

# **Social Reading and Privacy Norms: The Aesthetic of Simplicity, Online Reading, and Interface Confusion**

by

Dr. J. Richard Stevens  
Assistant Professor of Journalism  
The University of Colorado at Boulder  
1511 University Ave., 478 UCB  
Boulder, CO 80309  
303-492-0817  
rick.stevens@colorado.edu

A Research Paper Submitted for the  
International Symposium on Online Journalism, 2012

## **Abstract:**

Every year more legal codes and policy initiatives concerned with the regulation of consumer privacy are created throughout the world, yet the amount of personal information collected and stored continues to increase. Much of this data comes directly from individuals through small “trivial and incremental” interactions that “minimize its ultimate effect” (Cohen 2000, 1397).

Privacy attitudes are neither static nor inflexible. When individuals perceive that the potential benefits for information transactions outweigh potential risks, they voluntarily adjust their privacy decision-making to meet the demands of changing social contexts (Friedman, 1997; Murphy, 1964). Architecture itself creates social context and influences human behavior (Tuan, 1977).

The current work examines the effect of certain aesthetics (in particular, simplicity) in “architectures of vulnerability” that lead individuals to provide personal information in exchange for security, comfort, a sense of belonging and the ability to perform surveillance. Through the communication of communal aesthetics, online storefronts, social networking sites and other online venues create an image of a contextual paradigm that does not conform to the behaviors of the underlying digital architecture. The introduction of Facebook’s open graph platform, and news media outlets’ release of social reader applications provide yet another architecture of vulnerability, one masked by the interface on the installation screen. In this manner, interface design is used to create false social contexts and illusions of voluntariness that cause individuals to disclose more personal information than they normally would.

**Social Reading and Privacy Norms:  
The Aesthetic of Simplicity, Online Reading, and Interface Confusion**

The print journalism industry continues to contract, with some print newspapers discontinuing publication, some adopting new publication strategies, and some moving to online-only publication (Grabowicz 2012). At the same time, online social networking has increased in volume and popularity in recent years, as millions of people continue to turn to technology to mediate relational information. These two trends appear to be converging, as some news enterprises are contracting with social networking platforms to put news content into social networking space.

As a consequence of these activities, the large amounts of personal information stored by social networking platforms are being leveraged across multiple sites and services, often in ways users do not understand. Although the aggregation and consolidation of personal data presents a variety of risks to users, the privacy protection tools embedded in social networking platforms (such as Facebook) are often by default set to weak protection settings to facilitate easy connections (Gross and Acquisti 2005).

But even when comprehensive privacy enhancing technologies (PETs) and filters are available, users often do not implement available tools. Part of this reticence appears to come from inherent trust in the online community (boyd 2004; Gross and Acquisti 2006). But little research exists that examines the role interface plays in establishing privacy expectations. This paper examines the aesthetic of simplicity in social reader interfaces (specifically, the open graph application offered by Facebook), the affordances communicated by it, and its potential effect on the negotiation of user privacy choices.

### Privacy's Context

Privacy attitudes are neither static nor inflexible. When people see that the potential benefits for an information transaction outweigh the potential risks, they often voluntarily adjust their privacy comfort levels (Friedman, 1997; Murphy, 1964). Stutzman (2006) surveyed 200 university students and found that while students tend to view protecting their identity information online as important and cite concerns about the consequences of sharing information, they do not feel their online identity is well-protected nor do they plan to curb their future disclosure activities. In order to grasp how privacy norms are manipulated in online environments, it will be necessary to examine what role contextual clues play in the information disclosure decisions of Internet users.

McMillan and Morrison (2006) used qualitative analysis to show college students' increasing reliance on Internet technology in each of four primary domains (self, family, real communities and virtual communities). But the relationships maintained in each of these domains can be fundamentally different, and the information disclosure decisions were found to be inconsistent between domains. The context of one's interactions appears to be rather important to how one manages personal information.

Rosen (2000) described privacy in terms of context, as decisions concerning information disclosure depend heavily on the circumstances, audience and perceived implications of the potential disclosure. Palen and Dourish (2003) argue that privacy in online contexts is a negotiated process conditioned by the expectations and experiences of the disclosing users.

Dey, Abowd and Salber (2001) defined context as

... any information that can be used to characterize the situation of entities (i.e., whether a person, place, or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves. Context is typically the location, identity, and state of the people, groups, and computational and physical objects” (106).

Grudin (2001) presented an example of how changes in the context of information dissemination through aggregation of a search engine for a newsgroup called *Deja News* altered the experience for newsgroup readers. By allowing archives of previous contributions and conversations to become searchable, the access to past interactions created new contexts of understanding, often contributing contextual facts that were undesired. As one respondent explained, “we were discovering things about our colleagues that we didn’t want to know” (281).

Privacy decisions are largely informed by expectations, expectations that rely on context. From the genesis of the legal construct of privacy in American culture, privacy advocates have tried to control the circumstances under which certain facts about themselves could be disclosed. Technology has always played a key role in social deliberations over the boundaries of privacy. The next section will briefly review the origins and developments of American privacy in order to frame issues related to the current topic.

### Considering the Technological Roots of American Privacy

Prior to 1890, no formal privacy code existed in the American legal system. But the political stagnation that had followed the Civil War (Cherny 1997) began to yield to a new age of commerce, technological innovation and industrialization. Into this environment, one major technological innovation (flash photography) led directly to the

establishment of a privacy protection for upper class members. The introduction of flash powder to the photography process cut the exposure time, and photographs could be taken in less than a single second. As a result, “snap shots” let a photographer take photographs without the permission (or even the knowledge) of the subject.

Following an event of scandalous reportage, two young lawyers from Boston decided to challenge the photographers’ newly acquired abilities with the law. The first law governing American privacy appeared in an 1890 *Harvard Law Review* article written by Samuel D. Warren and Louis D. Brandeis titled, “The Right to Privacy.” Warren and Brandeis did not attempt to establish a right of privacy from either a constitutional justification or an argument of privacy’s intrinsic value to all societies. Rather, the argument presented posited that as American society had evolved, a “certain level of sophistication” in society has made it increasingly difficult for a person to retreat from external scrutiny:

Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual, what Judge Cooley calls the right ‘to be left alone.’ Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that “what is whispered in the closet shall be proclaimed from the housetops (Warren and Brandeis 1890, 195).

This argument frame led to their definition of the right to privacy simply as the “right to be left alone,” a reference to Judge Thomas Cooley’s statement concerning “personal immunity” (1888, 29) two years earlier. While elegant, this phrase was of little help in the legal arena, as determining to what extent someone should be left alone has varied almost as often as the circumstances under which the right is challenged by a competing right of access.

The authors argued that a right of privacy is due a person out of respect for his or her standing, and claimed that the unauthorized disclosure of private facts (the only form of violation mentioned in their article) can corrupt a society by encouraging the nation to divert its attention away from important political and economic issues. The article also claimed that each person possesses an “inviolable personality,” an abstract collection of images, texts and facts that when assembled, form a person’s identity. This view allowed the authors to argue that this “inviolable personality” should be controlled by the possessor, because the “common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others”(198). In effect, the argument applies the precedent of copyright law to make a person the owner of his or her image, with the implied control and disposal rights granted private property. Eventually, this link between privacy and copyright law also implied that a citizen had the right to sell his or her image as a commodity. “Inviolable personality” is an abstract self: made up of images, texts and facts, the collection of which can be sold as a commodity. Thus, the abstract self soon became a commodity in its own right.

Though privacy law has evolved and been adapted to safeguard other areas of personal control, inherent in most access-based privacy arguments is the foundational argument that people have a right to preserve their reputation and that the public disclosure of private facts is the root concern of privacy law. Controversies over privacy norms and expectations almost always occur when new technologies change the context or access to previously accepted information collections. For many privacy scholars, this connection ties privacy disputes to concerns about information management. For

example, Gandy (1993) persuasively argued that access to one's data allows individuals to be categorized by others in ways with which few would be comfortable. Because these categories predict market behavior, consumer information has become a commodity in the information economy.

In the networked age, information is routinely collected through a variety of information sources for modification and analysis (Castells 1996, 32). Modern Americans leave data trails with almost every interaction in which we engage: privacy may not be possible in a world in which credit cards, cell phones, biometric cameras and even toll roads are all used to track the movements of individuals (Bennet, Raab and Regan 2003).

It is increasingly difficult for users to know what information is being collected, what it is being connected to, and who has access to it. When one considers the number of privacy disclosure agreements users sign in a given year (just a few common examples: medical disclosure forms, mortgage agreements, software agreements, credit card agreements, online bank access agreements, loans, cable and television service, etc.), it quickly becomes apparent that little about a person's behavior is not known by someone.

Americans are not wholly ignorant of these issues, but seem ill equipped or unwilling to act in meaningful ways to protect their data. For example, a study conducted by Jupiter Research (2002) revealed that while 70 percent of U.S. consumers worry that their privacy is at risk, they report doing little to protect their data. Of particular interest, the study found that only 40 percent of those polled even read privacy statements before handing over personal information to websites (and only 30 percent of online consumers find website privacy statements easy to understand).

Leathern (2002) argued that consumers should learn how to manage their data in ways that allow them to capitalize on its exchange and get value from its use. “Data” is defined as the plural form of “datum,” which means “something given.” Data is a commodity in the information economy, and yet it appears many users give away their data for little economic return.

### Interface as Social Control

Interface design can serve as a form of social control. Wood (1974) defines social control as the “the use of power with the intention of influencing the behavior of others” (53). Berndt (1962) argued social control covers “all the processes and procedures which regulate behavior, in that they exert pressure on persons and groups to conform to the norms” (11). When describing media exposure, Mathiesen (1997) described social control as exerted by “disciplining our consciousness” (216).

In physical space, architecture creates psychological and social effects (Tuan 1977) including altering individual conduct (Katyal 2002). In the classical example of contextually driven attitudes, a sense of crowdedness can depend on intentionality and environment, such as whether one is at a rock concert or ballroom dancing (Tuan 1977, 61). Architecture alters intentions by connecting schema with opportunities for action, though not always consciously. Benjamin (1935) explained that architecture is experienced habitually and in a state of distraction, but nonetheless perceived.

Digital architecture affects online behavior in similar ways. Mok (1996, 46) explained that “[i]nformation design makes information understandable by giving it a context. Information design builds new relationships between thoughts and places” (46).

In order to use online networks, almost every user must participate in the consensual hallucination: users believe they “visit” sites when in fact they are having online content delivered to their computer. The contextual frame of online media usage is not the setting of one’s computer, but rather the setting on the screen. Humans interface with the people and institutions of the world through the mental schema they develop. We constantly filter stimuli (tuning out noise, for example) by directing attention towards specific elements. Too much sensory input can cause stress and inhibit functionality (Brown and Wiser 1997), a core assumption of usability analysis. To some degree, all individuals interpret the world through mental representation. Gibson (1979) described this phenomenon as the reading of affordances, the practice of interpreting the world as an offering of possible actions, communicated through structural design. According to Gibson, one’s perception is influenced by environment, embodiment and perceived possible action.

Taking these perspectives into consideration, it becomes apparent that changes in context may not explicitly control actions so much as shape schema by directing attention towards particular features or visual cues. Contextual cues often cause cognition to be directed in a particular way, which can either encourage or discourage certain patterns of behavior. Users are not often aware of the differences between interface design and back-end architecture. As Raskin (2000, 5) explained, “As far as the customer is concerned, the interface is the product.”

In his treatise on the aggregation of personal data through online interactions, Solove (2004, 99) explained that current practices create “architectures of vulnerability,” insecure structures that create opportunities for significant harm. Such architectures

encourage individuals to expose themselves to those who have greater access to online structures and thus more power. Currently, most of the collection of personal data occurs out of the user's view. Most users do not appear to know when their information is gathered, where it is stored or how it is used. Furthermore, most companies that gather information are often not accountable to consumers.

But Solove's architectures of vulnerabilities are filled with personal data by willing participants, who do not seem to understand the significance their actions take when interacting with digital object. This confusion may or may not be intentional, but is certainly created by the differences between what the interface communicates and what tasks the back-end architecture actually performs.

#### Interface Design, Aesthetics and Usability

Interface is defined by Steven Johnson (1997) as "software that shapes the interaction between user and computer." The interface serves as a translator and interpreter, mediating between the two parties "making one sensible to the other" (14). Manuel Castells (1996) describes the back-end of systems architecture as "unseen logic of the meta-network, where value is produced, cultural codes are created and power is decided" (508).

Human-computer interaction (HCI) is the area of study concerned with computer users' mental processes and behaviors as they interact with computers. Researchers in the area of HCI have historically focused on the utility of interactions in terms of usage effectiveness or efficiency. Recognizing the limitations of these approaches, some

scholars have begun to explore more holistic experiential measures (Hassenzahl and Tractinsky 2006).

Much of the traditional HCI research on website and computer interfaces analyzes usability. The International Organization for Standardization (2010) defines usability as “[t]he extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency, and satisfaction in a specified context of use.” Usability guru Jakob Nielsen (1999) defined usability as consisting of five attributes: learnability, efficiency, memorability, errors and satisfaction, and presents simplicity as a key factor behind a usable design. In this context, simplicity is defined as the lack of obstruction, or lack of complexity.

However, usability measures imply intentional uses and attitudes towards use, rendering the technology exclusively as functional object. Instead of seeing technological objects as instruments for specific goal-oriented use, researchers should struggle to give them “meaningful presence” (Hallnäs and Redström 2002, 198). Usability presumes that the goals of the user and the information object align, that the object’s use merely serves to facilitate the goals of the user. But what if the goals embedded in the design of the object diverge with those of the user? Researchers do not often appear to consider that some interfaces might intentionally designed to be, in certain respects, unusable.

As one scholar explained,

What is needed [in technology design] is not the modern praise of new technology, but a critical and creative aesthetic-technical production orientation that unites modern information and communication technology with design, art, culture and society, and at the same time places the development of the new mediating technologies in their real every day context of changes in lifestyle, work and leisure” (Ehn 1998, 154).

Social networking (and thus activities that occur within its platform, like social reading) would appear to be an area in which goals between users and digital objects are at odds. Because digital objects treat all relationships as equal relationships, actions performed outside of a user's view might be deemed inappropriate for one type of relationship even if it were appropriate in another. This tension, allowing technology to manage relationships, represents a core paradox at the heart of the function social networking in regards to privacy negotiation. Though social networking generally represents the unprecedented potential for diverse global contacts, most people continue strive to maintain local, strong ties connecting to members of the user's work and physical environment (Putnam 2000). But the social networking connection to those strong ties is mediated by the social networking platform, a mediation that shapes social practices (Bakardjieva 2005). These mediated connections are influenced by design affordances, the "functional and relational aspects which frame, while not determining, the possibilities for agentic action in relation to an object" (Hutchby 2001, 44).

For example, in an early study on the online behavior of teenagers, Livingstone (2008) found that social networking sites' affordances created a false sense of intimacy between users that challenged the distinctions between public and private spaces for media production and display. In that work, Livingstone related the seeming confusion concerning intimacy in a public space to a lack of teens' online literacy exacerbated by the affordances of the social networking platform.

For nondeterministic types of interactions, HCI scholars have recently begun to employ measurements of aesthetics in an attempt to move away from the functionalism of traditional HCI and towards a more integrative and critical perspective on how

technology affects users and user behavior. Classic aesthetics literature has long attempted to identify and evaluate the attributes of beautiful objects. Relevant attributes include contrast and clarity (Gombrich 1995, Solso 2003), taken from classic considerations of the competing attributes of simplicity and complexity (Birkhoff 1933; Eysenck 1941).

Noam Tractinsky (1997) demonstrated a correlation between users' perception of the aesthetic appreciation of automatic teller machines (ATM) and usability. Building upon this work, Tractinsky et al. (2000) demonstrated a consistent relationship between perceptions of visual aesthetics and perceived usability, inspiring a series of studies examining the relationship between visual aesthetics and perceptions of usability (Ben-Bassat et al. 2006; Hartmann et al. 2007; Hassenzahl 2004; Sutcliffe and de Angeli 2005; Thüring and Mahlke 2007). General findings suggest that positive visual aesthetics in design interfaces can improve user performance (Moshagen et al. 2009; Sonderegger and Sauer 2010).

A variety of other perception changes have been shown to result from visual aesthetics, most relevant to the current work, credibility (Fogg et al. 2003) and trustworthiness (Cyr et al. 2008; Karvonen 2000; Kim and Moon 1998). Karvonen (2000) found that the aesthetical appeal of simplicity increases perceptions of trust. For experienced users, webpage design “acts as a sign of technical refinement that lies underneath the visual layout, on the level of the infrastructure of the system behind the user interface” (3).

Legacy news media organizations have, until recently, shied away from social networking protocols (or at least, the kinds of social networking protocols that involve

automated interactions among users). However, the recent adoption of news media social reader applications draws journalists and media companies more fully into social networking protocols, complete with the tensions created by differences in what is communicated through interface when compared to the computing functions occurring outside the view of the user.

### Considering Open Graph and Social Readers

Open graph, or “frictionless sharing,” is a platform introduced at Facebook’s f8 event on September 22, 2011. Open graph is a protocol that allows media producers to embed content into social networking structures for the purpose of integrating it into social media platforms. Combined with the Facebook Connect API, the seams between Facebook and media site content began to blur, and the personal information contained in Facebook’s account profiles and the media usage statistics began to be freely exchanged between sites.

The connections result in media content increasingly accessible from within Facebook, and Facebook account services available on external sites. Some media companies, hoping to capitalize on the push features of Facebook sharing, entered into agreements with Facebook in 2011 to leverage the Social Reader app to integrate the functions and user experiences between Facebook and their news content sites.

Due to the viral nature of open graph’s function, the first few months following the Social Reader’s introduction, the participating media companies saw an increase in traffic. By November 28, nine weeks after open graph was publicly announced, 10 million users had signed up for the Yahoo Social Reader, four million users had

subscribed to the *Guardian's* social reader and 3.5 million users had registered with the Washington Post Social Reader (Sonderman 2011). Currently, only 9 percent of American adults report getting their news from Facebook (Mitchell, Rosenstiel and Christian 2012), but that number is expected to grow in the coming years.

Not all print journalism outlets poised to take advantage of open graph chose to do so. Former *Times* developer Michael Donohoe (2011) explained privacy concerns were at the heart of the *New York Times's* decision not to release a social reader version of its content.

Controversies concerning the disclosure of personal information are hardly new for Facebook. A series of controversies involving the use of member data have demonstrated to users the potential for abuse when disclosing personal data online. These controversies, while stressful for many involved, actually shed light on the abilities of many firms dealing in personal information who choose not to disclose their privacy practices.

In September 2006, *Facebook* members suddenly found their social network filtered through an aggregating tool that reported the latest actions of members to a member's personal network. Within hours, tens of thousands of users voiced their anger over the changes (Calore 2006), claiming that the aggregation of information was invasive. *Facebook* responded by posting a blog entry by founder Mark Zuckerberg, explaining that none of the information portrayed in the feeds was unavailable before the aggregation. "Nothing you do is being broadcast; rather, it is being shared with people who care about what you do – your friends" (Zuckerberg 2006).

A survey of 180 undergraduate students conducted by the author soon after the controversy erupted reported that while more than 90% of respondents considered online data management to be important and more than 2/3 did not agree that *Facebook* protected their personal data, only one student reported actually leaving *Facebook* because of privacy concerns, and even that one reported logging in via a friend's account to keep up with the content of her friends' pages (Stevens 2007).

Another controversy occurred in November 2007, when *Facebook* launched Beacon, an aggregating advertisement utility that published users' activities on partner websites like *eBay*, *Fandango*, *Travelocity*, *Overstock* and *Blockbuster* (Story 2007). To protest, more than 50,000 *Facebook* users signed an online protest organized by *MoveOn.org* (Story and Stone 2007).

In February of 2008 another controversy erupted when many users discovered that should they ever decide to delete their *Facebook* account, their information would continue to be a permanent part of the network (Aspan 2008). An analysis of the site's policy agreement suggested that its use of data was legal in the U.S., though it would not be in the European Union (Ramasastry 2008).

In each of these controversies, users expressed surprise and outrage at the changes in delivery format their data underwent to be distributed to other users. Though the users had personally supplied the data, the general lack of understanding of underlying database structures displayed by the more vocal critics indicated many users do not understand the implications of the distribution of data across networked environments.

What makes *Facebook* unusual compared to the millions of online venues that collect personal data is not its information collection techniques. Presumably, most sites

that collect data are equally capable of combining together information strings and the contextual threads. *Facebook* becomes controversial for the transparency with which it operates. By allowing users to see their data reconfigured and redistributed into multiple contexts, the site causes distress by demonstrating information aggregation techniques that have been enacted behind a veil of technological secrecy for years.

*Facebook* appears to offer one set of expectations (drawn from the interface aesthetic, organized around the simplicity affordance) for its users, while the output of the collected data demonstrates a radically different relationship between the user and the architecture. In most data transactions, users are not privy to the output of their data collection, nor do they expect the simple interactions they engage in to create such processes.

### Privacy Presentation Through Interface Design

Because simplicity aesthetics are utilized within most sites that collect personal information, most users have little or no awareness about how their data is treated within online databases. Because the interface is designed to reduce the orientation tendencies that distract users from content, the access provided between software and personal information is rarely explained in explicit terms.

Privacy decisions depend heavily upon perceived context, and yet it appears that many users do not possess a sense of digital literacy necessary to make informed decisions regarding their personal data. The interface that facilitates one's ability to easily use digital technology prevents observation of the underlying technology:

Put simply, the importance of interface design revolves around this apparent paradox: we live in a society that is increasingly shaped by events in cyberspace,

and yet cyberspace remains, for all practical purposes, invisible, outside our perceptual grasp. Our only access to this parallel universe of zeros and ones runs through the conduit of the computer interface, which means that the most dynamic and innovative region of the modern world reveals itself through the anonymous middlemen of interface design (Johnson 1997, 19).

Framing the context of interaction as a sense of place instead of a tool set is critical to understanding online interactions. Dourish (2001) explained that where users are located (or perceive they are located) determines what behavior or decisions are considered appropriate, rather than the abilities of a tool. One example he presented was the different behavior users engage when using a cell phone, depending on the setting of its use.

Online aesthetics also create a sense of environment: how a user drafts an email to a bank representative will likely be different than the text comprising a message to friends. Dourish (2001) utilized Suchman's (1987) use of ethnomethodology (Garfinkel 1967) to bring a sociological understanding of interaction, ultimately arguing that "interaction is intimately connected with the settings in which it occurs" (19).

Dourish encapsulated this view in his term "embodiment," which recognized that:

[t]he technical infrastructures that deliver information into our homes and work environments create barriers that separate one stream of information from another and make coordination difficult. Humans respect barriers, too, but they are barriers of different sorts; boundaries between public and private, between home and work, between personal time and the company's time, and so forth. These barriers are more or less flexible, subject to negotiation and adapted to the needs of the moment. However, they map poorly to the kinds of barriers that technological systems put into place (197).

Embodiment considers the establishment of meaning by considering the "place" of interaction (Harrison and Dourish 1996) and in particular by examining the interpretations of interface presentation (Dourish and Button 1998).

A user's understanding of a performed action within a given interface is heavily

influenced by the aesthetic and affordances used by the designer of the interface.

Hutchins et al. (1986) identify the “gulf of interpretation” as the difficulty of interpreting the system’s state as a response to a user’s command. Dourish (2004) illustrated particular concerns about network security, as computers negotiate heterogeneous network protocols in the name of seamless access (and its corresponding aesthetic), making a user’s awareness of the particular security protocols at any given moment impossible, since the networking decisions are made at the architecture level, hidden from the user’s view (12). These same observations apply to a user’s understanding of how his or her data is collected, stored, analyzed or transmitted within a system or between systems.

To read a social app story, users are prompted to install the Washington Post Social Reader app (though, no mention of the affordance “install” appears on the displayed screen). The user is presented with two options, “Okay, Read Article,” and “Cancel.” Clicking “Okay, Read Article” button installs the app into a user’s Facebook profile and displays the article in the browser window. Clicking the “Cancel” button loads the article from the corresponding website into the browser window without installing the social reader software.

No communication of the actual function of this offered choice is explicit: users are apparently expected to understand that “Cancel” will load the desired article from the *WashingtonPost.com* site instead of in the Social Reader app. In contrast with the “Okay, Read Article” button, the “Cancel” affordance takes on a connotation of NOT reading the article, which is precisely the opposite function clicking the button entails.

This affordance presentation also takes advantage of the user's goal in the interaction: by clicking on a news story associated with a trusted friend's profile, the user is encouraged to become a distributor for *Washington Post* content (and other content offerings by publications with affiliated connections to the *Post*) in their choice that appears to be an articulation of whether or not the article can be read.

On the page presenting the choice, the user is informed the purpose of the app is to "See what your friends are reading, and let your friends know what you read," though the relationship between these two functions is not clear. The user can opt to customize the distribution list for the app, and is informed the app will access "Your basic info," "About You" and "Your likes," though nothing is stated about how this information will be used. Finally, the app install screen disclaims, "This app may post on your behalf, including articles you read and more." This statement discloses that content will be published FROM the user's profile to the news feeds of his or her friends (the "may" is particularly misleading given the sole purpose of the app is to perform the task it disclaims it "may" do, though whether "may" is supposed to convey a sense of possibility or permission is unclear).

Once a user clicks the "Okay, Read Article" button, any article link the user clicks on (whether not that click originates from the Facebook site or the Washington Post site) is displayed on the news feed for that user. Furthermore, all of this activity happens automatically in perpetuity (or until the user uninstalls the app). So by the act of choosing to "read," the user chooses to become an unpaid distributor of content for a media organization.

### Analysis and Conclusions

Ishii and Ulmer (1997) argued that Americans live in two worlds: the world of computation (“bits”) and the world of physical reality (“atoms”). Recognizing both as part of a user’s context, designers of information collection interfaces bear a responsibility for communicating the implications of computation in terms of the potential effect in the physical reality. Whereas computer interactions have largely been described in the past in terms of objects (computers themselves), computing decisions now consist of a myriad of situations, all represented to users by aesthetics (interfaces) that imply contexts that may or may not exist.

For most users, privacy decision-making is still performed in ways Warren and Brandeis defined in 1890 and Goffman articulated in 1959: the manipulation of image in public space. Though that framing of privacy is protected by laws originating from the invasion of the mechanical technology in the beginning of the industrial age, the legal codes protecting one’s reputation do little to protect one’s data or prepare users to make educated decisions regarding their data in response to the introduction of digital technologies in the present age.

Warren and Brandeis struggled to control the public display of images, but the challenge facing most contemporary information consumers is the nonpublic display of personal data between unknown data brokers. Thus, agents clandestinely trade credible “gossip” about users that does not defame anyone’s public reputation, but nonetheless has no less real consequences for matters of authentication, trust and access.

But methods of information gathering, designed using aesthetics of simplicity to encourage interactions, are usually divorced from this brokerage altogether. Users have

one experience of the digital object, which in turn populates a different (and invisible, as far as the user is concerned) object, which in turn communicates with other objects far from the user's view.

Pertinent regulations pertaining to data practices do exist. The *Code of Fair Information Practices* ("U.S. Dep't. of Health," 1973) is one such example, based on five noteworthy principles:

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

However, most Internet users report fears about data security but take no action to protect or account for how their data is being used. Because consumers have legal protections, most sites create carefully worded disclosure statements about the use of data, but then present such disclosures in a onerous way that makes it unlikely that a consumer will engage the disclosure statement in any meaningful way, hiding behind the aesthetic of simplicity that implies a context unrepresentative of the network structure of most tools.

The surveillance and storage of user data will continue to be an important part of computer and network interactions. For many, surveillance is viewed as a mere negative

side effect, apparently not seeming intrusive enough to make us give up new technology services.

Trust between individuals in our society continues to decline (Paxton 2005; Putnam 2000). Individuals are increasingly likely to interact with strangers without the information needed to assess reputation (Heimer 2001), primarily because they are increasingly part of large impersonal communities with highly mobile populations (Nock 1993, 11-12). As a result, the core assumptions of American privacy law, forged during the Industrial Revolution during a time of intense class warfare, do little to protect one's personal data from being collected, transmitted, stored and transferred between credentialing agencies in the 21<sup>st</sup> Century.

Interfaces serve as the digital ambassadors of systems interactions to the world of users. In most cases, interfaces and their embedded affordances (and what they communicate to the user) influence whether, and to what extent, users will interact with a given set of systems or tools. When affordances communicate a particular set of information values that are not held or practiced within the system, surprise and confusion occur when the difference is discovered. But the difference will rarely be discovered, as the back-end architecture of most systems is necessarily veiled from the gaze of the interacting users. User interfaces are currently not designed to explicitly communicate how data is used and stored, what potential risks are involved or even what can be done with the information provided.

News media organizations that adopt social reader applications contribute to this problem by offering their content as an enticement to increase the rate of social reader diffusion. By linking the apparent affordance of "read" to the poorly communicated

“install” function (without explicit communication of the consequences of a user’s choices in the interface), for example, news media organizations exacerbate the confusion that undermines a user’s ability to make informed privacy decisions. If users are to obtain an understanding of information processes necessary to take responsibility for their choices and actions, those processes should be communicated more effectively through the user interface.

Reference List

- Acquisti, A. and R. Gross. (2006). Imagined communities: awareness, information sharing, and privacy on the Facebook. In the *Proceedings of Privacy Enhancing Technology (PET 2006)*, Cambridge, June 28-30, 2006.
- . (2005). Information revelation and privacy in online social networks (the Facebook case). In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA, USA, November 7, 2005: 71-80.
- Alexander, K. (2007). Fast times at make-believe high. *Boston Magazine*. February 4. [http://www.bostonmagazine.com/articles/fast\\_times\\_at\\_make\\_believe\\_high](http://www.bostonmagazine.com/articles/fast_times_at_make_believe_high).
- Aspan, M. (2008). How Sticky Is Membership on Facebook? Just Try Breaking Free. *The New York Times*. February 11. <http://www.nytimes.com/2008/02/11/technology/11facebook.html>.
- Bakardjieva, M. (2005). *Internet Society: The Internet in Everyday Life*. London: Sage.
- Ben-Bassat, T., J. Meyer, and N. Tractinsky. (2006). Economic and subjective measures of the perceived value of aesthetics and usability. *ACM Transactions on Computer-Human Interaction* 13, 210- 234.
- Benjamin, W. (1969). The Work of Art in the Age of Mechanical Reproduction. *Illuminations: Essays and Reflections*. New York: Schochen Books: 217-252.
- Bennett, C., C. Raab, and P. Regan. (2003). People and Place: Patterns of Individual Identification within Intelligent Transportation Systems. In David Lyon (Ed.) *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*. London: Routledge.
- Berndt, R.M. (1962). *Excess and Restraint*. Chicago: University of Chicago Press.
- Birkhoff, G.D. (1933). *Aesthetic measure*. Harvard University Press, Cambridge.
- boyd, d. (2004). Friendster and publically articulated social networking. In the *Extended Abstracts of the Conference on Human Factors and Computing Systems (CHI 2004)*. Vienna, Austria: 1279-1282.
- boyd, d. and J. Heer. (2006). Profiles as Conversation: Networked Identity Performance on Friendster. In *Proceedings of the Hawai'i International Conference on System Sciences (HICSS-39)*, PersistentConversation Track. Kauai, HI: IEEE Computer Society.
- Brown, J.S., and M. Weisner. (1997). "The Coming Age of Calm Technology," *Beyond Calculation: The Next Fifty Years*. New York: Copernicus: 75-85.

- Calore, M. (2006). Privacy fears shock Facebook. *Wired*. September 6.  
<http://www.wired.com/news/culture/0,71739-0.html>
- Castells, M. (1996). *The Rise of the Network Society*. Cambridge, Mass.: Blackwell Publishers.
- Cherny, Robert W. (1997). *American Politics in the Guided Age: 1868-1900*. Wheeling, Ill.: Harlan Davidson, Inc.
- Cooley, T.M. (1888). *A Treatise on the Law of Torts*. 2 Chicago: Callaghan & Co.
- Cyr, D., G.S. Kindra, and S. Dash. (2008). Web site design, trust, satisfaction and e-loyalty: The Indian experience. *Online Information Review* 32, 773-790.
- Dey, A.K., G.D. Abowd and D. Salber. (2001). A Conceptual Framework and a toolkit for Supporting the Rapid Prototyping of Context-aware Applications. *Human-Computer Interaction*, 16 (2-4): 97-166.
- Donohoe, M. (2011). September 26. *Tumblr*.  
<http://donohoe.tumblr.com/post/10683087630/wp-social-reader>
- Dourish, P. (2004). What We Talk About When We Talk About Context. *Personal and Ubiquitous Computing*, 8(1): 19-30.
- . (2001). *Where the Action Is: The Foundations of Embodied Interaction*. Cambridge: MIT Press.
- Dourish, P., and G. Button. (1998). On Technomethodology: Foundational Relationships between Ethnomethodology and System Design. *Human-Computer Interaction*, 13(4): 395-432.
- Ehn, P. (1998). Manifesto for a Digital Bauhaus. In *Digital Creativity*. 9(4): 207-216.
- Eysenck, H. (1941). The empirical determination of an aesthetic formula. *Psychological Review* 48, 83-92.
- Fogg, B.J., C. Soohoo, D.R. Danielson, L. Marable, J. Stanford, and E.R. Tauber. (2003). "How do users evaluate the credibility of Web sites?" In *Proceedings of the 2003 conference on Designing for user experiences*. ACM, San Francisco, California, 1-15.
- Friedman, B. (1997). Social Judgments and Technological Innovation: Adolescents' Understanding of Property, Privacy, and Electronic Information. *Computers in Human Behavior*, 13 (3): 327-351.

- Gandy, O.H. (1993). *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, Colo.: Westview.
- Garfinkel, H. (1967). *Studies in Ethnomethodology*. Cambridge: Polity Press.
- Gibson, J.J. (1979). *The Ecological Approach to Visual Perception*. Boston: Houghton Mifflin.
- Goffman, E. (1959). *The Presentation of Self in Everyday Life*. Garden City, NY: Doubleday.
- Gombrich, E.H. (1995). *The story of art*. Phaidon, London.
- Grabowicz, P. (2012 March 8). Print Editions Decline. *The Transition to Digital Journalism*. <http://multimedia.journalism.berkeley.edu/tutorials/digital-transform/print-editions-decline/>
- Gross, R. and A. Acquisti. (2005). Information revelation and privacy in online social networks (the Facebook case). In *Proceedings of the 2005 ACM workshop on Privacy in the electronic society*, Alexandria, VA, USA, November 7, 71-80.
- Grudin, J. (2001). Desituating Action: Digital Representation of Context. *Human Computer Interaction*, 16 (2-4): 269-286.
- Hallnäs, L. and J. Redström. (2002). From Use to Presence; On the Expressions and Aesthetics of Everyday Computational Things. In *ACM Transactions on Computer-Human Interaction (ToCHI)*, Vol. 9, No. 2, June 2002, 106-124.
- Hartmann, J., A. Sutcliffe, and A. De Angeli. (2007). Investigating attractiveness in web user interfaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. San Jose: ACM Press, 387-396.
- Hassenzahl, M. (2004). The interplay of beauty, goodness, and usability in interactive products. *Human-Computer Interaction* 19, 319-349.
- Hassenzahl, M., N. Tractinsky. (2006). User experience - a research agenda. *Behaviour & Information Technology* 25, 91-97.
- Heimer, Carol A. (2001). Solving the Problem of Trust. In Karen S. Cook (ed). *Trust in Society*. New York: Russell Sage Foundation: 40-89.
- International Organization for Standardisation (ISO). (2010). *Human Centered Design Process for Interactive Systems*. ISO 13407.
- Harrison, S. and P. Dourish. (1996). Re-Place-ing Space: The Roles of Space and Place in Collaborative Systems. *Proceedings of ACM Conference on Computer-*

- Supported Cooperative Work*: 67-76. New York: Association for Computing Machinery.
- Hutchby, I. (2001). Technologies, Texts and Affordances. *Sociology* 35(2): 441–56.
- Ishii, H., and B. Ullmer. (1997). Tangible Bits: Towards Seamless Interfaces Between People, Bits and Atoms. *Proceedings of ACM Conference on Human Factors in Computing Systems*: 234-241. New York: Association for Computing Machinery.
- Johnson, S. (1997). *Interface Culture: How New Technology Transforms the Way We Create and Communicate*. San Francisco: HarperEdge.
- Jupiter Research. (2002). Seventy percent of US consumers worry about online privacy, but few take protective action. [http://www.jmm.com/xp/jmm/press/2002/pr\\_060302.xml](http://www.jmm.com/xp/jmm/press/2002/pr_060302.xml).
- Katyal, N. (2002). Architecture as Crime Control. *Yale Law Journal* 111: 1039-1139.
- Kristiina K. (2000). The Beauty of Simplicity. In *Proceedings on the 2000 conference on Universal Usability* (CUU '00). ACM, New York, NY, USA, 85-90.
- Kim, J., and J.Y. Moon. (1998). “Designing towards emotional usability in customer interfaces - trustworthiness of cyber-banking system interfaces.” *Interacting with Computers* 10, 1-29.
- Livingstone, S. (2008). Taking Risky Opportunities in Youthful Content Creation: Teenagers' Use of Social Networking Sites for Intimacy, Privacy and Self-Expression. *New Media Society* 10(3): 393-411.
- Mathiesen, T. (1997). The Viewer Society: Michel Foucault’s ‘Panopticon’ Revisited. *Theoretical Criminology* 1(2): 215–234.
- McMillan, S.J. and M. Morrison. (2006). Coming of Age in the E-Generation: A Qualitative Exploration of How the Internet has Become an Integral Part of Young People’s Lives. *New Media & Society* 8(1): 73-95.
- Mitchell, A., T. Rosenstiel, and L. Christian. (2012). What Facebook and Twitter Mean for News. *The State of the News Media 2012*. <http://stateofthemediamedia.org/2012/mobile-devices-and-news-consumption-some-good-signs-for-journalism/what-facebook-and-twitter-mean-for-news/?src=pre-twitter>
- Mok, C. (1996). *Designing Business*. San Jose: Adobe Press.

- Moshagen, M., J. Musch, and A.S. Göritz. (2009). A blessing, not a curse: Experimental evidence for beneficial effects of visual aesthetics on performance. *Ergonomics* 52, 1311-1320.
- Moshagen, M. and M.T. Thielsch. (2010). Facets of visual aesthetics. *International Journal of Human-Computer Studies*, 68(10), 689-709.
- Murphy, R. F. (1964). Social Distance and the Veil. *American Anthropologist* 66: 1257-1274.
- Nielsen, J. (1999). *Designing Web Usability: The Practice of Simplicity*. New Riders Publishing, Indiana.
- . (1993). *Usability Engineering*. Academic Press, Boston.
- Nock, S.L. (1993). *The Costs of Privacy: Surveillance and Reputation in America*. New York: A. De Gruyter.
- Palen, L., and P. Dourish. (2003). Unpacking “Privacy” for a Networked World. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*: 129-136. New York: Association for Computing Machinery.
- Paxton, P. (2005). Trust in Decline? *Contexts*. 4(1): 40-46.
- Prosser, W.L. (1960). Privacy. *California Law Review* 48: 338-423.
- Putnam, R.D. (2000). *Bowling Alone: the Collapse and Revival of American Community*. New York: Simon & Schuster.
- Ramasastri, A. (2008). On Facebook Forever? Why the Networking Site was Right to Change its Deletion Policies, And Why Its Current Policies Still Pose Privacy Risks. *FindLaw.com*. February 29.  
<http://writ.news.findlaw.com/ramasastri/20080229.html>.
- Raskin, J. (2000). *The Human Interface: New Directions For Designing Interactive Systems*. Reading: Addison Wesley.
- Rosen, J. (2000). *The Unwanted Gaze: The Destruction of Privacy in America*. New York: Random House.
- Shneiderman, B. (1998). *User Interface Design*. 3rd ed., Reading (MA), Addison-Wesley.
- Solove, D.J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York: New York University Press.

- Solso, R.L. (2003). *The psychology of art and the evolution of the conscious brain*. MIT Press, Cambridge.
- Sonderegger, A., and J. Sauer. (2010). The influence of design aesthetics in usability testing: Effects on user performance and perceived usability. *Applied Ergonomics* 41, 403-410.
- Sonderman, J. (2011, November 30). How news orgs are reaching millions through Facebook's new apps. *Poynter*. <http://www.poynter.org/latest-news/media-lab/social-media/154470/6-lessons-from-new-facebook-stats-on-social-news-sharing/>
- Stevens, J.R. (2007). Facing Change: The Role of Context and Privacy Expectations in Facebook Disclosure Decisions. Paper presented at the Midwinter Meeting of the Association for Education in Journalism and Mass Communication in Reno, NV.
- Story, L. (2007). The Evolution of Facebook's Beacon. *The New York Times BITS blog*. November 29. <http://bits.blogs.nytimes.com/2007/11/29/the-evolution-of-facebooks-beacon/>.
- Story, L. and B. Stone. (2007). Facebook Retreats on Online Tracking. *The New York Times BITS blog*. November 30. <http://www.nytimes.com/2007/11/30/technology/30face.html>.
- Stutzman, F. (2006). An Evaluation of Identity-sharing Behavior in Social Network Communities. *International Digital Media and Arts Association Journal* 3(1).
- Sutcliffe, A., and A. de Angeli. (2005). Assessing Interaction Styles in Web User Interfaces. In *Proceedings Human-Computer Interaction - INTERACT 2005*. pp. 405-417.
- Thüring, M., and S. Mahlke. (2007). Usability, aesthetics and emotions in human-technology interaction. *International Journal of Psychology* 42, 253-264.
- Tractinsky, N. (1997). Aesthetics and Apparent Usability: Empirically Assessing Cultural and Methodological Issues. In *Proceedings of the SIGCHI conference on Human factors in computing systems (CHI '97)*. ACM, New York, NY, USA, 115-122.
- Tractinsky, N., Katz, A.S., Ikar, D., 2000. "What is beautiful is usable." *Interacting with Computers* 13, 127-145.
- Tuan, Y. (1977). *Space and Place: The Perspective of Experience*. Minneapolis: University of Minnesota Press.

- U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens. (1973). viii.
- Warren, S.D. and L.D. Brandeis. (1890). The Right to Privacy. *Harvard Law Review* 4: 193-220.
- Wood, A.L. (1974). *Deviant Behavior and Control Strategies*. Lexington, MA: D.C Health.
- Zuckerberg, M. (2006). Calm down. Breathe. We hear you. *Facebook Blog*. Sept. 5. <http://blog.facebook.com/blog.php?post=2208197130>