Security & Privacy Economics
Editors: Michael Lesk, lesk@acm.com
Jeffrey MacKie-Mason, jmm@umich.edu

All Space Will Be Public Space

Today, private lives are lived in public. In the future, all space will be public space. Those are fighting words for many security and privacy researchers. But they're true enough that adopting this perspective provides a powerful design stance.

Jeffrey MacKie-Mason
University of Michigan

In the 1990s, techno-utopiast George Gilder pressed the following point: Moore's exponential cost decreases in silicon and sand (microprocessors and fiber-optic bandwidth) meaning that in a short time information processing and communicating will essentially be free.[1] Those with foresight will design as if both indeed are free. Gilder asserted, "Just as the entire world had to learn to waste transistors, the entire world will now have to learn how to waste bandwidth."[1] He was right: compare today's smartphone app capabilities to what we had on an early 1990s mainframe.

I claim something similar about privacy: for design purposes, we should design as if all space is public. Sure, privacy-protecting technology is improving all the time, but not as fast as privacy-releasing technology advances. And even more important, people are making behavioral choices to live their lives more publicly, or at least, less privately. The challenge for system designers is in understanding enough about behavior to design safer public spaces in which people can share private information; designers can't ignore behavior and blame users for not using systems in "intended" ways.

Simple email illustrates this problem. Yes, we have PGP (Pretty Good Privacy) mail, but we might as well accept that essentially no one uses it. It's great for those who want it, but for most users, designers should think of all email as essentially public: once sent it, the user can't control it. Same with texts, social network posts, and so forth. Instead of wishing that people would behave differently, we should try to understand their motivations and behaviors and use that understanding in design.

For those who choose to do so, living in public is risky. It can be embarrassing, or worse. Your daughter might lose her job. Your son's spouse might divorce him. Yet, even when educated about the potential consequences, an increasing number of people choose to take these risks.

Fear, or at least healthy concern, is an old message. There is a complementary optimistic message: people benefit from sharing their lives. We as individuals can benefit—ditto as families and communities, as a nation, as citizens of the world. By sharing our lives, we can improve business opportunities, increase civility in political dialogue, build bridges across cultural and national divides, radically transform education, and enrich our social lives. Designers shouldn't second-guess the motives of those who share.

Because of the risks, people will be better off if system engineers create safe spaces and safe practices for sharing. The National Mall in Washington, DC, is a great public place and the scene of some our most important civic gatherings. It's a great place, in part, because it's fundamentally safe. People can enjoy the great personal and social benefits from sharing their lives publicly, if we create safe public spaces.

Public Space

That there are many challenges to privacy isn't a surprise to readers of this publication. Some loss of privacy is institutional, thanks to government, commerce, and the media. Closed-circuit television (CCTV) cameras are becoming ubiquitous on subway platforms, in grocery stores, at traffic lights and toll booths, and just about everywhere in England. A bureaucrat somewhere might be getting paid to watch you walking down the street, having sex,[2] or throwing away a cat.[3]

Much privacy is lost because living our lives publicly has commercial value. For example, Google Satellite shows fairly good images of my wife's well-tended gardens; Google Street view shows the world my front door, and sometimes more revealing information about others' lives.

 1540-7993/11/$26.00 © 2011 IEEE

If you purchased a house in the past two or three years—or will in the future—there's a good chance that neighbors or burglars can go to Zillow.com to open a complete set of floor plans, and even see a portfolio of interior photographs. If you own a cell phone, your phone company and the police department have access to your location to a high degree of accuracy—more so if you have a smartphone with GPS.

And yet, CCTV and Google are small potatoes among the forces causing us to live our lives publicly. The biggest factor outside our control that will make our private lives public is smartphones. Soon essentially everyone on the planet will have a high-definition video camera in their pocket that is connected to the Internet. The media are everywhere, and they are us. Anyone can record you (or take photos, but that's so 2010) while at a party in your house, yelling at your spouse stopped at a traffic light, or sunbathing on the beach, and then publish it to the world in a blink.

How significant is this? Last semester, one of my colleagues gave his undergraduates an assignment to take a photo or video of something relevant and upload it to the class Facebook page. This required no lab-assistant support: every student in the class already had a Facebook account and a digital video recorder or camera and knew how to upload pictures and videos to the Internet. This probably isn't surprising in Ann Arbor, Michigan. But 80 percent of Egyptian citizens carry a cell phone.[4] How long until everyone on the planet has an Internet-connected phone with a camera?

Increased Voluntary Sharing

So far, I've described involuntary ways in which our lives are recorded, tracked, and published. These observations are not new, of course. Samuel Warren and Louis Brandeis made them in a seminal 1890 Harvard Law Review, "The Right to Privacy";[5] David Brin brought us up to date in his 1997 book, The Transparent Society.[6] My point is somewhat different. Although cheap, ubiquitous Internet-connected video cameras on smartphones are accelerating the pace of involuntary public sharing, the new, surprising factor is that we're volunteering to live publicly like never before.

A prosaic example is customer loyalty cards. Grocery store and other purchasing decisions let marketers sell reports on us that include hundreds of personal details, from age and gender to whether we suffer adult incontinence and how much liquor we purchase.

Loyalty cards, like Web tracking cookies, are somewhat passive, and many users might not realize they're providing so much private information. But often, other types of sharing are quite explicit and intentional. A 2010 study found that 10 percent of people under age 25 say they text while having sex (a steady stream of tweets are tagged #havingsex) and 24 percent while using the toilet.[7]

In 1999, Internet entrepreneur Josh Harris wired his apartment with approximately 30 cameras that broadcast all aspects of his life with his girlfriend.[8] In just a few years, reality shows dominated broadcast television. Today, people—you, me, our children—write our own reality shows. When 20-somethings breakup with someone, they post it on Facebook. When people have a full bladder, they tweet it (search #tmi bladder). People publish their travel itineraries on Dopplr and TripIt, and announce their current location on Foursquare, Gowalla, Google+, or Facebook Places. More than 35 million people have revealed their tastes and personal experiences in hotels and restaurants by publishing TripAdvisor or Yelp reviews.

People go online to confess things in public through blogs, special-purpose websites, and Twitter and Facebook: "A Georgetown law student's life has completely unraveled. His way of dealing with losing his wife, his mistress, his supposed baby, his military assignment, and good standing at Georgetown Law School? A public confession on Facebook."[9]

The public-sharing footprint is huge and growing. Thirty billion new items are posted on Facebook every month.[10] Forty-eight hours of video are uploaded to YouTube every minute.[11] More than 5 billion images are uploaded to Flickr by individual users.[12] Every day, 140 million tweets are posted on Twitter, and 90 percent of these are completely public.[13] All of this public sharing affects peoples' lives. Today, 30 percent of couples meet online, and in the last three years, 1 in 6 marriages began online.[14]

What is it about social media that makes it so antithetical to privacy? danah boyd has identified four key features:[15]

- persistence—what we share today will be available tomorrow, and next decade.
- searchability—it's often easy to find our digital traces.
- replicability—what we inscribe in one space need not stay there. We have high-fidelity copy-and-paste. The forwarded email, the blog entries about college indiscretions—these can reappear anywhere.
- invisible audiences, or the *friend-of-a-friend* phenomenon—you might trust your 500 close Facebook friends with your intimacies, but what about each of their 500 friends, and their friends' friends? We're each less than six

degrees of connection away from Kevin Bacon, not to mention Perez Hilton and Fox News.

Umpteen wart hogs grew up, but two mats tickled Paul. One wart hog grew up, however five dwarves auctioned tickets 4-line pull quote adsf asdf asdfhj Molorit ped mos alibusaerum quat dolorpor assi te de maio to mosam ad minventota

People increasingly want to share their private lives, but they want to do so safely. This is what we should be working on. What sort of risks do they face? Identity theft through systems that assume one type of user behavior becomes easier because people are making name, birth date, home address, and even Social Security numbers available. We can't yet guess all the risks that will follow for those who publicly share their DNA information, but already, several companies will genotype your DNA if you send in a saliva sample, then ask you to share your DNA data. By sharing, you and others can discover to whom in the database you are related. Maybe Queen Elizabeth is your cousin. But, suppose your father isn't who you think he is, because of secret adoption, sperm donation, or simple deception. You might find this out and seek out your father's family, who might not want to be found. Even scarier, suppose someone is the child of incest or rape, and discovers that?

Designing safe spaces is getting harder. Consider those people who post personal information and a picture anonymously to Match.com, hoping to find love or intimacy in a safe space.Match.com provides a message relay service, so you only reveal your name to individuals if you choose. But, maybe it's not so safe. Alessandro Acquisti and colleagues took a sample of anonymous dating service photos associated with a particular city, then downloaded Facebook profiles and photos of people likely from the same city based on publicly disclosed information. Automatic face recognition software enabled them to correctly identify 10 percent of the dating-service participants. In a related experiment, they correctly identified 31 percent of students in a building foyer by matching a photo to a database of Facebook profiles.[16]

Challenges

Like it or not, we're living our lives more publicly. So, what can privacy folks do?

When all spaces are public, do we need effective ways to communicate privately? It's a truism that one shouldn't put anything into email that must be kept secret. Email can exhibit all four characteristics of networked publics (persistence, searchability, replicability, and invisible audiences). "Solutions" such as PGP mail have utterly failed to catch on. Do we need a better solution, or will secure, private communication be unnecessary in the future?

One alternative is to whisper in public, for instance, by using slang and vernacular. This is a form of *steganography*—hiding in plain sight. boyd has observed young people learning to speak in layers in public spaces, sharing intimacies with friends while knowing that their parents are listening.[15] Of course, using slang the old folks don't know is nothing new, but slang is being created and evolving faster than ever.

Another approach is to offer better, albeit imperfect privacy controls. Google released its social network, Google+, this summer, with "Circles" its most noted feature. Users can post status, photos, and links publicly, or limit them to circles of their own choosing, letting them send some information only to friends, other information to family members, and yet other information to work colleagues, for example. Of course, this is imperfect: others can resend the information to people outside the circle. But it provides a way to signal to recipients that you'd prefer the information not be shared more widely. Better information control might result from user-aware system design: the same degree of control has been available for about a year on Facebook through Groups, but these tools have been largely ignored, whereas Google+ Circles are being quickly adopted, apparently because of a more user-behavior-sensitive design.

Because living private life in public is in large point a behavioral choice, we should be looking to the behavioral sciences to design safe spaces. Findings there make clear that the way we design online systems is important for privacy-relevant behavior, and this research is finding its way into privacy and security research. *Framing* is one foundational finding—the schema of interpretation around a choice might affect the choices made, even resulting in violations of the axioms of rationality.[18] A more recent, related finding of considerable practical importance is the significant influence that the presentation of the default choice has on the choice made: for example, whether to opt in or out of a privacy-preserving feature.[19] Another is the endowment effect—how giving up versus receiving something can influence choice, even when the

net effect is the same.

Humans are communicating creatures. We live better when we communicate more. The Internet and the emergence of social media provide amazing new communication opportunities. But sharing our private lives in public is also risky.

In a world in which people voluntarily live their private lives in public, we need to work with behavioral science to design and create safe public spaces. Rather than bemoan the "stupid" or "lazy" users who won't protect their privacy more, let's design privacy-enhancing technologies to make public spaces safer and to give people who want to live most of their lives in public some safety. And, maybe, a technology that lets us whisper now and then. □

References

1. G. Gilder, "Into the Fibersphere," *Forbes*, 7 Dec. 1992; www.seas.upenn.edu/~gaj1/fiber.html.
2. J. Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," *The New York Times*, 22 Dec. 2005;www.nytimes.com/2005/12/22/nyregion/22rooftop.html.
3. "Cat in Bin in Coventry," YouTube, 22 Aug. 2010; www.youtube.com/watch?v=MOuCjzVAO_w.
4. C. Le Coq, "Egypt's Mobile Market Nears Saturation at 80 Pct Penetration," *Daily News Egypt*, 3 Jan. 2011; www.thedailynewsegypt.com/it-a-telecom/egypts-mobile-market-nears-saturation-at-80-pct-penetration.html.
5. S.D. Warren and L.D. Brandeis, "The Right to Privacy", *Harvard Law Review*, vol. 4, no. 5, 1890, pp. 193–220.
6. D. Brin, *The Transparent Society*, Basic Books, 1999.
7. B. Snyder Bulik, "Apparently That Text Can't Wait—Not Even during Sex," *Advertising Age*, 5 May 2010; http://adage.com/article?article_id=143705.
8. S. Dalton, "The Rise and Fall of Josh Harris? The Twitter Generation's Voice from the Bunker," *Times*, 17 Oct. 2009; http://goo.gl/uupJk.
9. K. Hill, "The Truth Will Set You Free? A Broke, Adulterous, Disgraced Georgetown Law Marine Issues a Public Confession on Facebook," *Above the Law*, 24 June 2010; http://goo.gl/fBpV.
10. "Statistics," Facebook, 2011; http://goo.gl/B7l7.
11. "Thanks, YouTube Community, for Two Big Gifts on Our Sixth Birthday!" *Broadcasting Ourselves*, 25 May 2011; http://goo.gl/fqPIN.
12. "5,000,000,000," Flickr, 19 Sept. 2009; http://goo.gl/Hs.Mg.
13. "Twitter Statistics," Twitter KISS Metrics blog, 12 Mar. 2011; http://blog.kissmetrics.com/twitter-statistics.
14. "Match.com and Chadwick Martin Bailey 2009–2001 Studies: Recent Trends: Online Dating," Match.com, 2010; http://cp.match.com/cppp/media/CMB_Study.pdf.
15. d. boyd, "Why Youth (Heart) Social Network Sites: The Role of Networked Publics in Teenage Social Life," *Youth, Identity, and Digital Media*, D. Buckingham, ed., MIT Press, 2008, pp. 119–142.
16. A. Acquisti, R. Gross, and F. Stutzman, "Privacy in the Age of Augmented Reality," to be published in *Proc. National Academy of Sciences*, 2011.
17. d. boyd, "Social Steganography: Learning to Hide in Plain Sight," *Digital Media and Learning: The Power of Participation*, 23 Aug. 2010;http://goo.gl/6pML.
18. A. Tversky and D. Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science*, vol. 211, no. 4481, 1981, pp. 453–458.
19. E.J. Johnson, S. Bellman, and G.L. Lohse, "Defaults, Framing and Privacy: Why Opting In-Opting Out," *Marketing Letters*, vol. 13, no. 1, 2002, pp. 5–15.

Jeffrey MacKie-Mason *is the dean of the School of Information and a professor at the University of Michigan. Contact him at jmm@umich.edu.*