebook site. The information that is entered constitutes a reflection or image of the individual in the sense that a reflection is a reduction—a 'trace' of the person as some surveillance scholars suggest. The representation is a selected subset of all possible information about that individual. In the case of Facebook, the template structures the image created by specifying categories in which one must present one's self. Just as the image one sees in a mirror depends on the nature of the mirror, the Facebook templates control what sort of representation a user can construct.

Entry into the Facebook house of mirrors might be thought initially to be a self-reflection. The user fills in the profile and sees how it looks, i.e., sees the presentation of self. Of course, the reflection is generally created for presentation to a particular audience, one's (Facebook) friends. The self-presentation is partial and affected by the viewing conditions, including the viewing medium. Two aspects of the construction of this original reflection are particularly important to consider.

First, this reflection is constructed not only out of text but also links, photos and video. The multi-media nature of the Facebook reflection enhances the power of the original reflection. As part of the Facebook templates, links allow a person to refer to anything on the internet and comment on it, positing positions on politics, music, food, humor and so on. Photographs allow users to present their identity in relation to family and activities or events that are considered photo-worthy. One's profile potentially lists relatively enduring aspects of identity, such as certain social roles (employee, spouse), tastes in media, political views, religion, and so on. Similarly, the groups a person joins or the persons or entities of which one becomes a "fan" also suggest relatively enduring aspects of a person. The daily flow of activity, on the other hand, offers the chance for immediate performance of one's self. One's "status updates" are broadcast to all friends right away, and they include commentary on anything imaginable, from mood to meals to news to Facebook itself. Likewise, one's photos capture current events, and comments on others' statuses, photos, or comments represent an asynchronous conversation with others, or perhaps a contingent representation of self. The different modes of expression, then, allow for a rich presentation of self, both in the moment and over time.

Second, Facebook requires that the representation be linked to a real person and *only* one person. This produces the practical result that individuals have only one profile, not multiple identities. In some sense, Facebook seems to invite individuals to build a single network that encompasses all of their experiences, from high school, college, work, and any other shared experiences. Thus, one account includes all of a user's friends, although knowledgeable users can spend time forming different categories of friends and then control the content that each category sees. For many users, *all* of a person's friends are

the primary audience for their reflection.

Once the user sets up a Facebook site and designates friends, the representation bounces as in a house of mirrors, from place to place, that is, viewer to viewer. To whom the image bounces depends on how the user has specified the Facebook settings for their site. If the user does nothing, the default settings determine who has access. The privacy settings determine how broadly beyond an identified circle of friends a user's postings reach. A user's information may be available to "friends of friends," one's "network," or even just "everyone." The bouncing occurs not just from user to other users for Facebook itself is one of the watchers. Fackbook follows users' clickstreams. As well, advertisers and applications can glean information from a profile; interested officials can exploit a shared network or even employ a subpoena to collect information; and search engines can pick up the data that Facebook requires to be public.

As these images bounce to audiences seen and unseen, highlighting and shading occurs, according to the perspective of the viewer. On Facebook friends are encouraged to comment, respond, provoke, and engage. In doing so, certain aspects of the original image are emphasized (highlighted) and others are ignored (shaded). These responses can crucially affect the self-presentation of the original individual because they inflect the original comment, assertion, argument, photograph or link. In other words, friends' comments may reframe the presentation of self, in unexpected ways. Distinctly personal information like political views, religion, sexual orientation, and marital status are all potentially highlighted in the system. The news feed highlights the instant thoughts and opinions of one's friends, inviting a reactive response. Users are notified of others who respond to the items to which they responded, highlighting that particular conversation topic even more. Multiple viewers each focus on different aspects of the user, highlighting particular features that are of interest to them while shading everything else.

The final stage in a house of mirrors is rendering. The operations of Facebook—the interactions among friends, the responses of friends, the uses of information by friends and non-friends, the architecture of the system and its policies, yield multiple renderings of the user. Various friends form views of the user, Facebook has an account of the user, unintended viewers such as advertisers, potential employers, and law enforcement all render accounts of the user.

While these four processes do not capture all that goes on in Facebook, they demonstrate just how Facebook is more like a house of mirrors than a simple reflection of a person. Taking a deeper step into the house of mirrors, we can explore the range of relationships and accounts produced in Facebook.

**Constituting Accountability Relationships in Facebook**

Facebook is a private sector company that derives revenue through advertisements that it hosts on its system. In 2009, Facebook had the third-highest advertisement impressions of any media property in the United States (comScore 2010), and after losing money for years, media reports say it now turns a profit and will have over $1 billion in revenue in 2010 (Eldon 2010). Facebook, which defines itself as "giving people the power to share and make the world more open and connected," began as a social networking site for college students. It was started by Harvard students in 2004 from the directory of new freshmen with names, hometowns, and small black and white photos. Its roots are thus within the American college social setting. In 2006, Facebook opened up registration to

everyone, and its membership is now predominantly non-students (comScore 2010). As of this writing in 2010, Facebook reports more than 400 million active users with 70 percent of Facebook users being outside the United States. Thus the profile of Facebook users has evolved beyond the original college population to one that is older, more diverse, and more international. Facebook provides the following current statistics: more than 35 million users update their status everyday; the average user spends more than 55 minutes each day on Facebook; more than 3 billion photos are updated to the site each month; more than 5 billion pieces of content (web links, news stories, blog posts, notes, photo albums, etc) are shared each week; the average user has 130 friends on the site; and the average user is a member of 13 groups (Facebook 2010).

As already suggested, in using the house of mirrors metaphor, we frame Facebook as an accountability system. The accountability frame may seem unusual since most think of Facebook as a social networking site which frames it as a system for creating, maintaining and managing personal relationships, not a system in which they are 'held to' account. Facebook can, indeed, be thought of as social infrastructure or infrastructure for sociality. Nevertheless, it is a system of accountability in the sense that individuals create, display, and convey accounts of themselves and others (friends, advertisers, other watchers) use those accounts to form opinions and make decisions about those whom they watch. In some sense, this is a way of saying that social relationships inherently involve accountability and Facebook constitutes relationships and accountability in distinctive ways. The architecture, policies, and business model of Facebook shape the kinds of relationships that are established, maintained, transformed, broken, etc. We should add here that Facebook has itself been shaped by its users.

Framing Facebook as a system or systems of accountability directs us to see that at least seven types of accounts and accountability relationships are constituted in Facebook. *First*, individuals make an account of themselves for themselves. On their own profile, users post a wide range of personal information (education, work, favorite quotations, etc.), as well as updated comments, photos, and links of interest. The user makes a presentation of self, perhaps testing their social picture, trying on a certain appearance—and watching themselves to see if it fits. In this account, the watched produces the account and the watcher and the watched are one and the same. The individual user is responsible to the self and the norms are internal to that individual.

A *second* account, and the one most often associated with Facebook and other social networking sites, is the account that individuals create for their "friends" and the continual and dynamic interactions among the individual and those friends. In this account, the individual crafts a set of images that are available to a group of "friends," a display of one's self to one's social network (boyd 2007). Users first choose friends (often selected from pre-existing networks, like one's high school or college class) to whom they will be accountable. Facebook then provides various fora through which to communicate with "friends." Friends, in turn, can engage with a person in several modalities. They can post on one's "Wall," a public space in a profile that anyone can see. They can send private messages, much like email within Facebook. They can comment on any content the friend posts (or just click to say they "like" it). Users see their friends' posts most easily through the "News Feed," which includes the recent activity of their friends such as comments, photos, and links they posted, friends they have made, etc. Users can petition their friends, through various applications to join a game, participate in the game (usually through accepting and then reciprocating some kind of gift/feature of the game), or just to express some opinion or taste. Further, friends

can anonymously view their friend's profile, or any profile that is open to them. These various postings are the means by which users watch and are watched and in the process become accountable to their friends. The norms that operate will depend largely on the number and heterogeneity of the friends one has. Facebook allows individuals to create something of a hierarchy, or concentric circles, of friends, although the effort required to distinguish these layers means that most users have an undifferentiated set of friends. The smaller and tighter the circle of friends, the more likely the norms will be similar and shared.[3] A larger and more diverse set of friends is likely to involve more diverse norms. Further, the operative norms can be emergent, shifting as the SNS and the network of friends develops. However accounts once created remain somewhat permanent as they are remembered and archived; thus elements of previous accounts are never truly forgotten (Johnson and Blanchette 2002).

A *third* account is the one that Facebook itself makes of its members; this is largely an administrative account that includes the terms of use, the default settings, the archiving of an individual's site, and the individual's reactions to the various (and changing) services that Facebook offers. The terms of service outline the contractual relationship between the company and users, and specify the rules and help to establish norms that moderate accountability between both parties. The company captures users' clickstreams in order to improve the site by making it more usable and more profitable for the company. Further, they monitor profiles for content they deem objectionable on the ground of keeping Facebook safe and protecting other people's rights. If they find such content, they might warn the user, remove the content or remove the user's profile entirely. Objectionable content includes material that violates their terms of service (such as hateful, threatening, pornographic, or that contains nudity or graphic or gratuitous violence). Further, it seems that Facebook relies largely on users to report objectionable content, rather than policing it directly. The norms for objectionable content are thus arguably unclear.

A *fourth* account is the one Facebook makes to a variety of advertisers. This account involves some aggregate market research and some limited information from a particular user's profile, as well that person's behavior in response to their advertisements. The formally stated Facebook policy, in bold, is that "We will not share your information with advertisers without your consent. We allow advertisers to select characteristics of users they want to show their advertisements to and we use the information we have collected to serve those advertisements" (Facebook 2010b). However, as one reads through the details of the privacy policy, it becomes clear that users need to "opt-out" of various features that share information with advertisers in order to ensure that the formal policy is indeed followed. These ads can draw on a variety of information about users, especially the personal data that the users themselves provide, and in at least some users' judgment are "off-key" or "creepy." According to a *New York Times* story on these ads, "Facebook does not have the employees to review each ad, but relies largely on member feedback to flag inappropriate messages" (Stone, 2010). In this case there is a three-way accountability relationship among Facebook, users and advertisers with mutual watching for purposes of both transparency and surveillance.

[3] It is important to note that users have at least nominal control over access to their accounts by establishing their privacy settings, which determine what parts of their accounts are open to whom. Their friends, in turn, establish privacy settings that determine what information they can see. In general, a user can make their page, or aspects of their page and their posts, available to only friends, to friends and friends of friends, to community or school-based networks (which are being phased out), or to everyone. However, there are some categories of information "such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to [that] are considered publicly available to everyone, including Facebook enhanced applications" (Facebok Privacy Notice). In other words, despite a user's privacy preferences, a variety of specific information *will be made public*.

The *fifth* account consists of the information that a user's Facebook applications collect about that user, whether it is personal information from the user's profile or merely the clickstream of the user's interaction with the application. These third-party applications are not owned or operated by Facebook but are only accessible through it (Weaver and Morrison, 2008). Applications can serve to display more information about a person (favorite music or movies, places they've been, etc.), but they also provide some means for interacting with others (from person-to-person games like scrabble, to larger-scale social games involving groups). If users agree to accept an application, often on the suggestion of a friend, the application gains access to all of a user's profile. Although the user receives notice that this will happen, it is likely that few people think about the ramifications of this. Users are also given information in the "Facebook Platform" section of the Privacy Policy to help them navigate these rather complicated arrangements—as well as the instruction that "If you find an application or website that violates our rules, you should report the violation to us on this help page and we will take action as necessary" (Facebook 2010b). Here again there is a three-way accountability relationship among users, Facebook and third-party applications; however, the relationship is removed from users and to a large extent removed from Facebook, allowing the third-party applications more surveillance capability and control over the account, and providing less transparency to users than is available to them with Facebook the company and advertisers.

The *sixth* type of account is the one available to a number of other entities that are at least tangentially part of Facebook and monitor the online behavior of Facebook members for their own particular purposes. Law enforcement officials, employers, and college administrators have taken advantage of Facebook's affordances to create accounts about its users. Law enforcement officials may also operate under cover, posing as friends to try to collect information on suspects (Lardner 2010). Employers use it to gather information about job applicants (Holt, 2006; DiBianca, 2006; Millard, 2007). College administrators see the system not only as a community-building technology (Hass, 2006), but also as a means to examine student profiles for evidence of underage drinking and other campus violations. In these accounts Facebook users are being held to the norms not of their friends or online social communities but to the norms of their offline roles and responsibilities.

A *seventh*, and final, type of account is made to non-members of Facebook so that users are potentially accountable to others outside Facebook. This public account picks up information from one's account that Facebook makes publicly available so that search engines, for example, can pick it up and re-deliver it as search results for specific names, including group memberships, and friend lists. In part this occurs because of the information in one's profile that Facebook requires to be publicly available and in part because they may, knowingly or inadvertently, set their privacy settings in such away that information is available to everyone. In one prominent case, a criminal was caught in Mexico when law enforcement officials accessed the public parts of his Facebook account (Lardner 2010). But Facebook's general position is that: "We share your information with third parties when we believe the sharing is permitted by you, reasonably necessary to offer our services, or when legally required to do so." The standard Facebook employs regarding when legally required is if "we have a good faith belief that the response if required by law." This standard and the "reasonably necessary" administrative standard are rather low thresholds.

Uncovering the number of accounts and the multiple relationships that are constituted in Facebook suggests in itself that thinking about Facebook as social networking site or even as a system for peer-to-peer transparency or peer-to-peer surveillance may be much too simplistic and even misleading. These labels hide the complexities and indirect (intentional and unintentional) processes by which accounts are configured and individuals rendered to their friends and others. Just what Facebook *is* is better understood by revealing what goes on behind the scenes.

**Reconfiguring Facebook's House of Mirrors**

We began with a concern about the tension between revelation of personal information and privacy. On the one hand, the house of mirrors analysis of Facebook suggests that the kind of surveillance that goes on in Facebook is much more complicated than many other forms of surveillance. On the other hand, because the analysis provides a model of how personal information is created, bounced, highlighted and shaded, and rendered, the analysis reveals points in the house of mirrors at which changes might be made to counter (limit or mitigate) surveillance. Keeping with the house of mirrors metaphor, we refer to these interventions as 'reconfigurations' of the house of mirrors. In other words, we do not call for elimination/destruction of houses of mirrors. Systems of accountability, especially those constituted in digital medium, will always be houses of mirrors. Our only hope of diminishing surveillance and protecting privacy is to reconfigure the mirrors so as to change the character of surveillance and minimize or mitigate its effects. So, what forms of intervention seem plausible given the house of mirrors analysis?

The stage of entry into a house of mirrors is the most powerful stage. The information a user enters when she sets up a Facebook site is what is bounced, highlighted and shaded, and rendered throughout the system. For this reason, the entry conditions are the most important for intervention. Here it is important to consider both the user and the Facebook architecture.

The user can exercise some control of what happens in the house of mirrors by controlling what information is posted. Of course, for the user to make informed decisions, the user has to understand how Facebook works. Educating users is, obviously important, and it would seem that Facebook users have, collectively, learned over time to be more careful about what they post. This no doubt will continue but arguing for informed consumers simply moves privacy intrusion into the maze of informed consumerism and technological literacy, an important but inadequate approach.

The Facebook architecture is a more powerful way to affect the entry stage in that the template prompts users to enter certain kinds of information. The Facebook template is a salient example of Lessig's famous statement that 'code is law' for the template encourages users to enter certain kinds of data and not to enter other kinds; the template encourages individuals to classify themselves in certain categories and disallows other categories. [Gender is a good example here; Facebook treats gender as important enough to be there but also treats it as binary.]

The Facebook template is determined by the company and several parts of that template could be modified and amended. For example, individuals could be given the option of having multiple Facebook accounts, for the multiple roles they play in their lives, thus allowing them to have more control over what information, photos, updates and

comments are available to which sets of "friends." Such segmentation by Facebook account would provide more technical and psychological control than would trying to segment one individual account in ways that represent one's various roles. From Facebook's management perspective and from the advertisers' perspective, this might be more cumbersome and, depending on how it is implemented, less lucrative in terms of information gathering for marketing; hence, there is likely to be resistance. Some users do set up aliases so it is difficult for unknown people to access them or to connect their Facebook activities to their offline identities (Raynes-Goldie 2010) but that is frowned upon by Facebook but seems to be inconsistently enforced.

The required and optional fields in the profile template could also be changed. One user commented: "Simply setting up your first page is a nightmare. There are no sound instructions on how to do anything. There is nothing on this site that is intuitive in any sense of the word" (Susan, commenting on Hiar 2011). Optional fields might be offered to subscribers not at the initial sign-in but later, making it clearer what is indeed required and what is optional. Date of birth, a rather unique identifier, is required to "encourage authenticity" and "provide only age-appropriate access to content;" one can "hide the information" from one's profile but that requires entering the labyrinth of Facebook's Privacy Policies.

To address the bouncing processes of Facebook, we have to consider Facebook's privacy policies. Bouncing is, of course, essential to social networking, i.e., users post information so others can see it. However, users not only want bouncing within their social network, they also want to control who sees what and to know how bouncing is occurring. Facebook's privacy policies have been the subject of enormous criticism and analysis—and can only be summarized here in terms of their relevance for adjusting the mirrors. It is important to point out that the general trend over Facebook's history has been to default settings that share more personal information with more parties and to more complicated privacy policies. On the first point, Matt McKeon (2010) has created an infographic that vividly illustrates the trend to more sharing. As he demonstrates, the default settings for the range of Facebook information (including: name, picture, demographics, extended profile data, friends, networks, wall posts, photos, and likes) have steadily been set to extend from the individual user in the center outward to concentric circles of friends, network, all Facebook users, and the entire Internet.

In 2005, the defaults for most categories of information were set primarily to friends with defaults for name, picture, demographics, friends and networks extending only to network. By 2010, the defaults for all but contact information and birthday were set to the entire Internet. The Electronic Frontier Foundation textually conveys what it terms "Facebook's eroding privacy policy" by extracting relevant passages from Facebook's privacy policies since 2005. In order to convey this erosion, a few relevant excerpts from EFF (Opsahl, 2010) appear below:

> 2005: "No personal information that you submit to Facebook will be available to any user of the Web Site who does not belong to at least one of the groups specified by you in your privacy settings."
>
> 2006: "Our default privacy settings limit the information displayed in your profile to your school, your specified local area, and other reasonable community limitations that we tell you about."

> Nov. 2009: "You decide how much information you feel comfortable sharing on Facebook and you control how it is distributed through your privacy settings…The default privacy setting for certain types of information you post on Facebook is set to 'everyone.' "
>
> Dec. 2009: "Certain categories of information such as your name, profile photo, list of friends and pages you are a fan of, gender, geographic region, and networks you belong to are considered publicly available to everyone, including Facebook-enhanced applications, and therefore do not have privacy settings. You can, however, limit the ability of others to find this information through search using your search privacy settings."

A May 2010 *New York Times* article, and accompanying graphic, points out that "To manage your privacy on Facebook, you will need to navigate through 50 settings with more than 170 options" (Gates, 2010). Additionally it notes that, in contrast to the erosion of privacy in these privacy notices, the length of the notices has blossomed with 2005 privacy notices of 1,004 words, 2006 notices of 2,313 words, 2007 notices of 3,067 words and 2010 notices of 5,830 words.

An equally significant problem with Facebook's privacy policies is that they change rather frequently, often in ways that engender opposition which Facebook initially responds to but then backslides to do what it originally proposed. The most recent example of this is its January 14, 2011 proposal to provide Facebook members' addressed and mobile phone numbers to third-party application developers. Due to instant criticism, it backed off from that proposal on January 17th but then resumed its plan in late February. During this time, public interest groups and Congressmen Markey (D-MA) and Barton (R-TX) raised questions and objections.

Typically Facebook members are not quiescent when the company appears to have altered the contract and initiates practices to which members object. The architecture of Facebook makes it relatively easy to organize such opposition. For example, in early September 2006, Facebook decided to add two new features, *News Feeds* and *Mini-Feed*, which tracked and published changes that users made to their pages, including notifying users when friends posted new photos. The user community protested, finding the new features to be "stalker-esque," "creepy," and denying the community control over the content. E.J.Westlake reported that some users felt monitored in a way that made them uncomfortable, other users worried about stalking, and others were annoyed at the amount of insignificant information they were receiving (2008, 22). Michael Calore (2006) commented that: "The outcry suggests the exhibitionism and voyeurism implied by participation in social networking sites has ill-defined but nonetheless real limits, and expectations of privacy have somehow survived the publishing free-for-all." Yet despite the outcry, Facebook kept the *News Feeds* feature, and it now operates as a central feature of the site. More recently in December 2009, Facebook changed its default privacy settings to make text, photo and video updates publicly visible to everyone rather than to friends only – again provoking online protests, as well as broader media criticism (Kirkpatrick 2010, Perez 2010). As of this writing, these protests have not led Facebook to change the policy. One protest that did have an effect, however, was the protest against the "Beacon" program, in which users' activities on other sites (partnered with Facebook) were transmitted into a users' news feed. In one infamous case, a user purchased a ring that was to be a surprise for his wife, only to have the surprise spoiled when she saw the purchase appear in his news feed. In September of 2009, Facebook

settled a class-action lawsuit that resulted from objections to the program (McCarthy 2009).

Most observers would agree with Marc Rotenberg of EPIC who, in congressional testimony, argued that Facebook's "privacy settings have not worked. They are too confusing, too elaborate, too inconsistent, and too difficult for users to make real decisions" (Rotenberg 2010). Stan Schroeder made a similar point on Mashable noting that the "detailed" settings give users "the ability to fine-tune the privacy aspects of almost every little" part of their account but that "for most users, this level of micromanagement makes Facebook's privacy settings a convoluted mess" (Schroeder 2011). There is increasing evidence that Facebook members do indeed care about protecting their privacy on Facebook; are concerned about embarrassment, stalking and identity theft; and are frustrated with not being able to protect their privacy (Gross and Acquisti 2005; boyd and Hargittai 2010; Regan and Steeves 2010). But, the history of Facebook's trajectory of privacy decisions indicates that there are significant limitations on effectively reconfiguring the mirrors through privacy notices—unless these notices are all set so that the default is not to share information and to require an opt-in for each instance of sharing. It would also need to be made clear what the implications of sharing would be.

In terms of shedding light on how the mirrors actually work, Facebook's "Preview My Profile" option lets a user see the profile as someone else would. This can thus operate as a "privacy lens" by which a user can see how the mirrors are working. This option could be refined, provided more often to a user (for example, when photos are uploaded or wall comments are posted), and made easier to use. The ability to see how information is bouncing and how information may have been highlighted or shaded by others is a powerful tool in the house of mirrors. Another tool is a "privacy scan" created independently of Facebook by ReclaimPrivacy.org, which gives users a "privacy report," of good, caution or insecure, showing exactly what their privacy setting are as they navigate their activities on Facebook (Henry, 2010). One problem with this outside privacy scan is that it relies on the scan being up-to-date in terms of Facebook's policies. Finally, users may also use an application to see who has accessed their account. This feature gives users information as to who has been in their house of mirrors, even if it doesn't convey what the users see, do, or how they interpret the images.

The question of interpretation brings us to the highlighting and shading that occur on Facebook. The facts that there are so many types (demographic, photos, opinions, relationships) of information, with such fine-grained detail, and retained over such a long time period combine to provide powerful components for highlighting and shading—and for composing narratives that are divorced from reality in fundamental ways. There are two techniques available to reconfigure the mirrors in ways to limit highlighting and shading. The first is to tie component pieces of information together so that it is technically harder for others to extract from the original file (be it a photo or text) and merge it with something else or isolate it from the whole. This would serve to retain its "contextual integrity" (Nissenbaum 2010). The second would be to set "data death" features so that information could not be retained indefinitely by either Facebook or by users who might download information. Limitations on the life of images and information can be effective in controlling highlighting and shading.

The final rendering brings us back to the various relationships on Facebook, each of which is interested in a particular type of account of the individual. Controlling bouncing

and highlighting and shading will serve as well to control the final renderings that are possible. Additionally, the Facebook architecture could reveal the types of actors that exist on Facebook, e.g. individual, business, school, non-profit, government, etc. This would enable other users to "see" who was looking at them and what type of account that entity might be interested in rendering.

Given the complexity of Facebook's architecture and business model, our analysis of how the house of mirrors might be reconfigured also reveals how limited the impact of such reconfigurations is likely to be. The scale and reach of Facebook's operations and huge number of people on Facebook also points to the need, and justification, for regulatory action. Facebook has over 500 million users, is a global operation, and sits at the center of an online web of third-party applications, business partners and advertisers. Its scale is perhaps best captured in a statement that Marc Rotenberg made in congressional testimony in 2010: "If Facebook were a country, it would be larger than the United States, Germany and Japan combined." The Federal Trade Commission, congressional committees, and international privacy officials have all tried to determine exactly how Facebook is processing personal information and with what impacts, and require Facebook to comply with more privacy-friendly policies—with no effective result.

We thus need to consider whether Facebook has reached the level of a critical infrastructure, indispensable to current social, political, economic, and cultural life. If Facebook is playing a fundamental and dominant role in modern life, then has it become comparable to a public utility? Does it have monopoly power over key social and economic operations? In other words, is Facebook the Ma Bell of the 21st century—and should it be regulated as such? If Facebook is being used for every purpose imaginable, then has Facebook become public space and should it be regulated in accordance with public trustee principles? If the answers to these questions are in the affirmative, then some regulatory scheme—that goes well beyond the privacy tinkerings that have been proposed to date—are in order.

## Conclusion

Using the house of mirrors metaphor, we have identified four processes that, taken together, describe what happens to the image or representation of a person in Facebook. Although the system is appropriately described as a social networking system and as a system of peer-to-peer transparency and peer-to-peer surveillance (Albrechtslund 2008, Andrejevic 2005), none of these labels adequately capture the processes by which individual identities are constituted and rendered. Yet threats to privacy are insidious in those processes. When Facebook users enter Facebook, they enter into relationships with friends and a variety of others (who they may or may not be aware of). The relationships they enter into are based on accounts of the user, accounts that are constantly change. How the user is rendered in these accounts is effected by a complex combination of Facebook's architecture, Facebook's policies, Facebook's business model, the particular information that the user inputs, the reactions of those who view the information, and more. Privacy protection must address all of the components. We have argued that entry is the most powerful stage of engagement with Facebook because once information is entered it bounces, gets highlight and shaded and rendered for a variety of purposes.

Not surprisingly, our house of mirrors analysis has not uncovered a magic bullet. We have reviewed a variety of strategies that would, in the metaphor, reconfigure the mirrors.

These include changing what users put in by choice, changing the architecture of Facebook, changing Facebook's privacy policies, and finally slicing through the Gordian knot, by transforming Facebook into a public utility. Yet another possibility is the one implicit in our account and that is to reconceptualize Facebook as a house of mirrors. This has the advantage, at least, of signaling to users that there is a lot more going on than social networking.

**References**

Albrechtslund, Anders. 2008. "Online Social Networking as Participatory Surveillance," First Monday, vol. 13, no. 3 (3 March). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2142/1949

Andrejevic, Mark. 2005. "The work of watching one another: Lateral surveillance, risk, and governance," *Surveillance & Society*, volume 2, number 4, pp. 479–497. Available at: http://www.surveillance-and-society.org/articles2(4)/lateral.pdf

boyd, danah. 2007. "Why Youth (Heart) Social Network Sites: The Role of Networked Publics
in Teenage Social Life." *MacArthur Foundation Series on Digital Learning – Youth, Identity, and Digital Media Volume* (ed. David Buckingham). Cambridge, MA: MIT Press.

boyd, danah and Eszter Hargittai. 2010. "Facebook Privacy Settings: Who Cares?" *First Monday*, vol. 15, number 8 (Aug.2). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/3086

Calore, Michael 2006. "Privacy Fears Shock Facebook," *Wired News* (Sept. 6). Available at: http://www.wired.com/news/culture/1,71739-0.html

comScore. 2010. "The 2009 U.S. Digital Year in Review: A Recap of the Year in Digital Marketing." Available at: http://www.comscore.com/Press_Events/Presentations_Whitepapers/2010/The_2009_U.S._Digital_Year_in_Review/%28language%29/eng-US. Accessed March 10, 2010.

DiBianca, Margaret. 2006. "MySpace and Facebook in your face: social networking sites as recruiting tools." *Delaware Employment Law Letter*, December.

Eldon, Eric. 2010. "Facebook Revenues Up to $700 Million in 2009, On Track Towards $1.1 Billion in 2010." *Inside Facebook*. Weblog post on March 2. Accessed March 10, 2010. Available at: http://www.insidefacebook.com/2010/03/02/facebook-made-up-to-700-million-in-2009-on-track-towards-1-1-billion-in-2010/

Facebook, Inc. 2010. "Press Room: Current Statistics" Accessed March 18. Available at: http://www.facebook.com/press/info.php?statistics.

Facebook, Inc. 2010b. "Privacy Policy." Accessed March 18. Available at: http://www.facebook.com/policy.php

Gates, Guilbert. 2010. "Facebook Privacy: A Bewildering Tangle of Options," *The New York Times* (Business Day, May 12). Available at: http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html

Gross, Ralph and Alessandro Acquisti. 2005. "Information Revelation and Privacy in Online Social Networks," (pp.71-80) *Proceedings of the 2005 ACM Workshop on Privacy in the Electronic Society.* New York: Association of Computing Machinery.

Hass, Nancy. 2006. "In Your Facebook.com," *The New York Times* (Jan.8). Available online at: http://nytimes.com/2006/01/08/education/edlife/facebooks.html

Henry, Alan. 2010. "ReclaimPrivacy.org Helps Solve Facebook Privacy Problems," PC Magazine (May 18). Available at: http://www.pcmag.com/article2/0,2817,2363922,00.asp

Hiar, Corbin. 2011. "Timeline: Facebook's Stormy Relationship with Privacy," *Media Shift* (February 8, 2011). Available at: http://www.pbs.org/mediashift/2011/02/timeline-facebooks-stormy-relationship-with-privacy039.html

Holt, Thomas F. 2006. "Find the Right Fit: The Latest Tool for Employers" Metropolitan Corporate Counsel, November.

Johnson, Deborah and Jean-Francois Blanchette. 2002. "Data retention and the panoptic society: The social benefits of forgetfulness". *The Information Society* 18 (2002): 1-13
Kirkpatrick, Marshouse. 2010. Why Facebook is wrong: Privacy is Still Important. Read Write Web. Available at: http://www.readwriteweb.com/archives/why_facebook_is_wrong_about_privacy.php

Lardner, Richard. 2010. "When Tweets Can Make You a Jailbird." Associated Press Article. March 16. Available at: http://www.nytimes.com/aponline/2010/03/16/us/politics/AP-US-Feds-on-Facebook.html?_r=1&scp=5&sq=facebook%20mexico%20law%20enforcement&st=cse

McCarthy, Caroline. 2009. "Facebook Beacon Has Poked its Last" *The Social* (Sept. 18). Available at: http://news.cnet.com/the-social/?keyword=Beacon

McKeon, Matt. 2010. "The Evolution of Privacy on Facebook." Available at: http://www.mattmckeon.com/facebook-privacy/

Millard, Elizabeth. 2007. "Online background checks: as social networking sites grow, so does the ability of employers to discriminate" American Bar Association, January.

Nissenbaum, Helen. 2010. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press.

Opsahl, Kurt. 2010. "Facebook's Eroding Privacy Policy: A Timeline," *Business Insider* (April 30). Available at: http://www.businessinsider.com/facebooks-eroding-privacy-policy-a-timeline-2010-4

Perez, Sarah. 2010. The 3 Facebook Settings Every User Should Check Now. New York Times. January 20. Available at: http://www.readwriteweb.com/archives/the_3_facebook_settings_every_user_should_check_now.php

Raynes-Goldie, Kate. 2010. "Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook," First Monday, vol. 15, no. 1 (4 January). Available at: http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2775/2432

Regan, Priscilla and Valerie Steeves. 2010. Kids R Us: Online Social Networking and the Potential for Empowerment. *Surveillance & Society* 8(2): 151-165. Available at: http://www.surveillance-and-society.org/ojs/index.php/journal/issue/view/Empowerment

Rotenberg, Marc. 2010. "Testimony for Hearing on Online Privacy, Social Networking, and Crime Victimization" before the Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary (July 28). Available at: http://epic.org/privacy/socialnet/EPIC_Testimony_House_Jud_7_10.pdf

Schroeder, Stan. 2011. "Facebook Privacy: 10 Settings Every User Needs to Know." Available at: http://mashable.com/2011/02/07/facebook-privacy-guide/

Stone, Brad. 2010. "Ads Posted on Facebook Strike Some as Off-Key." *New York Times*. March 3. Available at: http://www.nytimes.com/2010/03/04/technology/04facebook.html?hp&pagewanted=all&pagewanted=all&pagewanted=all

Weaver, Alfred C. and Benjamin B. Morrison. 2008. "Social Networking," *Computer* (February), pp. 97-100.

Westlake, E.J. 2008. Friend Me if You Facebook: Generation Y and Performative Surveillance. TDR: The Drama Review, Vol. 52, No. 4, 21-40.