Speaking of Privacy

When Plato, quoting Socrates, said "the unexamined life is not worth living," he was talking about self-examination. Today, it seems every life is examined, but more frequently by others than by ourselves.

Carl E. Landwehr

Parents, concerned for their children's safety, can check their paths through cyberspace via various forms of monitoring software and their paths through physical space via cell-phone location-tracking services. Meanwhile, retailers track buying habits by offering discounted prices to those willing to be identified. Convenient RFID tokens enable tracking of vehicles on toll roads. Growing numbers of video cameras monitor private premises and public plazas for the purpose of deterring crime. Some data that, although officially public, was only accessible by visiting a physical office, is now available anywhere in the world with a few mouse-clicks.

In such a world, it's difficult not to feel like the object of a study in which the interested parties, including your telephone, medical insurance, and credit-card companies, online book and video stores, and even Internet search engines seem to know more about you, or at least your health and habits, than you do. I might feel better about this if I could read the study results, but I'm probably not going to get them unless a profit can be made in the process.

Was Scott McNealy right in 1999 when he proclaimed, "you have zero privacy anyway—get over it"? I don't think so, but I do think we need to gain a better understanding of what we mean by "privacy" in the modern world if we expect to preserve it, especially as monitoring increases. And it might help us to consult a living philosopher in the process.

Privacy, in the words of a recent National Research Council study,[1] is a multifaceted term that has many meanings depending on how and where you use it. To some, it might seem like a data attribute: some data are private and some are public. To others, privacy isn't a property of particular data but a right to control when and on what terms personal attributes can be disclosed.

At this year's IEEE Symposium on Security and Privacy, Helen Nissenbaum of New York University and resident philosopher of the Portia project (Privacy, Observations, and Rights in Technologies in Information Assessment; http://crypto.stanford.edu/portia/), proposed that privacy be viewed as "contextual integrity." (In the spirit of full disclosure, the US National Science Foundation funded Portia during my tenure there, although not through my program.) I confess I had no idea what these words meant initially, but she explained the concept as follows.

S&P's new editor in chief

Congratulations to Carl E. Landwehr on his appointment as *IEEE Security & Privacy*'s editor in chief for 2007–2008!

He has served as associate editor in chief since *S&P* launched in 2003 and brings years of experience in computer security to the magazine. Carl is manager of the Information Assurance Research Program at the Advanced Research and Development Activity, on assignment from his position as senior research scientist at the University of Maryland's Institute for Systems Research. He recently completed an assignment as founding director of the Cyber Trust program at the National Science Foundation. He was a senior fellow at Mitretek Systems, and earlier he headed the Computer Security Section of the Center for High Assurance Computer Systems at the US Naval Research Laboratory.

He has been active internationally as the founding chair of IFIP WG 11.3 (Database and Application Security) and is also a member of IFIP WG 10.4 (Dependability and Fault Tolerance).

S&P looks forward to working with Carl in the years ahead to bring his editorial vision to life, increasing efforts to address security concerns in the *S&P* community and far beyond.

Information is only sensitive (or not) relative to context, and the rules governing the flow of information from one party to another depend on the nature of the context. Thus, people freely disclose transactional information to their retailers, financial information to their bankers, health information to their doctors, and moral views to their religious advisers with no sense that these disclosures violate privacy. The feeling of violation occurs when the individual learns that the retailer, banker, physician, or religious advisor has shared this information inappropriately with others either within or beyond the relevant context; in other words, when the confidentiality rule has been broken. Confidentiality is only one of many rules; the analysis of contextual integrity posits many other rules and many other contexts.

We won't really know if this is a workable definition of privacy until we apply it in a variety of situations and it seems to be satisfactory to the community. But thinking, and speaking, of privacy in this way suggests that we at least try to identify different contexts and the rules that we would want to apply to handling data within and between contexts.

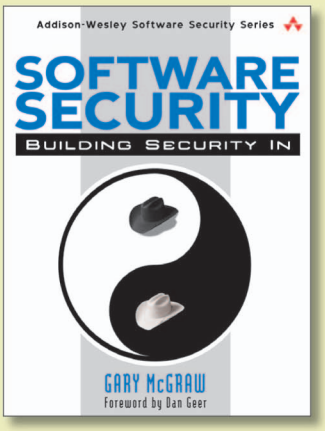
For example, in which situations can video camera recordings be properly disclosed (or denied) to authorities seeking copies of them? Under what conditions can we provide specific statistical summaries of sensitive data for research purposes? What are the appropriate contexts and rules for information, such as Web searches, that people might not realize is being collected? What about contexts that overlap, such as between pharmacological research and healthcare delivery systems? Can we maintain contextual boundaries for information as system boundaries seem to melt? Under what conditions should the force of law compel disclosure?

Though I'm a technologist at heart, I believe privacy technology will be an unguided missile without the proper conceptual framework. In particular, we need concepts that can express our shared and varied notions of privacy without being so rigid as to place us on a Procrustean bed and without being so malleable that they don't provide any real protection. I don't know if contextual integrity is the perfect basis for solving this riddle, but I do think it's a concept for privacy worth further study. ▢

Reference

1. Committee on Authentication Policies and Their Privacy Implications, "Who Goes There? Authentication through the Lens of Privacy," Nat'l Academies Press, 2003.

BUILDING SECURITY IN...



SOFTWARE SECURITY:
Building Security In
GARY McGRAW
READ CHAPTER 5:
Architectural Risk Analysis ONLINE.
ISBN: 0-321-35670-5

PUT SOFTWARE SECURITY INTO PRACTICE TODAY WITH THESE BOOKS!

SOFTWARE SECURITY LIBRARY
GARY McGRAW, JOHN VIEGA, and GREG HOGLUND
Avoid risks and build security into your software with these three field-defining books: ***Building Secure Software***, ***Exploiting Software***, and ***Software Security***.
ISBN: 0-321-41870-0

FOR A SNEAK PEEK, DOWNLOAD SAMPLE CHAPTERS ONLINE AT
www.awprofessional.com/security
Available wherever technical books are sold.

Addison Wesley