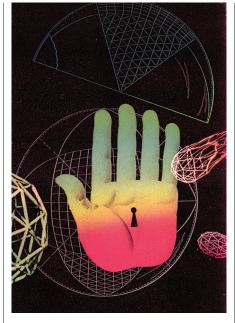Susan Landau

Privacy and Security
A Multidimensional Problem

It's not just science or engineering that will be needed to address security concerns, but law, economics, anthropology, and more.

WHEN THOSE OF us who are now editors of this magazine were in graduate school, it was easy to believe that with the inevitable exception of automation, social implications of computing technology could be ignored with impunity. Yes, before the public Internet, there was discussion of social impact—Joe Weizenbaum's ELIZA, the Department of Health, Education, and Welfare report, *Records, Computers, and the Rights of Citizens*,[a] the establishment in Europe and Canada of data commissioners, the "I am a [person]. Please don't bend, fold, spindle or mutilate me," joke that made the rounds in the 1970s,[b] the role of computers in President Reagan's Star Wars program—but it was easy to maintain the fiction that the machines we built and the code we wrote had as much social impact as the designers of John Deere tractors have on the migratory patterns of cliff swallows: minimal and not really significant.

Tom Lehrer once sarcastically characterized a famous astronautics engineer, "'Once the rockets are up, who cares where they come down? That's

not my department,' says Wernher von Braun."[3] But while the view that scientists bear responsibility for the social impact of their work was perhaps radical when it was espoused by Joseph Rotblat (a nuclear physicist who later won a Nobel Peace Prize for his work on nuclear disarmament) in the decade after Hiroshima and Nagasaki, this expectation is no longer unusual. It is also no less true for technologists now than for scientists.

This is part of the ACM code. The original ACM Code of Ethics and Professional Conduct stated, "An ACM member shall consider the health, privacy and general welfare of the public in the performance of the mem-

ber's work." It went on to say that, "An ACM member, when dealing with data concerning individuals, shall always consider the principle of individual privacy and seek the following: To minimize the data collection; To limit authorized access to the data; To provide proper security for the data; To determine the required retention period of the data; To ensure proper disposal of the data." (The current ACM code of ethics contains a similar set of principles, though it omits the requirement regarding proper disposal of data.) But observing current computer privacy and security practices leads one to question whether this code is honored more often in the breach.

Each week brings yet another news story of a major security breach, of the ability to do a cross-site scripting attack on the new favorite mailer, of the polymorphic virus code that changes its signature to evade detection. We aren't getting privacy and security right.

We aren't even asking the right questions. A recent U.S. Department of Defense (DoD) effort to develop an Iraqi ID database of bad guys is one such example. The database includes not just names, but biometric identifiers: fingerprint records and iris scans; its purpose is to maintain records on the people who keep turning up in an area soon after an explosion has occurred.[2] As any developer knows, of course, this database will not be used only in this way. One such likely use will be at checkpoints—and currently in Iraq, it can be

---

a   This report, which recommended legislation supporting Fair Information Practices for automated data systems, was highly influential in both Europe and the United States; see http://aspe.hhs.gov/DATACNCL/1973privacy/tocprefacemembers.htm.

b   This was a takeoff on IBM's instructions for the handling of punch cards.

quite dangerous to be a Sunni at a Shiite checkpoint (and vice versa). Now, to its credit, the Defense Science Board, an independent board advising the DoD, recommended that the military "engage responsible advocates of privacy early in the design and application of identity management systems,"[1] yet somehow this database system was developed for use in a place in which a name of the wrong ethnicity can lead to being murdered. Technologists did not stop to consider "once the rockets are up, where will they come down?"

One reason for our failure of cyber privacy and security is that these problems are difficult to resolve. Yes, over 30 years ago we had the ideas of Multics and the Orange Book, but such solutions have little traction in the current environment, especially when (almost) all users seek to mount their newest untrusted device on their (less than fully protected) systems. In the rush toward releasing a product, there is little economic incentive to spend the time properly designing privacy and security into systems.

We don't ask: What system design for highway toll collection gives appropriate privacy protections? Do we really need to store the toll records any longer than a month after billing? Should we passively collect any data on a user as he or she visits an e-government site? How sensitive is an IP address? (Does it reveal any information about the user?) Is our organization's system for managing passwords usable? (Or are users finding an insecure workaround?) Is there a way that the digital-rights system can find cheating users without compromising everyone else's privacy? What are the security risks of that CCTV surveillance system? Can this database system really help us find the bad guys, or does it risk the safety of ordinary citizens? As technologists, we have a responsibility to investigate such issues before we build—not after.

No company wants to appear on the front page of the *New York Times* or in front of the Article 29 Data Protection Working Party of the EU Commission explaining how its system failed to protect important health care/financial/personal data. But while there may be breach laws that require notification in the case of data exposure, there have

Solutions for computer privacy and security are not mathematical theorems, but instead lie in the complexity of human behavior.

been precious few liability suits against the companies whose technologies allowed the problem to occur in the first place. Legal and policy systems simply haven't kept up with technology. Meanwhile our technology keeps evolving at an ever-increasing pace. Our networked, interconnected systems pose new threats and present new challenges; we need to find new ways of working.

The right technical answers are not always obvious; because the problems involve societal concerns, often the solutions are less than clear-cut. What is the way out of this mess? The sorry state of computer privacy and security is a state for which technologists bear part of the responsibility. We can—and must—be part of the solution. Yet there is another part of this story, namely that computer privacy and security are both technical concerns and social ones.

Solutions for computer privacy and security are not mathematical theorems, but instead lie in the complexities of human behavior. One person's good identity management scheme may violate another person's view of adequate control of personal data; another person's method for securing a network may be simply too restrictive to permit appropriately private access by the network's users. It is not just science that will enable us to solve these problems, or engineering, or business acumen, or even anthropologic studies of what makes users tick. It will be a combination of all of these, and more.

Communications will publish articles on computer privacy and security in the Practice, Contributed, and Research sections of the magazine. This column will present peoples' opinions on privacy and security concerns—and their possible solutions. Because the

problems are not only technical, this column will present a diversity of viewpoints on the issues, soliciting responses from lawyers, economists, political scientists—and computer scientists.

We will also seek geographic diversity. The Internet knows no physical boundaries. As we know, its privacy and security breaches don't either—consider the ILUVU virus that apparently originated in the Philippines, the Nigerian 419 scam[c] that can as easily originate in Russia as Nigeria, and a breach in a system designed in Mountain View, CA can cause serious problems in Melbourne, Australia. People are as concerned about data retention in Korea as they are in Europe (and apparently more so than they are in the U.S.). To solve the problems of computer privacy and security, we must look at the issues globally.

Protecting the privacy and security of data in networked computer systems is a major challenge of our age. The challenge of this column is to present ideas that stimulate the critical thinking needed to develop solutions to this multifaceted problem. Yours is to read, ruminate, and change the system—and systems—that currently harbor such poor protections of privacy and security. Change is slow, and changes of this order of magnitude are very difficult. If this column has even a minor impact on improving the privacy and security of computer systems, it will have succeeded in its mission. ▣

References
1. Defense Science Board, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics. *Report of the Defense Science Board Task Force on Defense Biometrics*, March 2007, 71.
2. Frank, T. U.S. is building database on Iraqis. *USA Today*, (July 21, 2007); www.usatoday.com/news/world/iraq/2007-07-12-iraq-database_N.htm.
3. Lehrer, T. *Too Many Songs by Tom Lehrer*. Pantheon Books, New York, 1981, 124–125.

Susan Landau (Susan.Landau@sun.com) is a Distinguished Engineer at Sun Microsystems Laboratories in Burlington, MA.

c   This is a scam in which victims are offered large amounts of money from someone who has unexpectedly died (typically in a plane crash) leaving no will or known next of kin. In order to participate, the victims must first demonstrate their seriousness by funding efforts to access the money. It is called a "419" scam after the part of the Nigerian Criminal Code that deals with obtaining property through false pretenses.