The Information Society

An International Journal

Routledge
Taylor & Francis Group

ISSN: 0197-2243 (Print) 1087-6537 (Online) Journal homepage: http://www.tandfonline.com/loi/utis20

The emotional context of information privacy

Luke Stark

To cite this article: Luke Stark (2016) The emotional context of information privacy, The Information Society, 32:1, 14-27, DOI: 10.1080/01972243.2015.1107167

To link to this article: http://dx.doi.org/10.1080/01972243.2015.1107167

Published online: 22 Dec 2015.

THE INFORMATION SOCIETY
2016, VOL. 32, NO. 1, 14–27
http://dx.doi.org/10.1080/01972243.2015.1107167

Routledge
Taylor & Francis Group

The emotional context of information privacy

Luke Stark

Department of Media, Culture, and Communication, New York University, New York, New York, USA

ABSTRACT
Why are ongoing legal, design, and policy debates around information privacy often divorced from the lived experience of everyday digital media use? This article argues that human emotion is a critical but undertheorized element in users' subjective sense of information privacy. The piece advocates for a greater attention to the phenomenology of feeling and to the concept of "visceral" design in information privacy scholarship, policy, and design practice.

ARTICLE HISTORY
Received 22 September 2014
Accepted 1 August 2015

KEYWORDS
Contextual integrity; emotion; interaction design; law; policy; phenomenology; privacy; social computing; visceral design; visceral privacy

Information privacy and public feeling

In this article, I propose that human emotion is a critical element structuring the divide between our individual misgivings about information privacy, and the challenges that surround its protection in terms of lived experience, public policy, and design. Though emotion lurks at the margins of current popular and academic discussions regarding information privacy and surveillance, it is rarely addressed as a central factor in online privacy debates, particularly within legal and policy circles. Yet two contemporary examples suggest that our emotions are highly relevant to our privacy—and in a digital world, more pertinent than ever to its preservation.

On March 16, 2013, several months before Edward Snowden began to publicize the widespread domestic surveillance activities of the National Security Agency (NSA), security expert Bruce Schneier published an opinion piece for CNN titled "The Internet Is a Surveillance State" (Schneier 2013). Decrying the perceived lack of public outrage toward rampant governmental and commercial data mining, collection, analysis, and commoditization, Schneier concluded his piece in a particularly downcast tone. "Welcome to an Internet without privacy," Schneier declared; "we've ended up here with hardly a fight." Against the technical and rhetorical advances of Big Data analytics, American citizens had seemed only sporadically willing to stand up for their privacy rights, at least in the run-up to the Snowden affair. Schneier's pessimism may or may not be justified. Yet his article was noteworthy not only for the facts Schneier presented *per se*, but also for its negative sentiment: Closing in disillusionment, anger, and not a little defeatism, the emotional mood of Schneier's piece seemed to foreclose even a modicum of social or technological space for change or resistance.

A second example is more recent, and perhaps more infamous. In June 2014, the media picked up on the results of a paper published in *Proceedings of the National Academy of Science* (*PNAS*) by researchers from Facebook and Cornell University. The authors claimed that their experiment, which had slightly modified the positive or negative emotional content of more than half a million Facebook users' News Feeds, demonstrated that feelings expressed online were "contagious": Users viewing happier content posted happier content themselves and vice versa (Kramer, Guillory, and Hancock 2014). The study provoked tremendous controversy. Facebook was accused of manipulating the emotions of its users in the name of scientific research and corporate profit—"Prepare to have Facebook curate your feed with the most emotional of your friends' posts if they feel you're not posting often enough," one report warned (Hill 2014, online). Within the academy, the study generated heated debate around research ethics and social media, the role of institutional human subjects review boards in overseeing studies using Big Data analytics, and the ubiquity of live A/B testing in user experience (UX) design. Yet fundamentally, the enormous

CONTACT Luke Stark ✉ luke.stark@nyu.edu 🖃 Department of Media, Culture, and Communication, New York University, 239 Greene Street, New York, NY 10003, USA.

outpouring of feeling grounding the controversy stemmed from the fact that it was the emotions of individuals that had been tampered with without consent. Angry users said so themselves: "'They said, 'you can't mess with my emotions. It's like messing with me. It's mind control','" Jeffrey Hancock, one of the authors of the study, bemusedly admitted to *The New York Times* (Goel 2014, online).

I seek to make the links between human emotion and the legal, policy, and design facets of information privacy explicit rather than implicit. Examining information privacy in relation to its objects of interest—ordinary people using computers, smartphones, and other digital devices in their daily activities—is central to making such an analysis work. The ways in which digital media technologies influence our perceptions of information privacy are inextricably tied to the ways these technologies modulate our emotions in general: With a few exceptions (Taslitz 2002; Solove 2007; Nippert-Eng 2010; Andrews 2012), these questions have been undertheorized in the information privacy literature. Moreover, privacy scholarship in fields such as behavioral economics and the law only infrequently takes the interfaces and physical materials of digital media technologies into account in explaining privacy as a lived experience, underplaying their role in constructing the individual's subjective understanding of privacy. It is vital that scholars of all stripes take these domains seriously so that they can help policymakers in crafting effective legislative and regulatory responses to information privacy threats. It is also critical to bring this scholarship into conversation with the designers of digital media technologies, so that attention to human emotion and privacy can be built together into digital media artifacts and the broader systems in which they, and we, live.

My argument proceeds in four parts. I first define and advocate for the explicit inclusion of emotion as a matter of concern in current scholarship on information privacy. I subsequently provide a brief overview of how theories of mediation drawn from computer science and digital media studies provide a useful framework for concretizing emotion's role in shaping conceptions of privacy. I focus on the centrality of the lived, phenomenological experience of privacy in the third part of the piece, and conclude by suggesting legal, policy, and design interventions that will work in tandem to protect individual privacy through engagement with human feeling. Central to this final portion of the argument are the concepts of "data visceralization" and "visceral privacy," which I present as novel frameworks for bringing empirical research, law, policy, and design together. Throughout, I seek to strengthen the conceptual underpinnings of privacy research and point toward grounded, pragmatic ways for technology designers, policymakers, and ordinary people to feel differently about their privacy online—and thereby act, legislate, and design differently too.

Privacy and emotion in the age of big data

Emotion is a contested concept even within the disciplines traditionally most directly concerned with its study—philosophy, psychology, and neuropsychiatry. Related terms such as feeling, mood, and affect can also cause confusion. While a full rehearsal of these debates is beyond the scope of this article, theories of emotion can be classed into three broad categories. A first, *organismic* tradition in biology, psychology, neuroscience, and some philosophical work understands emotion as arising directly out of affects, physical drives that are outside of conscious control and that influence human thought, feeling, and behavior in broadly universal patterns (Ekman and Friesen 1971; Sahakian et al. 2008; Massumi 2010; Prinz 2004). A second, *interactional* school of thought has tended to focus on the expression of emotions as socially and culturally specific (Abu-Lughod and Lutz 1990). Finally, a third, *interactionist* approach favored by a number of interdisciplinary scholars contends that emotions spring from the dynamic, emergent interplay of internal factors (biological, affective, and psychological) and external ones (including social context and environment)—a pragmatic splitting of the causal difference that reads emotions as generative, transformative, and situational to the material and social contexts in which we live (Boehner et al. 2007; Hochschild 2003). In her seminal book *The Managed Heart*, sociologist Arlie Russell Hochschild argues persuasively for the interactionist ground: a model of emotion that is both dynamic and reciprocal. While these debates are long-standing, the interactionist perspective seems to convincingly incorporate the best of both theoretical worlds. For the purposes of this article, I follow Deborah Gould's useful definitions in this vein: Emotions (or a term I use interchangeably for them here, feelings) are affects—"nonconscious and unnamed experiences of bodily energy and intensity"—that become "actualized or concretized in the flow of living" through language, embodiment, custom, and technology (Gould 2010, 26). Yet our emotional responses are also attuned to other actors, and vice versa: "Just as modern linguists now examine language as it is used in social context," Hochschild writes, "so emotion, another sort of language, is best understood in relation to its social context" (Hochschild 2003, 212n). In our everyday emotional lives, it makes intuitive sense that our feelings are shaped by our milieu, but also that affects push and pull our behaviors and actions; emotions emerge as consciously reflected-upon bodily sensations springing from a dynamic and reflexive sense of self and others.

Bruce Schneier's lament notwithstanding, controversies such as the aforementioned Facebook study suggest that the digital mediation of emotions is of widespread public concern—as are worries about information privacy. In its September 2013 survey "Anonymity, Privacy, and Security Online," the Pew Research Center found that 86% of Internet users had tried to "minimize the visibility of their digital footprints" through a variety of means, ranging from the use of encryption and obfuscation techniques like providing false information, to clearing cookies and Web browser histories (Rainie et al. 2013). Perhaps unsurprisingly, strong majorities also reported desiring autonomy in determining who had access to a variety of information about online behavior, including the contents of e-mail and chat logs, the locations from which individuals used the Internet, and searches performed and digital software applications used.

The public, then, is indeed paying attention to information privacy, and it has good reason to do so. In the last decade, the integration of digital data collection into everyday life has gone from speculative research to institutional fact (Dourish, Brewer, and Bell 2005). The Apple Watch, wired refrigerators, thermostats, coffeemakers and crock pots, and the wide array of sensors integrated into smartphones are some examples of a trend toward computing devices that are wearable, mobile, and constantly connected to digital networks; specialized devices like the Nike FitBit and similar software applications track our gait, movements, sleep, blood sugar, and mood (Purpura et al. 2011; Dimos 2012). Alongside these mobile technologies have come new algorithmic techniques of data mining, data visualization, and data analysis, often classed under the misleading label of Big Data (*Economist* 2010; Andrejevic 2013; Barocas and Selbst in press). These technologies integrate the outputs of our devices into a detailed digital portrait of our dynamic, desiring lives, one that can be bought, sold, queried, and exploited at will by those with the financial and technical ability or wherewithal to do so, sometimes even including ourselves (Cohen 2000; Pasquale 2010; Nissenbaum 2011b).

Yet the interactionist model of emotion, which seems well placed to help unpack some of the complex privacy questions associated with these aforementioned sociotechnical phenomena, has a tenuous place in recent scholarship on information privacy, particularly in legal and policy discourse.[1] Ethnographic studies such as Christena Nippert-Eng's *Islands of Privacy* (2010) or Sherry Turkle's *Alone Together* (2011) have drawn attention to the lived experience of privacy as a personal matter of emotional importance, but skirt explicit analysis of emotion's place in the nexus of privacy practice, design, and policy. And with much of the debate around information privacy conducted in the language of behavioral economics, the lived nuances and messy complexities of how ordinary people engage with their own feelings about information privacy tend to be bracketed as nonrational, and outside of the scope of legal and technical analyses. The otherwise strong work of Alessandro Acquisti (Acquisti and Grossklags 2005), Lorie Faith Cranor (Hourcade et al. 2014), and others exploring the behavioral science behind privacy preferences is nonetheless grounded in rational choice as a model to enable claims about future behavior, and by extension to shape design and policy solutions (Garvin 1998; Wang et al. 2011; Acquisti 2012; Acquisti, Brandimarte, and Loewenstein 2015). This work has usefully highlighted the concepts of information asymmetries and bounded rationality in the behavior of individual actors online. However, this scholarship has difficulty transcending its own frame of reference to offer broader insights on the subjective experience of online life, and why people act in the "irrational" ways they seem to do.

As a result of its circumscribed focus, the policy agenda working to strengthen online privacy norms has tended to focus on relatively narrow questions such as the efficacy of notice and consent and its practical implementation (Barocas and Nissenbaum 2009; Cranor 2012; Balebako et al. 2013; Wang et al. 2014). This work is valuable, but insufficient. It is not simply the case that, as Julie Cohen has noted, people find it "difficult to assess the future significance off a loss of privacy, much less to compare that future harm with a currently offered benefit" (Cohen 2000, 1397). Some scholarship in this vein implicitly treats the "irrationality" of everyday citizens online as a fault to be lamented, and not a more complex phenomenon to be explored on its own terms. To observe that people "are demonstrably bad" at sacrificing present convenience for future value risks misreading, and reifying, behaviors as either "rational" and "irrational." My argument is not meant to dismiss or disregard the findings of behavioral privacy scholars, but instead to fill in the gaps where analyses of rational choice come up short. Grounding arguments about information privacy in an embodied account of the individual, her context of information technology use, and the longer history of subjective sensations of perception and feeling reframes privacy discussions toward what Daniel Solove terms "a more nuanced view," closely grounded in the welter of real-life thinking, feeling, and experience (Solove 2007).

Privacy and the mediated senses

In the digital landscape surveyed by information privacy advocates, feelings are hardly absent. Today, emotion is big business in the world of computational media, and the networked expressions of emotions are increasingly subjected to what historian of science Otniel Dror calls "the discourse of numbers" (Dror 2001). Text-based sentiment analysis, facial recognition technologies, and self-tracking by adherents to the "quantified self" movement are just three manifestations of the close contact between data, our subjective feelings about the world, and our physical feeling-out of it. This quantizing stance has already engendered pushback; indeed, when boyd and Crawford (2012) ask "Do numbers speak for themselves?" the answer is a resounding "'no'" (666). Yet as the 2014 Facebook emotional contagion episode suggests, data analytics are nonetheless increasingly applied to our interactions with information technologies to produce volumes of information about our patterns of emotional expression and behavior—data that are analyzed and processed far outside our awareness or control (Andrejevic 2013). Widely varied contemporary digital businesses seek to track, correlate, and predict online consumer behavior: Emoticons, emoji, and animated graphics allow individuals to emote, and be tracked, digitally. As Mark Andrejevic observes, "In such approaches statistical proxies for affective intensities displace reference, meaning, and comprehension" (54)—in other words, marketers are less interesting in learning the why and wherefore of the expression of online feeling if they can get enough of a sense of its general tones and moods to effectively sell products and services.

Contemporary information privacy scholars argue that these technological developments expose clumsy, outdated assumptions about the conceptual definition of privacy itself (Cohen 2000; Solove 2006a). Instead of conceiving privacy as perhaps tenuous control over personal data or necessarily imperfect knowledge of how that data is being used, Helen Nissenbaum locates the germ of privacy in the notion of "contextual integrity," which she defines as the "contextually appropriate" flows of information online (Nissenbaum 2011b). In Nissenbaum's view, personal information should circulate according to its rightful place in the complex and dynamic social texture of our lives. Yet at the same time that emotion's role in the design and use of information technologies is an increasingly prominent subject in technical and conceptual work on digital media, particularly by scholars in the subfield of computer science known as human–computer interaction (HCI), emotion is largely silent as a critical area for privacy's context to be understood.

Early scholarship in HCI and emotion focused on aspects of machine learning and cognition, and the practical ability and desirability of information systems to be able to "read" and categorize human feelings (Picard 2000). This work is grounded in what Kirsten Boehner (2007) and her coauthors term an "informational" model of feeling, in which emotions are quantifiable inputs to be measured and processed by the machine, building on a long history stretching back to the development of physiological classification as a recognized medical specialty in the nineteenth century (Dror 2001). However, recent work in HCI has advocated for a more explicitly interactionist approach to emotion and a focus on the contextual specificity of feeling, a view that chimes neatly with the work of Nissenbaum and others on privacy. In a reiteration of the interactionist model of emotion advanced by Hochschild, Boehner and her coauthors contend that even in matters computational, "Emotion is an intersubjective phenomenon, arising in encounters between individuals or between people and society, an aspect of the socially-organized life world we both inhabit and reproduce" (Boehner et al. 2007, 280).

Given that interactionist approaches to emotion in HCI are a relatively recent development (Gay et al. 2008), it is perhaps unsurprising that, in general, emotion has not yet come to play a major role in the interwoven technical, policy, and design debates around information privacy (Nippert-Eng 2007). Yet the interactive turn in HCI suggests that these discussions would benefit from a greater focus on emotion and privacy paired together as a complex, subjective experience particularly amenable to creative design solutions. Implicit in an interactionist model of emotion is the view that feeling is intimately tied to our physical perception of reality as conveyed through the senses; social science research has buttressed the view that emotions and sense perception condition our subjective constructions of privacy, online and off. [2] In the 1970s, anthropologist Irving Altman observed that while our understanding of what privacy entails differs based on cultural context and individual proclivity, managing our sense of world to carve out a private, autonomous space for individual dwelling is nonetheless a common concern for cultures of all sorts—what Nippert-Eng describes as "islands of privacy" now increasingly under threat from the rising tide of digital connectivity (2010). The ways in which we construct these subjective private spaces are implicitly affective. "Privacy regulation," Altman writes, "involves more than use of the physical environment alone, but includes a variety of verbal, nonverbal, environmental, and cultural mechanisms" (Altman 1977). According to Altman, humans maintain the parameters of privacy through the construction and maintenance of "barriers," some physical and material, some mental and emotional; most of these barriers are assemblages of various cultural, psychological, and material factors. Altman concludes that "the ability to regulate interaction is necessary for individual and cultural survival," citing the complex arrangements of a variety of cultures around the world as examples of the ways in which physical space and mental life can interact to provide different iterations of an individual sense of privacy (Altman 1977, 82). For a contemporary example of this mix of physical, psychological and social elements, consider the diversity and complex use dynamics of window coverings in dense urban spaces, in which public and private actors interact both in person and at a distance—such as along New York City's elevated High Line park (Nissenbaum and Varnelis 2012).

Implicit in Altman's insight is that affect and emotion are central elements facilitating and prompting our socialized sense of what is an appropriate privacy-preserving behavior. Moreover, emotions work in conjunction with numerous other sociotechnical elements to foster culturally contextual privacy situations: the built environment; patterns of movement and mobility; symbolic cues, rituals, and traditions; and technologies, including by extension our electronic and digital media. Of course, the notion of "context" itself can sometimes be a moving target, with social mores changing so quickly under the influence of new technologies that what is "appropriate" and what is not becomes a blurry and contested notion (Bellanova 2011). Yet the dynamism of an individual's context is precisely what links together one's sense of the private self *per se* with one's own feelings. Legal scholar Julie Cohen's conception of the salience of privacy to the freedom and autonomy of the individual is worth quoting at length:

> The self who is the real subject of privacy law and policy is socially constructed, emerging gradually from a preexisting cultural and relational substrate. … Privacy shelters dynamic, emergent subjectivity from the efforts of commercial and government actors. … It protects the situated practices of boundary management through which the capacity for self-determination develops. (Cohen 2013, 905)

Cohen is right to emphasize not merely the contextual, but also the dynamic and reciprocal nature of privacy: one that develops in and is reinforced by emotional reflection and self-determination.

Implicit in the work of both Nissenbaum and Cohen are the same societal concerns expressed by anthropologists like Altman, sociologists such as Nippert-Eng, and computer security experts like Schneier: that the rich diversity of life experiences both online and off will become increasingly trammeled, channeled, or eroded by the loss of privacy prompted by corporate and government data collection and data mining. Emotion is an implicit element within the broader theory of contextual integrity, though Nissenbaum does not specify it as a major component; emotions are just as central, though again implicit, to Cohen's vision of the dynamic and reflexive digital subject. I suggest we need to understand the construction of informational privacy actively through our senses, including our emotions, as embodied individuals with a particular subjective perspective on the world. The work of scholars such as Nissenbaum, Cohen, Altman and Nippert-Eng points toward the same important, but by no means fatal, omission in current information privacy research and design work, which I seek to correct: a lack of attention to the visceral, everyday experience of human emotion in digital media use as a key factor that shapes privacy decision making. How these feelings take shape is the subject for the next portion of the article.

A phenomenology of information privacy

At once sensory, intersubjective, and contextual, our emotions resist pigeonholing. Our sense of privacy is also a subjective, sensory, and contextual phenomenon at both the micro (personal) and macro (systemic) levels; it follows that we express feelings for, and preferences about, our information privacy online through words, thoughts, deeds, and emotions. The contexts for these feelings shape what we intuit as "appropriate" in terms of privacy, and vice versa—the particular subjective experience of privacy in a given situation conditions our emotional responses to online interactions, and about our particular privacy-related expectations, beliefs, and behaviors. Most critically, our feelings interact inelegantly with the digital information technologies at hand—or, more accurately, our technologies interact inelegantly with us. Today's digital media scramble and subvert the ways we perceive, understand, and express the emotional nuances of our privacy preferences; this is the central problem linking design, embodied experience, and policy that needs to be unpacked.

One way to illustrate the disjunctions between our subjective feelings about privacy and the digital affordances influencing our online actions is through an exploration of the material layers, or levels, of our digital media devices (Fransman 2002; Solum and Chung 2003). Since Clifford Nass and his colleagues demonstrated that computers serve as genuinely social actors (Nass, Steuer, and Tauber 1994), the research agendas of both media studies scholars and digital designers alike have become increasingly interested in exploring the social capabilities and psychological impacts of computational media (Norman 1989; Montfort and Bogost 2009). Interaction theorist Donald Norman's discussion of the emotional affordances of everyday technological objects is one recent well-known study in this area (Norman 2005). My own analysis draws on Nass, Norman, and on the design paradigm of embodied interaction as described by Paul Dourish (2004) to show how we as embodied individuals "feel" the nuances of these media layers out. Dourish defines embodied interaction as "the creation, manipulation, and sharing of meaning through engaged interaction with artifacts" (126). Social computing and social media, wearable computers, and mobile devices are all offshoots of the attention digital media hardware and software designers now pay to the way we create meaning in lived everyday experience—particularly, I argue, meaning through feeling.

Analyses of the layers of media often start at the level of infrastructure, but my initial subject here is hardware: the plastic materiality of the devices with which we interact to get and stay online. In terms of style and functionality, the objects through which we access the Internet have changed considerably over the past quarter century, but our subjective emotional attachment to the individual pieces of hardware themselves has remained constant, and perhaps even increased in an age of smartphones carried close to the skin. Our embodied relationship with our digital tools is not simply interactive; this relationship is also fundamentally accretive. The philosopher Martin Heidegger claimed that tools are most subjectively "present" to us when they break down, but tools will not break unless we use them first; it is necessary to build up a portfolio of practice with any tool. The learning curve of using a new device, and its own design affordances and failings, dictate how often these devices fail to respond in the ways we want them to do, and how we become accustomed to their foibles (Heidegger 1972; Sennett 2009). Reinforcing these conceptual insights is a burgeoning literature in technology repair and reuse, which has underscored the material temporality of digital devices. Steven Jackson (2014) and other scholars of repair have noted that our machines age with us: Hard casings grow scratched and dented; screens are battered and beaten up.

For some, these signs of wear and tear on a device are anathema, prompting the purchase of cases and protectors to preserve the faultless newness of the physical object; others, as documented in the press (Wax 2013), seem to take cracked iPhone screens or dented casings as badges of pride, and proof of the weathering of life's slings and arrows. Still other users occupy a middle ground, suffering damage to their devices but eager to upgrade when they have the financial or technical wherewithal. The personalization of hardware can also be deliberately accretive. Laptop users routinely affix decals and stickers to the back of their machines to personalize them, much as travelers once bedecked their trunks and musicians still decorate their guitar cases. Smartphone owners consistently bedazzle their units with jewels, cases, and other adornments, and even desktop users in institutional settings apply talismanic personal objects to the tops of their computer monitors. In a variety of ways, people forge subjective, personal connections with the devices they possess or work with on a regular basis, whether through preservation, modification, or decoration.

These individuating marks on hardware devices are often "felt" both with the hand (in the form of the texture of a scratched laptop or the ribbing of a new smart phone case) and with the heart. HCI scholars Alexander Meschtscherjakov, David Wilfinger, and Manfred Tscheligi have developed the concept of "mobile attachment," defined as "a cognitive and emotional target-specific bond connecting a person's self and a mobile phone that is dynamic over time and varies in strength" (Meschtscherjakov, Wilfinger, and Tscheligi 2014, 2319). The authors identify empowerment, enrichment, and gratification as three powerful motivators for this attachment; interaction theorist Sherry Turkle goes further, suggesting that these positive motivating factors prompt humans to turn their devices into what she terms "evocative objects" through their status as fellow travelers in our personal experience and as mediators of that same subjective life (Turkle 2007).[3] Turkle suggests that digital networks have pushed a cultural sense of "other-directedness" to a new extreme: "Without a firm inner sense of purpose," she writes, "people [now look] to their neighbors for validation," easily accomplished through digital communications (Turkle 2011, 161). Instead, I suggest that hardware devices become enlisted as feeling actors in of themselves precisely because it is through them that we are able to engage socially with others—our phones and tablets become, to modify Bruno Latour's term, "emotive actants" (Latour 1992; Latour 2005).

These emotional attachments to and through hardware frequently activate and engage a user's willingness to take actions to protect the privacy of the hardware object in particular, in part because hardware is something users manage in a literally "hands-on" fashion. Users expend considerable time and attention ensuring that their devices, particularly their smartphones, are with physically present on their persons, fully charged and ready to use. Users also tend to be reluctant to lend these devices to strangers, and protect their smartphones as they would protect their wallets and other valuable personal possessions—to the extent that Google and other companies are actively seeking to integrate the functions of the latter into the former (Versace 2013). And when a particular hardware object is lost or damaged, users tend to react emotionally, and not merely because such breakage jeopardizes our digital connection with other people. These devices feel "trusty," objects that we are attached to; their loss produces emotions that, if more or less fleeting, are nonetheless certainly nonephemeral.

Intimately buttressing our emotional connection to hardware is our engagement with the software interfaces through which we access the online world. It is no accident that 86% of respondents in Pew's September 2013 survey on privacy claimed to have "Cleared cookies and browser history" as a way to protect their privacy online, a simple yet intimate intervention accomplishable via a browser's interface with a few clicks of a mouse (Rainie et al. 2013).[4] Most mobile devices are run by an operating system stored within the device itself. The enormous public outcry prompted by Apple's update to iOS 6, which replaced Google Maps with a proprietary Maps application ridiculed for its gross inaccuracies, illustrates the ways in which our experiences with an operating system can prompt strong emotions (Rodriguez 2012), a principle well known to user experience designers. Video game researchers in particular have explored how the hardware and software interfaces of our devices work together in practice to prompt particular visceral sensations and feelings in users (Juul 2010). The longer we use a particular device with a particular interface, the more we personalize its settings and note its quirks; we develop a positive, felt connection with the experience of using the particular device, "our" device. The decline of the Research in Motion (RIM) BlackBerry has been in part attributed to corporate information technology (IT) departments bowing to the pressure from their employees to support smartphones made by Apple or Samsung, precisely because these devices were customizable to the liking of their individual users and used continuously outside of the workplace. In a similar vein, one of the advertised attractions of cloud-based services like Dropbox and Gmail is that these products provide a personalizable account interface that persists across multiple pieces of institutional or public hardware. Other methods of personalization such as "skinning," or modifying the aesthetic features of the interface, also help users build feelings of comfort, familiarity, and attachment to the hardware and software through which they interact with a digital device—a feature that even a pizza company such as Domino's has incorporated into its digital interface.

Earlier, I noted that the context for our feelings shapes what we intuit as "appropriate" in terms of our desire for privacy. Yet our affective and emotional connection to the hardware and interfaces of our devices is precisely what prompts us to be less conscious, and thus less uneasy, about what is the most critical element of information privacy: our device content, our own "small" trails of data and metadata. Scholars at MIT recently made the seemingly diffuse and intangible connection between online behavior and real-world physicality clear with a project provocatively titled Pavlov Poke, which one of its founders describes as "a shocking solution to Facebook and email addiction" (Morris and McDuff 2013, online). The researchers devised a mechanism that administers an electric shock to the Internet user who accesses Facebook or e-mail services too frequently. While cheeky in its conceptualization, Pavlov Poke's originators write seriously about their desire that devices such as theirs assist individuals in the process of "affective self-discovery," as a way to fend off the addictive properties of digital technology and to make the link between online data flows and offline behavior more palpable.

Yet design projects such as Pavlov Poke are the exception rather than the rule: Because users do not generally experience the circulation of intangible digital data through sense perception; they do not "feel" for its loss and possible misuse in visceral, embodied, emotional ways. As such, our understanding of the appropriateness of the flows of our personal data, and incorporation of these data into and analysis through large data sets, is highly skewed. This blind spot persists in part because our bundled hardware and software interfaces are richly appreciable through multiple sensory channels: We see a device's buttons, hear its alarms and beeps, caress its touch screen, smell the plastic cover that we have purchased to protect it, perhaps even hold it in our mouth and taste it while we tie our shoes. And in being drawn emotionally to the connectivity and interactivity these devices enable, and the personal history they represent as material artifacts, we become attached to the objects and interfaces themselves, not necessarily to their contents. But much of the data we produce on a daily basis, particularly our metadata, is not traditionally connected to these phenomenological, sensory attributes. Worse, digital data is famously replicable, transferable, and shareable beyond the bounds of our senses; we are not immediately threatened by third-party access to data because its promiscuity is, on a visceral level, unrealized and so in some sense unreal to our everyday lived experience (Stark and Tierney 2013).

These data are part of what legal scholar Ian Kerr terms the set of our personal "emanations" (Kerr and McGill 2007), informational ephemera shed inadvertently during the course of everyday life. Such data rarely seem worthy of notice, and the intangibility of data prompts users to feel less strongly about the fate of particular digital artifacts than they would material ones. Consider a thought experiment: Print out twenty of your favorite digital photographs, place them in a photo album, and then go about setting the album on fire. Even though there are still digital copies of these photographs in your possession, the investment in a material iteration will still likely prompt you to hesitate before lighting the match. Different types of data do prompt differing emotional responses based on content, context, and situation: Your digital photo library means more to you viscerally and emotionally than the particular copy of Microsoft Word or Adobe Acrobat running on your computer, just as the material on your Facebook profile might become particularly socially and emotionally charged after a breakup or a death (Gershon 2010). Yet as numerous scholars exploring the implications of Big Data analytics have observed, it is often the aggregation of multiple data points culled from our routine interactions with digital devices of all sorts that are both most ineffable, and most effective in abrogating privacy and enabling widespread surveillance (boyd and Crawford 2012; Cohen 2013)—and these are precisely the data in which we have the least visceral, least emotional investment.

The heterogeneous emotional responses prompted by different categories of personal information can give rise to what one might term "data myopia": the inability to see the "big picture" forest of comprehensive data profiling through the trees of our own particular, partial experiences of sharing personal information in a limited way. Because individual experience does not always feel unsafe, users are viscerally disengaged from the seemingly abstract dangers of data collection and aggregation, even if they know such risks exist. Our lack of felt connection to the aggregation of our everyday data, and our resulting data myopia, influence our broader attitudes toward information privacy and the appropriate flows of our personal information at a societal level.

Much of the time, our embodied interactions with our devices seem, if not entirely personal and private, then at least adequately "contextual." As Pew's research suggests, users do have some knowledge about cookies, third-party data brokers, and many other threats to privacy online; the Snowden revelations have also raised general awareness about digital privacy and surveillance (Madden 2014). Users do whatever they feel they can to protect themselves from these threats; nonetheless, the machinations of Big Data analytics seem disconnected—thus far—from the emotional landscape of everyday life, and thus not something that it is possible to devote too much worry about. Once a person becomes a victim of a phishing scheme or other form of online fraud, concerns around online privacy do tend to increase, as do the actions taken to protect one's personal data. This awareness of information privacy threats, and a desire to protect oneself against them, is also generational: In Pew's study, young adults aged 18–29 were most likely to have taken concrete steps to protect their information privacy from hackers, advertisers, and others (Rainie et al. 2013). Yet in general, it is difficult to know whether the flow of our information is emotionally appropriate if we have no emotional connection whatsoever to the flow itself; for users less familiar with the embodied experience of digital life, these flows often remain mysterious.

Making data, and privacy, visceral

In 1890, lawyer Samuel D. Warren and future Supreme Court Justice Louis D. Brandeis wrote "The Right to Privacy," a piece so seminal and familiar to American privacy scholarship that its ongoing intellectual generativity can be overlooked (Warren and Brandeis 1984). The topic of emotion is a case in point. Warren and Brandeis contend that emotion has always played a prominent part in the concept of personal identity: It was "regard for human emotions," the authors declare, which "soon extended the scope of personal immunity beyond the body of the individual" and into legal remedies such as nuisance law, slander, and libel (75). Warren and Brandeis suggest a civil law privacy tort precisely because it is a remedy to insure the law can accommodate "compensation … granted for mere injury to the feelings" (78). And while a hundred years of American civil law have focused on the relationship between privacy and property, Warren and Brandeis are just as invested in the link between privacy and emotion. "If, then," the authors write in regard to intellectual property cases, there is "a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression" (82). The broader principle of Warren and Brandeis's argument is clear: that, "emotions and sensations demanded legal recognition" (76). The individual to be safeguarded through the authors' famous formulation of "the right to one's personality" is an explicitly emotional person.

The privation implicit in the word "privacy" is a sensory and embodied privation: We have the right, according to Warren and Brandeis, not to be seen when we do not wish to be seen or where we do not wish to be seen, not to be overheard in private conversations, and not to be interfered with in our thinking and feeling persons. Yet in a peculiar reversal, contemporary digital technologies often seem overly invasive precisely because ephemeral data about ourselves are kept private from us: We do not see its accumulation, we do not feel its impact, and we do not know if it is being used "appropriately" or not. Users do not feel data's use and abuse unless that use and abuse is amplified or mobilized to interfere with them in a material way, such as embarrassment, arrest, or imprisonment. And both corporations and governments work hard to keep the emotional impact of the data they possess about us at a minimum. A phenomenon that I term the “notorious/nobody dichotomy” frequently comes into play within public debates about these institutional privacy violations: Users are either singled out for extreme positive or negative attention, or convinced that because they are so unimportant in the great mass of the anonymous, aggregated data, they have ”nothing to fear.” Sometimes, as Daniel Solove’s work illustrates, these strategies are used coincidently at the same time (Solove 2007).

Yet the lack of care with which large institutions treat our data speaks to how little these organizations are concerned with its day-to-day abuse, and how extremely anxious they are about its unauthorized, and therefore emotionally resonant, release. Online collective Anonymous has claimed to have hacked the databases of companies such as Sony, and released users’ nonsensitive personal information, in order to expose poor corporate security practices (Meyers 2011). These hacking incidents have prompted considerable institutional and law enforcement pushback against Anonymous, without much action to foster or impose better standards for corporate data security. The concern of these large institutions seems not to be about the security of data per se, but for the management of public feelings about information privacy, and by extension the possible pressure for regulatory and legal remedy, that are often divorced from the technical reality. Trust is at the heart of the confidence with which we shop online, provide information to the government, and leave ourselves exposed to the web of data mining and data analysis rapidly forming around us (Benkler and Nissenbaum 2006). Yet the notion of trust is replete with emotional resonances that can be encouraged by these large actors through conscious rhetorical strategies quite different from their actual practices. The institutions that manage our data thus have every incentive to suppress or disinhibit negative visceral reactions to information privacy breaches and similar incidents—witness the outraged description of retailer Target’s predictive marketing algorithms, designed to target expectant mothers, as “creepy,” a often-used term that captures the mix of emotional and visceral repulsion a loss of trust provokes (Duhigg 2012).

In light of the intimate connections between our feelings, our data, and ourselves, what can be done to carry the body’s emotional insights into the practical world of technical, regulatory, policy, and design work on information privacy? How can we as individual users feel close enough to our data to make the awareness of information privacy an emotional, even visceral experience? Two design strategies have predominated in attempting to provide technical answers for privacy protection (Hoepman 2014). Interpreted through an analytic lens focusing on emotions, these can be described as (a) provoking users to feel more attached to their personal data, and thus more inclined to consider its appropriate use from an emotional as well as a cognitive perspective; and (b) to separate identifiable data from users, and ensure information possessed by external entities is less tied to our bodies, selves, and the things we care about. Encryption—binding data with individual private keys—is exemplary of the first category, bringing data more closely into our emotional, embodied, and individual spheres of subjectivity; anonymization, on the other hand, aims to separate data from its pointers to our individuality (Spiekermann and Cranor 2009; Dwork and Mulligan 2013). Both encryption and anonymization have faced technical and logistical challenges; moreover, a focus on privacy as context makes it clear that neither technique is useful or appropriate at all times or in all situations (de Montjoye et al. 2015). While the most comprehensively “private” technical systems will make use of both encryption and anonymization deployed together, these techniques are not enough, even in tandem, when applied sparsely or inconsistently. One stronger technical solution would be to design systems that make anonymization and encryption bedrock principles, values assumed to be vital to the root user experience prior to anything else—one such system is Calyx Internet Access, founded by Nicholas Merrill in an attempt to build a privacy-oriented browser from the ground up (McCullagh 2012).

A third, more speculative approach builds on the principles of what Donald Norman terms “visceral design.” In the 2005 *Emotional Design*, Norman suggests that design elicits an emotional response at three different registers: the visceral level, the behavioral level, and the reflective level. While the reflective level connects a design with our cognitive responses and the behavioral level tracks to how we actively use a product, a design’s visceral level consists of its “look, feel and sound,” the materiality of an artifact as it is deployed to enable the artifact’s intended function. Norman assigns viscerality to the realm of appearance and sensation, where “heft” and “sensuality,” “shape and form matter” (Norman 2005, 69). Norman claims that humans “are exquisitely attuned to receive powerful emotional signals from the environment that get interpreted automatically at the visceral level,” at the level of affective response (65). Instead of endorsing Norman’s somewhat reductive classification in its entirety, I suggest visceral design can be understood more broadly in relation to the interactionist model of emotion in HCI already described. As such, I advocate for making privacy visceral through interaction and form-factor design across multiple senses. This vision of "visceral privacy" entails agreement between a user's subjective sense of information privacy and the objective material conditions of that user's data.

Seeing and hearing are the faculties most explicitly and consistently engaged with by information technologists and interaction designers, particularly in terms of the machine/human interaction (Friedberg 2009). Yet designers of information technologies have also implicitly engaged with two other human senses: the physical sensation of touch, and emotions—the "feel" and the "feeling." The historical advent of personal computing entailed an industry need to translate the robustly material fields of ergonomics and human kinetics into design principles enabling the comfortable manipulation of digital data by a range of users; today, haptic interfaces and wearable computing are major growth areas in commercial product development, and smell and taste are also being explored with increasing frequency in interface design studies (Brave and Dahley 1997; Obrist et al. 2014; Feldman and Kuber 2015). Engaging the senses of taste and smell through information technology has never been commercially successful, though not for lack of trying; recent product developments (Broverman 2013; Scentee 2013) may indicate renewed interest.

How to translate these design insights into interactive systems that make manifest the emotional dynamics of information privacy is a difficult yet stimulating challenge. Like gesture and touch, emotions have also long implicitly been of interest to the designers, producers, and marketers of various information technologies—but not always in a critical or emancipatory way. The material objects and marketing strategies for twentieth-century media technologies such as radio and television set were saturated with appeals to both the physicality and emotional charge of a device and its context of use. Appeals to emotion and touch have often gone hand in hand: The relationship between the depictions of bodies and media artifacts has long been carefully choreographed in consumer advertising. Manufacturers of consumer electronics continue to seek to influence both the particular contexts in which their products might be used, and how we as users feel and think about those contexts in turn.

The next frontier in privacy by design is to turn this engagement toward emotion on its head: By developing user interfaces that exploit haptic and aromatic technologies alongside visual and auditory strategies, digital objects can provoke a reflective emotional response tied to the user's visceral sense of privacy. Methodologies such as critical design and reflective design (Dunne and Raby 2005; Sengers et al. 2005) have a key role to play in envisioning prototype technologies that explore this practice of what I call "data visceralization"—making the tie between our feelings and our data visible, tangible, and emotionally appreciable (Stark 2014). The Pavlov Poke project is a strong example of the type of design work scholars might pursue as part of a move toward making visceral design a critical analytic tool in information privacy studies. These sorts of systems should range from proof-of-concept systems intended to jolt us into a new, and perhaps more critical, understanding of privacy's salience to consumer-grade products and services available to a wide range of users. Yet overall, a commitment to the concept of visceral privacy must involve focusing on how digital tools and technologies can work to help make abstract information have both a meaningful visceral and reflective impact on users.

Integrating the new technical and design strategies described in the preceding with novel policy and regulatory solutions is the final, and most complicated, piece in adding emotional context to the information privacy puzzle. As Nissenbaum (2011a) observes, law and technology are deployed together to mutually reinforcing regulatory effect in a number of online activities, including the enforcement of intellectual property and copyright law. For law and technology to work effectively together to safeguard information privacy's emotional context, more attention will need to be paid to the specific situations in which each shapes human experience through the affordances of particular technological objects. Conceptual, technical, and policy protections intended to safeguard our information privacy will fail if they do not acknowledge and meaningfully engage within their design and implementation with the emotional contexts, and material, embodied patterns of action, through which people feel more or less private (Taslitz 2002).

Information scholar Katie Shilton has written persuasively on the importance of what she terms "values levers": "practices that pry open discussions about values in design and help [to] build consensus around social values as design criteria" (Shilton 2013, 376). These moments of sociotechnical contestation facilitate elucidation of, and reflection on, shared social values like privacy, and their subsequent translation into concrete design decisions. Attention to the emotional context of information privacy can and should act as a central value lever in current debates around how to safeguard our autonomy and self-determination within a connected world. Here is considerable scope for further ethnographic research mapping the emotional complexities of how we apprehend our own information privacy, and how our feelings shape thoughts, habits and behaviors in our interaction with digital media. Recent works on how young people experience information privacy are models for this type of scholarship (Gershon 2010; boyd and Marwick 2011; Hasinoff and Shepherd 2014). Drawing out the ties between our private selves, our feelings, and the devices we use every day is difficult precisely because these embodied connections have often been felt but not articulated. In tracing the links between information privacy, human emotion, and digital media, I urge scholars, policymakers, and the public to overcome their sense of data myopia, and to feel the urgency of information privacy in the gut.

Acknowledgments

This research has benefited enormously from the generous comments and constructive suggestions of a great number of people. These contributors include the participants of the NYU Privacy Research Group, notably Helen Nissenbaum, Kathy Strandberg, Karen Levy, Solon Barocas, Kate Crawford, Jason Schultz, and Felix Wu; members of the ISTC–Social Labor and Technology reading group, including Winnie Posner, Marisa Cohn, Ellie Harmon, Lilly Irani, Lilly Nguyen, Courtney Loder, and Norma Möllers; Tarleton Gillespie, Jeff Bardzell, and Mic Bowman; the organizers of the 2014 Privacy Law Scholars Conference (PLSC); PLSC participants Nora Mari, Alan Rubel, Catherine Dwyer, Kate Crawford, David Gray, and Cheryl Brown; incisive feedback (and generous PLSC moderation) from Dawn Schrader; input from members of Future of Networked Privacy Workshop at ACM CSCW 2015, in particular Jen King, Louise Barkhuus, Jessica Vitak, Patrick Gage Kelley; and several anonymous reviewers.

Funding

This work has been supported by funding from the National Science Foundation (NSF) EAGER: Values in Design in the Future Internet Architecture (CNS/Nets 1058333) and EAGER: Values in Design in the Future Internet Architecture—Next Phase (CNS 1355398) grants, and by awards from New York University's Provost's Global Research Initiatives and Steinhardt School of Culture, Education, and Human Development.

Notes

1. This problem is nicely exemplified by an exchange between Daniel J. Solove and Ann Bartow on the occasion of the 2006 publication of Solove's now-canonical article "A Taxonomy of Privacy" (2006a). In response, Bartow faulted Solove's taxonomy for, in her words, suffering "from too much doctrine, and not enough dead bodies" (2006, 52). Chiding Solove for having produced for an overly dry schema of little practical use, Bartow declared that "a more effective taxonomy would dramatically and thoroughly document the consequences of privacy violations in very visceral, dramatic ways" (61). Nonetheless, Bartow herself provided only a few "real-world" cases of information privacy harms. In reply, Solove protested that the point of his original piece had not been to "spark the reader's anger or concern"; rather, Solove defended his taxonomy as a descriptive model to elucidate how "privacy is much more than just 'feelings of unease' … even if it doesn't involve oozing blood, financial ruin, or outrageous humiliation" (2006b, online). Both Solove and Bartow were in apparent agreement that visceral human feeling is central to even the most quotidian concerns around information privacy. Yet neither examined the close connection between information privacy and feelings, uneasy or not, in depth. One major exception to the general lack of interest in emotion and privacy in the law is Taslitz's 2002 article, which suggests recasting the Fourth Amendment in affective terms.
2. Hochschild (2003) suggests that emotion can be understood as a sixth human sense, connected to but also standing apart from the traditional five. The senses are a helpful framework within which to consider our emotions: Often triggered by smells, sights, touch, tastes, and sounds, our feelings help us interpret the world around us, and in doing shape our actions, behaviors and perceptions of the world in return.
3. Perhaps the most poignant and unsettling recent example of this human tendency toward anthropomorphic projection comes from research by the University of Washington's Julie Carpenter: soldiers mourning the loss of military bomb-disposal robots as if they were fallen comrades. "'Those goddamn Mahdi Army scum took him from this world far too early,'" one soldier posted to an online chat room; "'I am sorry for your loss,'" another wrote in reply (Waldman 2013, online).
4. The Pew survey does not distinguish between Internet usage on a desktop computer or on a smartphone.

References

Abu-Lughod, L., and C. A. Lutz. 1990. Introduction: Emotion, discourse, and the politics of everyday life. In *Language and the politics of emotion*, ed. C. A Lutz and L. Abu-Lughod, 1–23. Cambridge, UK: Cambridge University Press.

Acquisti, A. 2012. Privacy and market failures: Three reasons for concern, and three reasons for hope. *Journal on Telecommunications & High Technology Law* 10:227–33.

Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy* 3 (1):26–33. http://dx.doi.org/10.1109/MSP.2005.22.

Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347 (6221):509–14. http://dx.doi.org/10.1126/science.aaa1465.

Altman, I. 1977. Privacy regulation: Culturally universal or culturally specific. *Journal of Social Issues* 33 (3):66–84.

Andrejevic, M. 2013. *Infoglut: How too much information is changing the way we think and know*. New York, NY: Routledge.

Andrews, L. 2012. *I know who you are and i saw what you did: Social networks and the death of privacy*. New York, NY: Free Press.

Balebako, R. J. Jung, W. Lu, L. F. Cranor, and C. Nguyen. 2013. 'Little brothers watching you': Raising awareness of data leaks on smartphones. *SOUPS '13 Proceedings of the ninth symposium on usable privacy and security*. New York, NY: ACM. http://dx.doi.org/10.1145/2501604.2501616.

Barocas, S., and A. D. Selbst. (in press). Big data's disparate impact. *California Law Review* 104.

Barocas, S., and H. Nissenbaum. 2009. On notice: The trouble with notice and consent. Paper presented at the Engaging Data Forum: The First International Forum on the Application and Management of Personal Electronic Information, Cambridge MA, October.

Bartow, A. 2006. A feeling of unease about privacy law. *University of Pennsylvania Law Review* 155:52–62.

Bellanova, R. 2011. Waiting for the barbarians or shaping new societies? A review of Helen Nissenbaum's *Privacy in Context*. *Information Polity* 16:391–5. http://dx.doi.org/10.3233/IP-2011-0257.

Benkler, Y., and H. Nissenbaum. 2006. Commons-based peer production and virtue. *Journal of Political Philosophy* 14 (4):394–419.

Boehner, K., R. DePaula, P. Dourish, and P. Sengers. 2007. How emotion is made and measured. *International Journal of Human-Computer Studies* 65:275–91. http://dx.doi.org/10.1016/j.ijhcs.2006.11.016.

Boyd, D., and A. E. Marwick. 2011. Social privacy in networked publics: Teens' attitudes, practices, and strategies. Paper presented at A Decade in Internet Time: Symposium on the Dynamics of the Internet and Society, Oxford, UK, September. SSRN: http://ssrn.com/abstract=1925128.

Boyd, D., and K. Crawford. 2012. Critical questions for big data. *Information, Communication & Society* 15 (5):662–79. http://dx.doi.org/10.1080/1369118X.2012.678878.

Brave, S., and A. Dahley. 1997. inTouch: A medium for haptic interpersonal communication. In *Proceedings of CHI EA CHI '97 Extended abstracts on human factors in computing systems*, 363–64. New York, NY: ACM. http://dx.doi.org/10.1145/1120212.1120435.

Broverman, A. 2013. What does data taste like? *CBCradio.com*. http://www.cbc.ca/radio/spark/226-falling-in-love-with-artificial-intelligence-context-aware-computing-and-common-ground-soldiers-and-robots-the-beauty-of-glitch-art-1.2847901/what-does-data-taste-like-1.2847904 (accessed July 31, 2015).

Cohen, J. E. 2000. Examined lives: Informational privacy and the subject as object. *Stanford Law Review Online* 52 (5):1373–1438.

Cohen, J. E. 2013. What privacy is for. *Harvard Law Review* 126:1904–33.

Cranor, L. F. 2012. Necessary but not sufficient: Standardized mechanisms for privacy notice and choice. *Journal on Telecommunications & High Technology Law* 10:273–308.

de Montjoye, Y.-A., L. Radaelli, V. K. Singh, and A. S. Pentland. 2015. Unique in the shopping mall: On the reidentifiability of credit card metadata. *Science* 347 (6221):536–9. http://dx.doi.org/10.1126/science.1256297.

Dimos, J. 2012. 3 Apps for mood tracking. *Thebestlife.com*. http://www.thebestlife.com/3-apps-for-mood-tracking (accessed July 31, 2015).

Dourish, P. 2004. Social computing. In *Where the action is: The foundations of embodied interaction*, 55–97. Cambridge, MA: MIT Press.

Dourish, P., J. Brewer, and G. Bell. 2005. Information as a cultural category. *Interactions* 12 (4): 31–3.

Dror, O. E. 2001. Counting the affects: Discoursing in numbers. *Social Research* 68 (2):357–78.

Duhigg, C. 2012. How companies learn your secrets. *NYTimes.com*. http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html (accessed July 31, 2015).

Dunne, A., and F. Raby. 2005. Towards a critical design: Consuming monsters: Big, perfect, infectious (Catalogue essay). Paris, France: Le Design Aujourd'hui, Centre Pompidou. http://www.dunneandraby.co.uk/content/bydandr/42/0 (accessed August 5, 2015).

Dwork, C., and D. K. Mulligan. 2013. It's not privacy, and it's not fair. *Stanford Law Review Online* 66:35–40.

Ekman, P., and W. V. Friesen. 1971. Constants across cultures in the face and emotion. *Journal of Personality and Social Psychology* 17 (2):124–9.

Feldman, P., and R. Kuber. 2015. Tangibly enhancing haptics. In *TEI '15 Proceedings of the Ninth International Conference on Tangible, Embedded, and Embodied Interaction*, 563–68. New York, NY: ACM. http://dx.doi.org/10.1145/2677199.2687903.

Fransman, M. 2002. Mapping the evolving telecoms industry: The uses and shortcomings of the layer model. *Telecommunications Policy* 26 (9–10):473–83.

Friedberg, A. 2009. *The virtual window: From Alberti to Microsoft*. Cambridge, MA: MIT Press.

Garvin, L. T. 1998. Adequate assurance of performance: Of risk, duress, and cognition. *University of Colorado Law Review* 69:71–174.

Gay, G., S. Phoebe, K. Boehner, and M. Mateas. 2008. The disenchantment of affect. *Personal and Ubiquitous Computing* 12 (5):347–58. http://dx.doi.org/10.1007/s00779-007-0161-4.

Gershon, I. 2010. *The Breakup 2.0*. Ithaca, NY: Cornell University Press.

Goel, V. 2014. As data overflows online, researchers grapple with ethics. *NYTimes.com*. http://www.nytimes.com/2014/08/13/technology/the-boon-of-online-data-puts-social-science-in-a-quandary.html (accessed July 31, 2015).

Gould, D. 2010. On affect and protest. In *Political emotions*, ed. J. Staiger, A. Cvetkovich and A. Reynolds, 18–44. New York and London: Routledge.

Hasinoff, A. A., and T. Shepherd. 2014. Sexting in context: Privacy norms and expectations. *International Journal of Communication* 8:2932–415.

Heidegger, M. 1972. *On time and being*, trans. J. Stambaugh. New York, NY: Harper & Row.

Hill, K. 2014. Facebook manipulated 689,003 users' emotions for science. *Forbes*. http://www.forbes.com/sites/kashmirhill/2014/06/28/facebook-manipulated-689003-users-emotions-for-science (accessed July 31, 2015).

Hochschild, A. R. 2003. *The managed heart: Commercialization of human feeling*, 2nd ed. Berkeley, CA: University of California Press.

Hoepman, J.-H. 2014. Privacy design strategies. In *ICT systems security and privacy protection*, ed. N. Cuppens-Boulahia, F. Cuppens, S. Jajodia, A. A. El Kalam, and T. Sans, pp. 446–59. Berlin, Germany: Springer. http://dx.doi.org/10.1007/978-3-642-55415-5_38.

Hourcade, J. P., A. Cavoukian, R. Deibert, Lorrie Faith C., and I. Goldberg. 2014. Electronic privacy and surveillance. In *Proceedings of CHI EA '14 CHI '14 extended abstracts on human factors in computing systems*, 1075–80. New York, NY: ACM. http://dx.doi.org/10.1145/2559206.2579403.

Jackson, S. J. 2014. Rethinking repair. In *Media technologies: Essays on communication, materiality, and sociality*, ed.

T. Gillespie, P. J. Boczkowski, and K. A. Foot, 221–40. Cambridge, MA: MIT Press.

Juul, J. 2010. *A casual revolution: Reinventing video games and their players*. Cambridge, MA: MIT Press.

Kerr, I., and J. McGill. 2007. Emanations, snoop dogs and reasonable expectations of privacy. *Criminal Law Quarterly* 52 (3):392–431.

Kramer, A. D. I., J. E. Guillory, and J. T. Hancock. 2014. Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences* 111 (24):8788–90.

Latour, B. 1992. Where are the missing masses? The sociology of a few mundane artifacts. In *Shaping technology/building society: Studies in sociotechnical change*, ed. W. E. Bijker and J. Law, 225–58. Cambridge, MA: MIT Press.

Latour, B. 2005. *Reassembling the social: An introduction to actor-network theory*. New York, NY: Oxford University Press.

Madden, M. 2014. *Public perceptions of privacy and security in the post-Snowden era*. Washington, DC: Pew Research Center.

Massumi, B. 2010. The future birth of the affective fact. In *The affect theory reader*, ed. M. Gregg and G. J. Seigworth, 52–71. Durham, NC: Duke University Press.

McCullagh, D. 2012. This Internet provider pledges to put your privacy first. Always. *CNET News.com.* http://www.cnet.com/news/this-internet-provider-pledges-to-put-your-privacy-first-always (accessed July 31, 2015).

Meschtscherjakov, A., D. Wilfinger, and M. Tscheligi. 2014. Mobile attachment causes and consequences for emotional bonding with mobile phones. In *CHI '14 proceedings of the SIGCHI conference on human factors in computing systems*, 2317–2326. New York, NY: ACM.

Meyers, M. 2011. Report details extent of anonymous hack on stratfor. *CNET News.com*. http://news.cnet.com/8301-1009_3-57348995-83/report-details-extent-of-anonymous-hack-on-stratfor/ (accessed July 31, 2015).

Montfort, N., and I. Bogost. 2009. Random and raster: Display technologies and the development of videogames. *IEEE Annals of the History of Computing* 31(3), 34–43.

Morris, R. R, and D. McDuff. 2013. Pavlov poke. *www.robertrmorris.org*. http://www.robertrmorris.org/pavlovpoke (accessed November 23, 2014).

Nass, C., J. Steuer, and E. R. Tauber. 1994. Computers are social actors. In *CHI '94 proceedings of the SIGCHI conference on human factors in computing systems*, 72–78. New York, NY: ACM.

Nippert-Eng, C. 2007. Privacy in the United States: Some implications for design. *International Journal of Design* 1 (2):1–11.

Nippert-Eng, C. 2010. *Islands of privacy*. Chicago, IL: University of Chicago Press.

Nissenbaum, H. 2011a. From preemption to circumvention. *Berkeley Technology Law Journal* 26 (3):1367–86.

Nissenbaum, H. 2011b. A contextual approach to privacy online. *Daedalus* 140 (4):32–48.

Nissenbaum, H., and K. Varnelis. 2012. *Modulated cities: Networked spaces, reconstituted subjects* (Situated Technologies Pamphlets 9). New York, NY: Architectural League of New York.

Norman, D. A. 1989. *The design of everyday things*. New York, NY: Currency and Doubleday.

Norman, D. A. 2005. *Emotional design: Why we love (or hate) everyday things*. New York, NY: Basic Books.

Obrist, M., R. Comber, S. Subramanian, B. Piqueras-Fiszman, C. Velasco, and C. Spence. 2014. Temporal, affective, and embodied characteristics of taste experiences: A framework for design. In *CHI '14 proceedings of the SIGCHI conference on human factors in computing systems*, 2853–62. New York, NY: ACM. http://dx.doi.org/10.1145/2556288.2557007.

Pasquale, F. 2010. Reputation regulation: Disclosure and the challenge of clandestinely commensurating computing. In *The offensive Internet: Privacy, speech, and reputation*, ed. S. Levmore and M. C. Nussbaum, 106–23. Cambridge, MA: Harvard University Press.

Picard, R. W. 2000. *Affective computing*. Cambridge, MA: The MIT Press.

Prinz, J. J. 2004. *Gut reactions: A perceptual theory of emotion*. Oxford, UK: Oxford University Press.

Purpura, S., V. Schwanda, K. Williams, W. Stubler, and P. Sengers. 2011. Fit4Life: The design of a persuasive technology promoting healthy behavior and ideal weight. In *CHI '11 proceedings of the SIGCHI conference on human factors in computing systems*, 423–432. New York, NY: ACM.

Rainie, L., S. Kiesler, R. Kang, and M. Madden. 2013. *Anonymity, privacy, and security online*. Washington, DC: Pew Research Center's Internet & American Life Project. http://pewinternet.org/Reports/2013/Anonymity-online.aspx (accessed July 31, 2015).

Rodriguez, S. 2012. Apple devices upgraded to iOS 6 spike 29% after Google Maps release. *Los Angeles Times*, December 9. http://articles.latimes.com/2012/dec/19/business/la-fi-tn-apple-ios-6-spike-google-maps-20121219 (accessed July 31, 2015).

Sahakian, B., A. Lawrence, L. Clark, J. N. Labuzetta, and S. Vyakarnum. 2008. The innovative brain. *Nature* 456:168–69.

Scentee. 2013. Scentee. www.scentee.com. http://www.scentee.com

Schneier, B. 2013. The Internet is a surveillance state. *CNN.com*, March 16. http://www.cnn.com/2013/03/16/opinion/schneier-internet-surveillance (accessed July 31, 2015).

Sengers, P., K. Boehner, S. David, and J. J. Kaye. 2005. Reflective design. In *CC '05 Proceedings of the 4th Decennial Conference on Critical Computing: Between Sense and Sensibility*, 49–58. New York, NY: ACM. http://dx.doi.org/10.1145/1094562.1094569.

Sennett, R. 2009. *The craftsman*. New Haven, CT: Yale University Press.

Shilton, K. 2013. Values levers: Building ethics into design. *Science, Technology, & Human Values* 38 (3):374–97. http://dx.doi.org/10.1177/0162243912436985.

Solove, D. J. 2006a. A taxonomy of privacy. *University of Pennsylvania Law Review* 154 (3):477–564.

Solove, D. J. 2006b. A reply to Ann Bartow's response to *A Taxonomy of Privacy*. *ConcurringOpinions.com*, September 6. http://www.concurringopinions.com/archives/2006/09/a_reply_to_bart.html (accessed July 31, 2015).

Solove, D. J. 2007. *The future of reputation*. New Haven, CT: Yale University Press.

Solum, L. B., and M. Chung. 2003. *The layers principle: Internet architecture and the law* (Public Law and Legal Theory Research Paper 55). San Diego, CA: University of San Diego School of Law.

Spiekermann, S., and L. F. Cranor. 2009. Engineering privacy. *IEEE Transactions on Software Engineering* 35 (1):67–82. http://dx.doi.org/10.1109/TSE.2008.88.

Stark, L. 2014. Come on feel the data (and smell it). *The Atlantic*, May 19. http://www.theatlantic.com/technology/archive/2014/05/data-visceralization/370899 (accessed July 31, 2015).

Stark, L., and M. Tierney. 2013. Lockbox: Mobility, privacy and values in cloud storage. *Ethics and Information Technology* 16:1–13. http://dx.doi.org/10.1007/s10676-013-9328-z.

Taslitz, A. E. 2002. The fourth amendment in the twenty-first century: Technology, privacy, and human emotions. *Law and Contemporary Problems* 65 (2):125–87.

The Economist. 2010. Data, data everywhere. *Economist.com*, February 25. http://www.economist.com/node/15557443 (accessed July 31, 2015).

Turkle, S. 2007. What makes an object evocative? In *Evocative objects: Things we think with*, ed. S. Turkle, 307–27. Cambridge, MA: MIT Press.

Turkle, S. 2011. *Alone together: Why we expect more from technology and less from each other*. New York, NY: Basic Books.

Versace, C. 2013. Forget mobile payments, Visa and American Express: Here comes the Google Wallet card. *Forbes.com*. http://www.forbes.com/sites/chrisversace/2013/11/25/forget-mobile-payments-visa-and-american-express-here-comes-the-google-wallet-card (accessed November 25, 2015).

Waldman, K. 2013. Are soldiers too emotionally attached to military robots? *Slate*, September 20. http://www.slate.com/blogs/future_tense/2013/09/20/military_bots_inspire_strong_emotional_connections_in_troops_is_that_bad.html (accessed July 31, 2015).

Wang, Y., P. G. Leon, A. Acquisti, L. F. Cranor, A. Forget, and N. Sadeh. 2014. A field trial of privacy nudges for facebook. In *CHI '14 proceedings of the SIGCHI conference on human factors in computing systems*, 2367–76. New York, NY: ACM. http://dx.doi.org/10.1145/2556288.2557413.

Wang, Y., S. Komanduri, Pedro Giovanni L., G. Norcie, A. Acquisti, and L. F. Cranor. 2011. 'I regretted the minute I pressed share': A qualitative study of regrets on Facebook. Paper presented at Symposium on Usable Privacy and Security (SOUPS) 2011, July 20–22, Pittsburgh, PA.

Warren, S. D., and L. D. Brandeis. 1984. The right to privacy [The implicit made explicit]. In *Philosophical dimensions of privacy: An anthology*, ed. F. Schoeman, 75–103. Cambridge, UK: Cambridge University Press.

Wax, E. 2013. Beat-up cellphones with cracked screens are point of pride for some young people. *Washington Post*, May 17. http://articles.washingtonpost.com/2013-05-17/lifestyle/39333160_1_screen-iphone-lofton (July 31, 2015).