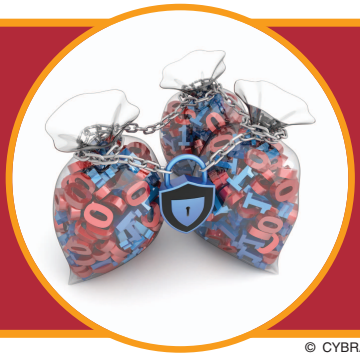
Privacy engineering emerges as a hot new career



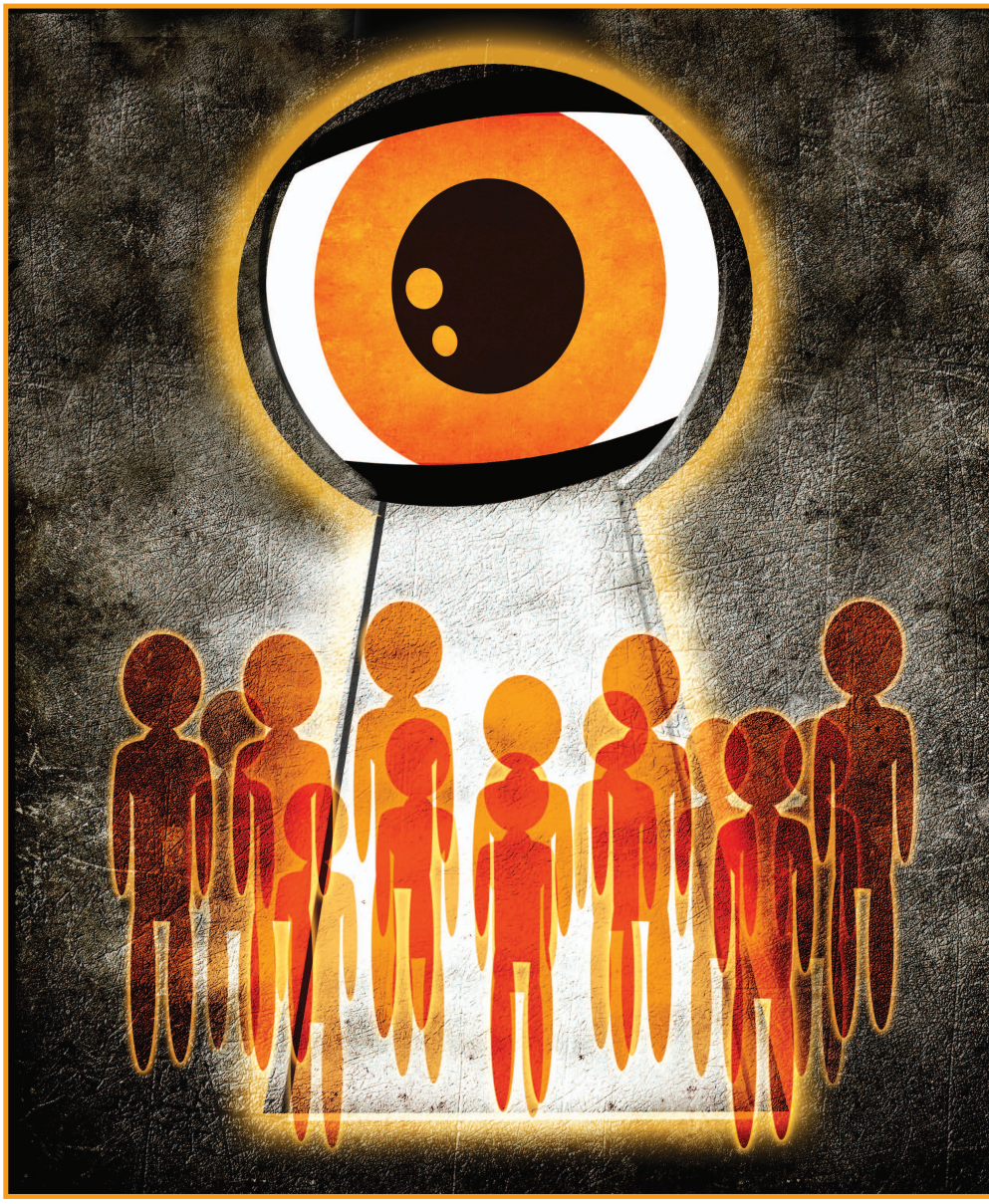
LORRIE FAITH CRANOR AND NORMAN SADEH

Are you concerned about the privacy implications of big data; government surveillance; or the ability of social networks, search engines, and online advertisers to amass detailed profiles of individuals? Do you want to use your technical skills to help reverse the trend toward diminishing privacy? Would you like to help find ways to design privacy into products and services without sacrificing functionality or convenience? Do you want to help people take control over their own personal information? If you answered "yes" to any of these questions, then a career in privacy engineering may be for you.

Privacy engineers are technologists responsible for ensuring that privacy is an integral part of the design process. Companies large and small are bringing in privacy engineers for well-paying jobs as in-house consultants who work as part of multidisciplinary teams. They must understand technology and be able to integrate perspectives that span product design, software development, cybersecurity, human-computer interaction, and business and legal considerations.

Jobs for privacy engineers

As companies become more sensitive to privacy issues and face increasing obligations to comply with legal and regulatory requirements related to privacy, we've seen an increasing number of companies and government agencies recruiting privacy engineers and technical privacy managers. For example, in a recent search for privacy jobs at Google, we found open privacy software engineering positions in both New York and London, as well as several privacy-related jobs in Mountain View, California—including privacy engineer, privacy program manager, data privacy analyst, and data privacy engineer for the privacy "Red Team." Already, Google reportedly employs 60 full-time privacy engineers (Gohring, 2011). Andrew Swerdlow, a Google privacy analysis engineer, described the role of Google's privacy engineers: "We work closely with legal, policy, and other engineers as products are being developed and released. At the beginning of product



Digital Object Identifier 10.1109/MPOT.2013.2277492
Date of publication: 4 November 2013

0278-6648/13/$31.00©2013IEEE

development, we sit with engineers to help them design products with privacy in mind. During development, we review, audit, and test the boundaries of products. After a product launches, we evaluate and reevaluate the product to ensure it remains true to our privacy standards."

We've also recently seen ads recruiting privacy engineers and managers at Microsoft, Facebook, Intel, Apple, Mozilla, and the National Institute of Standards and Technology, as well as financial companies, privacy-related startups, and government agencies, to name just a few. Job postings recruit engineers who can "develop technical solutions to help mitigate privacy vulnerabilities"; analyze "software designs and implementations from a privacy and UX (user experience) perspective"; "research, document, and help remediate design decisions, operating procedures, or processes that may directly or indirectly contribute to future privacy risks"; "create cutting-edge privacy feature prototypes"; "help us lead better on privacy by example"; and "partner with key business, technical, and legal stakeholders across various … business groups to implement Privacy by Design" (Cranor and Sadeh, 2013).

Maritza Johnson conducted research on Facebook privacy controls as a Ph.D. student at Columbia University and recently landed a job as a technical privacy manager at Facebook. Johnson now works with Facebook's cross-functional privacy team to evaluate the privacy impacts of existing and new Facebook products and to recommend and implement improvements.

Erin Egan, Facebook's chief privacy officer, explained that Facebook is adding to its team of professionals who develop products with privacy in mind. This team includes privacy engineers and product managers as well as security engineers. "As our team continues to grow, we are looking for candidates who have not only the technical skills to work on our products but a deep understanding of how building privacy into Facebook creates a great experience for our users," Egan told us when we asked her about the skills Facebook was looking for when they hire privacy engineers (Cranor and Sadeh, 2013).

At the annual Privacy Enhancing Technologies Symposium last July, Sid Stamm, lead privacy engineer at Mozilla, talked about the core privacy principles that guide data practices and operations at Mozilla. One of these principles, "user control," requires the design of products that obtain a user's consent before disclosing personal data. But designing meaningful consent experiences can be tricky because it is sometimes difficult to explain technical details in ways that users can understand, and users may not want to stop and read these explanations before trying out a new product or feature.

Stamm told us that Mozilla is also recruiting privacy engineers. "We're looking for strong programmers who have a knack for understanding nuances of data sharing and use. They have an ability to build systems that enable transparency and can find ways to help our users make good choices through understanding risks of sharing their data," he said. However, Stamm added that he's had difficulty finding qualified candidates for privacy engineering positions. "I've found that technologists who find an interest in privacy get attracted to work in policy and activism. What we need are software engineers who want to write tools and features that will enhance peoples' privacy online" (Cranor and Sadeh, 2013).

Indeed, we've heard from several companies who are trying to hire privacy engineers that they have trouble filling these positions with qualified candidates. Most privacy engineers and managers working in industry today were trained in other fields and learned about privacy on the job. Many come from computer security or software engineering backgrounds, learning about privacy after being assigned to work on a privacy-related project and getting up to speed by reading about privacy and attending privacy tutorials, such as those offered by the International Association of Privacy Professionals (IAPP). However, without an initial foundation in these areas, it can take years for these people to develop the skills of a privacy engineer and to gain an appreciation for the interplay between technical, business, human, and legal issues.

Privacy engineers might also come from legal or policy backgrounds but typically require technical training before they can play an engineering role. Companies have an urgent need for trained privacy engineers who can hit the ground running. Trevor Hughes, president and CEO of the IAPP explains, "As the field of privacy grows around the globe, we are seeing a clear need for highly trained engineers who can translate the complexity of privacy into technology. There are too few of these professionals today" (Cranor and Sadeh, 2013).

How to become a privacy engineer

Students interested in pursuing a privacy engineering career should develop strong technical expertise as well as skills in the privacy and security areas. As undergraduates, computer science and engineering students interested in privacy engineering should make sure to take at least one course on computer security. If you are fortunate enough to attend a school that offers a privacy course, take advantage of that. Modules on privacy are sometimes included in courses on computer security, technology and public policy, and computers and society. If you can find a faculty member willing to work with you, you might also design an independent study project or senior thesis on a privacy-related topic.

There are a growing number of master's degree programs in security-related fields that aspiring privacy engineers might consider. However, most of these programs don't actually include much privacy-specific content. We recently started a master's program focused on privacy engineering at Carnegie Mellon University. Currently, there are no other programs like this, but we expect it won't be long before similar programs emerge elsewhere.

Our master of science in information technology-privacy engineering is a one-year program designed for computer scientists and engineers who want to pursue careers as privacy engineers or technical privacy managers (http://privacy.cs.cmu.edu). This program includes two semesters of courses taught by leading academic privacy and security experts. Students take courses that cover legal and policy issues, the mathematical and technical foundations of privacy engineering, software engineering, usability assessment, and management as well as attend a weekly seminar covering current topics in privacy. The seminar also features guest lectures from privacy engineers working in the field. The program concludes with a summer-long capstone project in which students work as privacy consultants on client projects.

Doctoral students interested in privacy engineering should take as much privacy-related coursework as possible and focus their research on privacy. Several of our Ph.D. students who focused their graduate coursework and research on privacy have gone on to privacy-related careers. For example, one of our former Ph.D. students went on to lead

the World Wide Web Consortium's Do Not Track effort and now heads a privacy center at Stanford, another is a privacy manager at Microsoft, and another works for Google.

Students interested in privacy engineering should become student members of the IAPP (https://www.privacyassociation.org) and sign up for their daily online newsletter to stay abreast of privacy issues in the news. IAPP holds several conferences each year that are a good opportunity to learn about privacy issues and network with privacy professionals. The organization typically offers opportunities for students to apply for scholarships to attend these events. IAPP also offers a Certified Information Privacy Professional exam and certification program. In some cities, local IAPP groups offer seminars and networking events several times each year. The annual Computers, Freedom, and Privacy Conference (http://cfp.org) is another good opportunity to learn about privacy issues.

There are a number of research conferences that typically include privacy-related research. The Privacy Enhancing Technologies Symposium (http://petsymposium.org/) is a conference dedicated entirely to privacy research. The Symposium on Usable Privacy and Security (SOUPS) focuses on human factors issues related to both security and privacy but tends to have a large number of papers on privacy. In 2013, SOUPS (http://cups.cs.cmu.edu/soups/) featured papers on privacy in social networks as well as privacy concerns related to online behavioral advertising. Security conferences, such as the IEEE Symposium on Security and Privacy (http://www.ieee-security.org/TC/SP2013/), typically include some privacy-related content. The ACM Conference on Computer and Communications Security (http://www.sigsac.org/ccs.html) usually includes some privacy research but also includes a one-day Workshop on Privacy in the Electronic Society devoted entirely to privacy research. Conferences in human-computer interaction, ubiquitous computing, and health informatics are increasingly including privacy-related research as well. Students interested in privacy engineering careers should check out these conference proceedings and, if possible, participate in some of these events.

Read more about it

- L. Cranor and N. Sadeh, "A shortage of privacy engineers," *IEEE Security Privacy*, vol. 11, no. 2, pp. 77–79, Mar./Apr. 2013.
- B. Gohring. (2011, Dec. 8). Google, Microsoft teams work to keep pace with privacy laws. *Comput. World* [Online]. Available: www.computerworld.com/s/article/9222536/Google_Microsoft_teams_work_to_keep_pace_with_privacy_laws
- Google. (2013). Meet Andrew Swerdlow, a privacy analysis engineer. [Online]. Available: www.google.com/about/jobs/lifeatgoogle/meet-andrew-swerdlow-privacy-analysis-engineer.html
- Mozilla. (2013). MozillaWiki. [Online]. Available: https://wiki.mozilla.org/Privacy/Principles

About the authors

Lorrie Faith Cranor (lorrie@cs.cmu.edu) is an associate professor in the School of Computer Science and in the Engineering and Public Policy Department at Carnegie Mellon University.

Norman Sadeh (sadeh@cs.cmu.edu) is a professor in the School of Computer Science at Carnegie Mellon University.