Editor: Tara Whalen, twhalen@pobox.com

A Shortage of Privacy Engineers

Lorrie Faith Cranor and Norman Sadeh | Carnegie Mellon University

As organizations develop new products, services, infrastructures, and business processes that facilitate the collection and management of an ever-wider range of customer data, they're discovering that privacy issues must be addressed from the very beginning of the design process.[1] During the past several years, organizations large and small have started to create positions for *privacy engineers*—technologists responsible for ensuring that privacy is an integral part of the design process. These people are brought in 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.

However, companies that have embraced this privacy-by-design (PbD) approach are having trouble finding privacy engineers who can lead privacy design efforts. 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, it can take years to develop the skills of a privacy engineer and to gain an appreciation for the interplay among 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.

Designing in Privacy

Companies are increasingly realizing the importance of designing privacy into their products and services from the beginning. There are numerous cases in which companies have had to scramble to retrofit privacy into existing systems. Many highly publicized incidents have involved social networks whose users were surprised when they realized information they considered private was transmitted to other users, advertisers, or even the public.[2] We've heard from managers at some of these companies who are eager to grow privacy expertise on their engineering teams to address these concerns more proactively.

Since the 1990s, Ann Cavoukian, Ontario, Canada's Information and Privacy Commissioner, has been urging companies to adopt PbD, emphasizing the importance of designing products and services with privacy designed in from the beginning rather than patched on later to comply with laws or respond to problems. Although some complain that PbD can be expensive, Cavoukian argues that if done well, it can be a positive-sum approach in which privacy protections might ultimately improve products or facilitate more cost-effective solutions. On the other hand, when privacy issues aren't addressed early, companies risk costly privacy mistakes that might result in loss of customers, loss of reputation, lawsuits, launch delays, and redesign costs.

PbD can be applied in software system design as well as in the design of physical systems and business practices. For example, prompted by US healthcare privacy regulation, hospitals and doctors' offices began reconfiguring their waiting areas so that patients couldn't readily overhear conversations about sensitive medical issues. Even relatively small changes, such as moving hospital fax machines from open hallways to locked offices and adding a line behind which pharmacy customers must wait, can improve privacy. However, fax machines in locked offices might no longer be readily accessible to healthcare

1540-7993/13/$31.00 © 2013 IEEE Copublished by the IEEE Computer and Reliability Societies March/April 2013

workers who need quick access to faxed information. Offices designed from the beginning to include areas for private conversations and the receipt and storage of private documents can offer better privacy protections as well as an environment conducive to efficient workflows.

Although there are a growing number of guidelines (such as Microsoft's *Privacy Guidelines for Developing Software Products and Services*[3]) and case studies to draw from, there's no simple, universal formula for designing in privacy. PbD requires engineers with a diverse skill set to understand how both privacy-by-policy and privacy-by-architecture mechanisms can interact to protect privacy. Privacy-by-policy approaches include privacy notices and mechanisms for obtaining informed consent before data is collected or used. Privacy-by-architecture approaches aim to minimize the collection of personal data, anonymize as much of it as feasible, and reduce centralized data storage and processing.[4] Although organizations can easily implement simple techniques from both approaches, designing meaningful and usable informed consent experiences and implementing robust and sophisticated data minimization or anonymization techniques that preserve essential data utility are both nontrivial tasks.

Shortage of Privacy Engineers

We've seen an increase in companies recruiting privacy engineers, and many organizations are already reporting a shortage of people who are adequately trained to fill this crucial role.[5] Recent US Federal Trade Commission settlements with organizations both large and small and pending revisions to privacy laws in places like Europe will fuel increasing demand for privacy professionals.[6,7]

Recently, we've seen announcements recruiting privacy engineers and technical privacy managers at Google, Microsoft, Facebook, Intel, Apple, and the National Institute of Standards and Technology as well as financial companies, privacy-related startups, and government agencies, to name just a few. Already, Google reportedly employs 60 full-time privacy engineers.[8] Job postings recruit engineers who can "develop technical solutions to help mitigate privacy vulnerabilities"; analyze "software designs and implementations from a privacy and UX 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."

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 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" (www.google.com/about/jobs/lifeatgoogle/meet-andrew-swerdlow-privacy-analysis-engineer.html).

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 it hires privacy engineers.

Sidd Stamm, lead privacy engineer at Mozilla, 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 said 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 people's privacy online."

Training Privacy Engineers

One way to address the privacy engineer shortage is to offer educational programs in the subject. During the past decade, several universities began offering privacy-related courses in their computer science and engineering schools.

Our university, Carnegie Mellon, offers several privacy courses for undergraduate computer science and electrical and computer engineering majors; master's students in a variety of computer science, information systems, public policy, and business fields; and PhD students in computer science, engineering, and public policy. Privacy-related courses include Information Security and Privacy; Privacy Policy, Law, and Technology; Usable Privacy and Security; Foundations of Security and Privacy; and Privacy in the Digital Age. Students who

took all of these courses would have a solid foundation in privacy; however, typical students can't fit more than one or two of these courses into their schedule.

We've had a few students who focused their graduate coursework and research on privacy and have gone on to privacy-related careers. For example, one of our former PhD students went on to lead the World Wide Web Consortium's Do Not Track effort; another is a privacy manager at Microsoft. In addition, students who have gone on to other types of engineering roles in their careers have emailed us to report that they made use of their privacy expertise when their teams struggled with addressing privacy needs.

Over the past few years, we've been thinking about how to tie together our existing courses with some new privacy courses to create a comprehensive privacy engineering graduate curriculum. We've worked with our colleagues to propose an MS in Information Technology—Privacy Engineering (MSIT-PE) degree program and are currently recruiting students to enter the program next fall (http://privacy.cs.cmu.edu).

MSIT-PE is a one-year program designed for computer scientists and engineers who want to pursue careers as privacy engineers or technical privacy managers. This program includes two semesters of courses taught by leading academic privacy and security experts. Students will 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 will also feature 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 with students from other professional master's programs.

Currently, Carnegie Mellon is the only university to offer such a program, but we expect it won't be long before other universities offer similar degree programs. We've also observed a need for part-time and professional education programs for working professionals who want to gain privacy engineering expertise.

Privacy engineering is emerging as a new career path that addresses the critical needs of business and government organizations. As Trevor Hughes, president and CEO of the IAPP, explained to us, "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." New courses and degree programs are needed to train students for these privacy engineering jobs. ■

References

1. A. Cavoukian, "Privacy by Design," Office of the Information and Privacy Commissioner, Aug. 2009; http://privacybydesign.ca/publications/pbd-the-book.
2. K. Kindelan, "10 Privacy Blunders That 2010 Will Be Remembered For," *SocialTimes*, 21 Dec. 2010; http://socialtimes.com/10-privacy-blunders-that-2010-will-be-remembered-for_b32163.
3. *Privacy Guidelines for Developing Software Products and Services*, Microsoft, 29 Sept. 2010; www.microsoft.com/en-us/download/details.aspx?id=16048.
4. S. Spiekermann and L.F. Cranor, "Engineering Privacy," *IEEE Trans. Software Eng.*, vol. 35, no. 1, 2009, pp. 67–82.
5. "TRUSTe Unveils Top Online Privacy Predictions for 2012," TRUSTe, 19 Dec. 2011; www.truste.com/about_TRUSTe/press-room/news_truste_top_privacy_predictions.
6. T. Romm, "Web Giants Tagged for Privacy Audits," *Politico*, 14 Dec. 2011; www.politico.com/news/stories/1211/70453.html.
7. B. Bailey, "Google Recruiting Data Privacy 'Ninjas,'" *Mercury News*, 23 Aug. 2012; www.mercurynews.com/business/ci_21386267/google-recruiting-data-privacy-ninja-red-team.
8. B. Gohring, "Google, Microsoft Teams Work to Keep Pace with Privacy Laws," *ComputerWorld*, 8 Dec. 2011; www.computerworld.com/s/article/9222536/Google_Microsoft_teams_work_to_keep_pace_with_privacy_laws.

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

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