Privacy and innovation intersect in a variety of ways. For instance, a desire for privacy can spark specific or general innovation. It was the invention of the Hush-A-Phone, after all, a telephone receiver attachment intended to reduce the risk that a conversation would be overheard, that opened the door to device innovation in telephony in the 1950s.¹

An absence of privacy can stifle individual or firm creativity. People are less creative in the moment when they perceive they are being observed² and excessive monitoring may “incline choices toward the bland and the mainstream.”³ (Although Americans perform better each year on IQ tests, our capacity for creativity—like our privacy—appears to be declining.⁴) The law protects trade secrets in part to incentivize the development of intellectual capital.

A careless zeal for privacy could also stifle innovation. Some within academia and industry worry that overly restrictive rules around online consumer privacy will limit the development of novel services.⁵ Thus, for instance, Google may never have developed Flu Trends—a tool that predicts worldwide flu activity by analyzing historical patterns in search queries—were the company banned from retaining user search logs.⁶

¹ See Hush-A-Phone v. United States, 238 F.2d 266 (D.C. Cir. 1956).
⁴ See Po Bronson and Ashley Merryman, “The Creativity Crisis,” NEWSWEEK (Jul. 10, 2010).
⁶ See Comments of Google, Inc., U.S. Department of Energy Request for Information: Implementing the National Broadband Plan by Empowering Consumers and the Smart Grid (Jul. 12, 2010) at *5 (“Google engineers discovered that certain search terms are good indicators of flu activity, and developed Google Flu Trends using aggregated Google search data to estimate flu activity. This allows health officials, the media, and the public to learn about local flu outbreaks sooner than using traditional public health methods. … The value of innovative services like this would be lessened or lost completely by rigid or inconsistent data protection rules.”).
Then there is innovation within the discipline of privacy. Innovation in privacy happens at the level of theory. Daniel Solove’s imaginative new metaphor for privacy in the modern world is one example. Lior Strahilevitz’s recourse to social network theory to assess damages in privacy tort is another.

It also happens at the level of practice. Lorrie Faith Cranor, Helen Nissenbaum, Christopher Soghoian, and others have developed a wonderful array of technologies and standards to help individuals safeguard their information. Web companies have begun in recent years to compete with one another over privacy, including by building better tools of access, choice, and portability. As Reputation Defender and TRUSTe can attest, privacy has become a business model in its own right.

Empirical work around privacy has been particularly enlightening. Qualitative surveys, analyses of complaints, and experimental user studies have shed light on individual understandings and valuations of privacy. We know, for instance, that consumers will pay a premium to purchase goods from websites with better privacy. We also know that when people see the words “privacy policy” on a website—required under California law—they assume without foundation that the website operator will protect their data.

Even after years of creative thought and diligent analysis by researchers and firms, however, or perhaps because of it, entirely new dimensions of privacy continue to emerge. These new dimensions in turn help us understand and process the waves of sea change brought by the rapid evolution of technology and norms.

For example: we are only scratching the surface of the ramifications for privacy of user interface design. In a 1996 study, Lee Sproull and colleagues asked subjects the same set of questions using different website interfaces. The first interface was a normal set of text questions; the second introduced the anthropomorphic element of a human face. The team found that, in the “face” condition, people tended to skip sensitive questions.

---

7 See Daniel Solove, Privacy & Power: Computer Databases and Metaphors for Information Privacy, 53 STAN. L. REV. 1393 (2001) (arguing that Franz Kafka’s The Trial should replace George Orwell’s Nineteen Eighty Four as the dominant metaphor for privacy problems in the modern age).


12 Lee Sproull et al, When the Interface is a Face, 11 HUM.-COMPUTER INTERACTION 97-124, 112-16 (1996).
This year, Alessandro Acquisti and colleagues ran a test where they asked subjects to fill out an online questionnaire about ethics. In one experimental condition, the website had an official seal, a formal font, and a blue and white color scheme. In another, the website had a silly icon of devil and a header reading “R U bad?” The team found that subjects were more willing to self-incriminate where the interface was playful and casual, as opposed to official and formal.13

I believe that these and similar studies have profound repercussions for consumer and citizen privacy. Consider the policy ramifications of Acquisti’s findings. One of the online populations about whom we worry the most is children. Congress was concerned enough that in 1998 it passed a special law—the Children Online Privacy Protection Act—that requires additional notice and consent for commercial websites directed at children.14 Meanwhile, websites aimed at children tend to be the most casual and playful of any on the Internet.

Or consider what Sproull’s finding suggest about the nature of privacy harm. If people react to anthropomorphic or social technology as though a person were really there—and there is extensive evidence that we do15—then such interfaces can interrupt solitude or chill curiosity just as the presence of an actual observer might.16

Human-computer interaction expert Victoria Groom and I are presently working on an experiment comparing the qualitative and behavioral effects of a wide variety of interface specifications. We hope to explore whether the user experience itself can be a kind of “visceral notice,” that is, whether subjects faced with design elements such as anthropomorphism, formality, and self-awareness will report a more accurate understanding of a website’s potential to collect, process, and share information.

It is a very exciting time to work in privacy. We have answers to many questions; we have many questions we would like to see answered. And, every so often, we even find new questions to ask.

15 For instance, people pay for coffee on the honor system more often if a picture of eyes appears above the collection basket. See Melissa Batson et al., Cues of Being Watched Enhance Cooperation in a Real-World Setting, BIOLOGY LETTERS, 2(3):412–14 (2006).