Editors: Fred Cate, fcate@indiana.edu
Ben Laurie, ben@links.org

Deconstructing the Privacy Experience

Betsy Masiello
Google

Today's privacy dialogue often lacks attention to what should be a primary goal: informing the central tenets of product design. Conversations that center around opt-in versus opt-out, privacy policies, sensitive data, encryption, and retention periods tend to fade into a fog of legalese, often without tackling fundamental design challenges. Privacy today is hard. We need to make it simple.

We've long focused on transparency and choice as the pillars on which privacy rests because together they enable informed consent to data collection. On their own, however, transparency and choice say nothing about creating a usable privacy experience. Enabling informed consent to data collection isn't enough; product designers must aspire to this and more: enable informed consent without burdening user experience.

Deconstructing the privacy experiences available on today's social Web is a first step in engaging in a rich and nuanced dialogue about digital privacy. It quickly becomes apparent that the challenges ahead aren't focused on data collection—indeed, the reality is that we will continue to put data online and derive infinite utility from doing so. Instead, the challenge is how to build an authentic experience, enable meaningful choices, and make transparency accessible to the average user.

The Importance of Authentic Design

Twitter, a darling of the social Web, is a young enough service that it's undoubtedly still refining the privacy experience it offers. On the surface, this experience is quite simple: users set their accounts to be either public or private, and that setting covers all tweets sent from those accounts. Nonetheless, in some ways the experience is inauthentic—it doesn't always behave as expected, a quality that has ramifications for average users' privacy expectations.

This behavior manifests in two ways: first, public tweets are permanent, not ephemeral as we often experience them; second, you can't delete public tweets, despite the trashcan icon that indicates otherwise. Two students in MIT's 2008 class, in their capstone paper, "Ethics and Law on the Electronic Frontier," explored these facts; you can easily test their assertions yourself.[1]

Using Twitter, it's possible to feel like a tweet can be forever lost as quickly as the digital conversation evolves. This ephemeral nature might inspire users to share more information than they otherwise would, experiencing the harsh reality that most of what we say and do isn't important enough to get much attention. Yet, once expressed on a public Twitter feed, information is permanently accessible on the Web. This mismatch of expectation and reality is at the crux of the privacy design challenges that lay ahead.

An example from my personal feed illustrates the implications of Twitter's design for privacy. On 22 January 2009 at 3:01 p.m., jessicatornwald posted a tweet containing details about both her sex life and mental health in less than 140 characters. jessicatornwald had, at the time, relatively few followers by Twitter standards (roughly 35), but her tweets are public and thus available to the entire Internet. Her username is actually her real name (although obfuscated here), and she has a photo of herself on her profile. Although Twitter is a pseudonymous service, jessicatornwald is not tweeting under a pseudonym. And in one quick instant, she publicly and identifiably referenced both her sex life and therapy experience, content many of us consider private.

Ironically and tellingly, jessicatornwald requested that I obfuscate her username in this column to protect her future job prospects. (As of June 2009, no user by the name of jessicatornwald actually exists on Twitter.) Her request was surprisingly blunt: "Just keep me anonymous at all costs." Clearly, jessicatornwald does care about privacy, but Twitter has created a medium in which she's willing to share private information publicly. Notably, keeping her anonymous requires that I not even quote the tweet because doing so would let readers search for her identity.

The Paradox of Choice

Our definitions of privacy are continuously evolving, so it always seems appropriate to offer a new one. I'd like to suggest that the right to privacy in the 21st century is the right to not be mischaracterized, unsettled, or surprised by what personal information and communications about you are publicly available on the Web.

At the core of enabling privacy in this context is an authentic privacy experience, one that's as expected. Achieving this authenticity is such a challenge that few products and services, if any, come to mind as having fully done so, although equally few products and services have intentionally lied. Google, FriendFeed, Facebook, MySpace—we can view all these companies as having some design aspect that's not authentic, that requires too much work on the user's part to understand. Authentic privacy design is elusive not by any fault of our own but because it's an evergreen problem requiring engineering innovation.

Take, for example, the array of granular privacy controls available on Facebook, a service that's been both lauded and criticized for its privacy design. Facebook users can choose to share their personal data in numerous ways, a design choice that causes some to ask if it might be too much of a good thing. The conclusions to this train of thought, however, should be troubling to those of us who care about digital privacy.

Randall Stross of the *New York Times* made similar observations in a recent column (www.nytimes.com/2009/03/08/business/08digi.html). Stross drew the following conclusion: "When the distinction blurs between one's few close friends and the many who are not, it seems pointless to distinguish between private and public." Others have drawn similar conclusions, most notably David Brin, author of *The Transparent Society* (Basic Books, 1999). The lesson seems to be, if you want to participate in the social Web, you are best off doing so in a completely transparent way.

The conclusion that because privacy is hard, we should live completely transparent lives seems, to say the least, unsatisfying. Worse, it strips the burden of innovation from engineers. Technology's objective shouldn't be to radically warp our human qualities but to enhance the ways in which we live our fundamentally human lives. I've drawn different lessons from my own Facebook experience: first, social relationships are fluid, and privacy must adapt with them as they shift; second, when choice becomes a burden to manage, it isn't meaningful and might even create new privacy risks.

Engineering Meaningful Choice

To address these issues, we need to begin a dialogue about meaningful choice. Engineers and product designers could apply normative views about which choices users should want control over and which matter less—this might be one way to simplify choice. But this seems either a paternalistic or naïve approach to technology innovation.

One future might include tools that intelligently evolve the privacy choices available and display them in the least burdensome way. Another might include adaptations of features such as Gmail Chat's "off-the-record" feature. Both futures have flaws: they demand considerable trust in the technology, and we face technical limitations in implementing them.

To build tools to effectively negotiate a trustworthy relationship between users will demand attention from the smartest engineers in the world. Even if a product or service gives users meaningful choice, each user must still convey an enormous degree of trust in other users. The Internet has taken gossip and made it authoritative on a scale we haven't begun to comprehend. Mark Zuckerberg, Facebook's CEO, described the challenge on Facebook's blog:

> People want full ownership and control of their information so they can turn off access to it at any time. At the same time, people also want to be able to bring the information others have shared with them … onto other services and grant those services access to those people's information. These two positions are at odds with each other.

This is another undeniable reality we must face—if someone else puts information about you on the Web, it becomes persistent, replicable, and searchable almost immediately. Self-representation is difficult on the Web: rumors spread fast and are perceived as more trustworthy than in the traditional childhood game of "telephone." Engineers have looked for ways to make information become ephemeral or obscured as it is copied, similar to how a statement mutates from start to finish in a game of telephone, but have made little progress. Could we at the very least make digital information's immutable quality more apparent to users, or alternatively assure them that what remains behind a walled garden today will remain there forever?

Enhancing Privacy through Intelligible Transparency

Finally, any privacy discussion must consider the data collection that enables much of today's Internet economy to flourish but is often as obscured as it is pervasive. How do we create transparency that's accessible to average users,

such that their choices are adequately informed? There are two sides to the transaction: first, surfacing data collection as it happens and is used; second, making apparent the value obtained and risk inherent to sharing data. We've made great progress on former but are only beginning to conceptualize the latter.

How do we create transparency that's accessible to average users, such that their choices are adequately informed?

Google's Ads Preferences Manager, launched alongside its interest-based advertising product, made leaps forward in transparency in data collection and use. Cookies have in some ways obscured data collection for average users—although they're stored in the browser and accessible, many users can't interpret the meaning of cookie identifiers and contents. The Ads Preferences Manager has made the difficult easy: users can see their cookie ID, their opt-out status, and the interest categories used to serve them ads on the Google Content Network. We can imagine that future evolutions of this tool might make visible real-time data collection in a browser overlay.

These are remarkable steps forward for transparency, but to suggest this is all the innovation required would be naïve to say the least. During the next round of transparency innovation, we should focus on how to make apparent the value and risk of sharing data.

Companies collect data about users who interact with their Web sites for good reasons. Many are security-related, and many more support business models from which users derive substantial value. In neither case is the value immediately apparent to users. Unlike physical dangers that we can imminently imagine, technical security is harder to justify. And unlike prices for physical goods, understanding what we get in exchange for our data is often difficult. Analogous abstractions exist on the social Web. Unlike the experience of speaking to others in a physical room, it isn't always immediately apparent who is "listening" to our communications on the Web. We must consider how to improve interfaces to the Internet that enable these experiences to be as human-interpretable as their offline equivalents.

Sherry Turkle, director of the MIT Initiative on Technology and Self, wisely noted at a recent conference that, "In democracy today, perhaps we need to start with the assumption that we all have something to hide" (as quoted in danah boyd's Twitter feed on 11 March 2009; www.twitter.com/zephoria). As technologists, we need to respect this basic tenet as a truth, and more directly design solutions that enable hidden corners of our lives. On the social Web, privacy is a global and entirely subjective quality—we each perceive different threats to it. For some, it's government surveillance whereas others fear social embarrassment. Privacy is no longer a wholly legal issue but very much a social one, and the design community should tackle it as such.

I've suggested that we should understand privacy in part as a right to not be mischaracterized, surprised, or unsettled by information available about us on the Web. Among the best rationales I've seen put forth for a more nuanced definition than we've had to date is that we ought to "understand the function of privacy in part to remove the burden of defending private choices" (as Lawrence Lessig told me in a private email correspondence). We could aim to shift the privacy dialogue through social advocacy or by creating laws to regulate the publicly private. Or, we could put in front of our best and brightest engineers a series of design problems to ease average users' burden of defending private choices. The technology community has never waited for permission or requests to build a new future. Why should we wait to build a better privacy experience? □

Acknowledgments

This article reflects the opinions of the author and does not represent an official opinion on the part of her employer.

References

1. X. Xiao and Chris Varenhorst, "Stop the Tweet: Preventing Harm and Embarrassment to Twitter Users," 10 Dec. 2008, http://varenhor.st/papers/tweetshow.pdf.

***Betsy Masiello** is a policy analyst at Google. Her research interests lie at the intersection of information technologies and public policy, including privacy, economic, and telecommunications policies. Masiello has an SM in technology & policy from the Massachusetts Institute of Technology and an MSc in financial economics from Oxford University, where she was a Rhodes Scholar. Contact her at betsym@google.com.*

Interested in writing for this department? Please contact editors Fred Cate (fcate@indiana.edu) and/or Ben Laurie (ben@links.org).

IEEE Security & Privacy **is THE premier magazine for security professionals.**

Top security professionals in the field share information on which you can rely:

- **Silver Bullet podcasts and interviews**
- **Intellectual Property Protection & Piracy**
- **Designing for Infrastructure Security**
- **Privacy Issues**
- **Legal Issues & Cybercrime**
- **Digital Rights Management**
- **The Security Profession**

Visit our Web site at www.computer.org/security/

Subscribe now!

www.computer.org/services/nonmem/spbnr