Dirty Laundry: Privacy Issues for IT Professionals

Don Henley used to sing, "They love dirty laundry," an observation that might well apply to all of us—provided, that is, it's not our own laundry (dirty or clean) being exposed. In the wake of recent high-profile legal cases in North Dakota and Minnesota, some have suggested that consumers are questioning organizational practices supposedly designed to protect their personal information. With increased connectivity in the information age come increased threats to individual privacy. Organizations are finding that this issue inevitably challenges IT professionals in several domains, especially data management and security. Many organizations invest time, money, and human resources to enforce privacy policies (which may soon be legally enforced) as well.

In 1999, we distributed a survey to 560 data workers in the healthcare and financial fields. The results of the study suggest that privacy concerns are not confined to consumers, but the employees who access and collect the data are concerned as well. The survey (detailed results available at http://ecommerce.csc.ncsu.edu/ispp/) posed 15 questions regarding the responders attitudes about the organizational practices at their organization. The data collected from the survey reveals that healthcare workers are concerned about organizational practices causing errors in patient information, as well as unsanctioned use of patient information. Similarly, our survey research indicates that employees of financial institutions are concerned with organizational practices that allow improper access to customer information. Given the results in these two fields, IT workers and managers in all fields must be prepared to deal with this issue, for it is likely to confront them soon.

THE CURRENT STATE OF PRIVACY

Numerous commentaries, such as those in the 1 October 1998 issue of CIO and the 18 June 1998 issue of the Wall Street Journal, have focused on how the privacy debate affects the general public. Public opinion polls routinely suggest increasing concern regarding personal information privacy. Despite the recent e-commerce boom, surveys such as the FTC survey described below indicate that not many Web sites have privacy policies.

In the US

The FTC recently issued a report to Congress (http://www.ftc.gov/reports/privacy3/) revealing results of a study showing 85 percent of Web sites collect personal consumer information, whereas only 2 percent of these sites disclose a complete privacy policy.

Recent events indicate that personal information privacy may soon become an IT priority. In North Carolina, the state legislature recently
PRIVACY AND IT

Privacy Policy Guidelines

- Keep your passwords private!
- Never give out a customer's personal information, such as name, address, or phone number.
- Back up all critical data.
- Classify all network users.
- Use antivirus software.

stonewalled on adopting the Health Care Information Privacy Act. This legislation would have clarified many private situations, including when pharmacies should disclose patient information to others, such as law enforcement agencies and insurance companies. It would have established some ground rules on electronic media and privacy in the healthcare industry as a whole (Craig Jarvis, "Pharmacists Can't Always Keep Patient's Secrets," News and Observer, 6 February 1999, p.A1). The bill received input from healthcare providers, advocates, and industry groups, but dissent over some provisions prevented it from passing.

Although the North Carolina state government seems to be dragging its heels in the case of this legislation, the banking industry seems to at least be thinking about self-policing. Following a case in which the state of Minnesota sued US Bank for selling customer data to telemarketers, Bank of America eradicated a similar practice and concluded that it should not compromise consumers' trust and privacy. However, shortly after declaring this position, Bank of America issued a statement declaring there would be some exceptions and it would continue sharing information to certain third parties (Sam Zuckerman, "BofA Backs Off Privacy Vow on Client Data," San Francisco Chronicle, 17 June 1999, p. B1). Credit card companies such as Visa and American Express, supermarkets, airlines, and even gasoline companies maintain massive consumer databases from which any data miner could glean and exploit a customer's personal buying, financial, and health patterns.

Several media outlets, such as PC World, have devoted special issues to advise the public on how to protect personal, financial, and medical information. "You Are For Sale" (Jeffrey Rothfeder, in "Privacy in the Internet Age: A Special Report," PC World, Sept. 1998, pp. 97-106) highlights everyday activities that can result in unauthorized disclosures of personal information. A surprise to many consumers, these activities include such innocent activities as purchasing a house, subscribing to magazines, having a baby, mailing a warranty card, and registering to vote. When consumers provide their social security number, occupation, address, telephone number, income level, loan amounts, medical conditions, and medical background, these details can end up in often-unwanted inclusion in commercial databases. Whenever consumers have heard of these privacy violations, they have objected rigorously.

Such was the case of a 37-year-old recovering leukemia patient who learned of her pregnancy after completing two years of chemotherapy (A.R. Dowd, "You Protect Your Privacy," Money, Aug. 1997, pp. 104-115). One month into her pregnancy, she began to receive baby brochures and expectant-mother information in the mail. Unable to determine who released her personal and health information to medical marketers, she concluded, "It was like Big Brother was out there. It was really creepy. In my heart of hearts, I do not believe that any of (my) doctors who treated me betrayed my confidence. I suspect some anonymous person at the hospital's managed-care unit looked in the computer and saw that I was on prenatal vitamins and passed the information along."

The woman had made repeated attempts to protect her personal and medical information by not providing her telephone and address to merchants and requesting that she be removed from mailing lists. Nevertheless, when asked about protecting her health information, she said, "It's out of control. If you can find out about my pregnancy, they can find out anything about anyone."

In Europe

Privacy is not just an American issue; it's a global one. For instance, Imke Bubert, along with the Electronic Commerce Legal Issues Platform (ECLIP; http://www.jura.uni-muenster.de/eclip/), has described the privacy compromise that technology is introducing to modern healthcare in Europe. Bubert and ECLIP also detail the European Union guidelines for achieving a secure environment for information systems in medicine (SEISMED). The EU has established a formal privacy decree that includes consumer rights, user protection, and legal topics.

ORGANIZATIONAL POLICIES AND INDIVIDUAL PRACTICES

Unfortunately, information sharing in a database-enabled, e-commerce world often conflicts with consumers' desires to be shielded from unauthorized secondary use of their personal data. Organizations will soon experience increased pressure to sharpen their existing privacy policies (if they even have any). Thus, IT professionals should assess employee perceptions of information privacy practices within the organization. Such activities would lead to benchmarking organizational policy mandates against employees' actual practices. Therefore, IT professionals must implement sound data management and security measures for two reasons: first, to protect vital organizational data, and second, to safeguard a customer's personal information, thereby encouraging a more stable consumer base.

Authorized licensed use limited to: North Carolina State University. Downloaded on July 9, 2009 at 18:39 from IEEE Xplore. Restrictions apply.
PRIVACY: A MULTI-DIMENSIONAL CONCEPT

Thomas C. Rindfleisch ("Privacy, Information Technology, and Health Care," Communications of the ACM, Aug. 1997, pp. 92-100) prescribes the following concepts for consideration by IT professionals:

- **privacy**—a person’s right and desire to control the disclosure of his or her personal information;
- **confidentiality**—the controlled release of personal information to an authorized information custodian under an agreement that limits the extent and conditions under which that information may be used or released further; and
- **security**—policies, procedures, and safeguards used to help control access to the contents of information systems (particularly databases) while maintaining the integrity and availability of the data.

Though many organizations subscribe to Rindfleisch’s recommendations, CIOs agree that the most important threats to consumer confidentiality include accidental disclosures, insider curiosity, insider insubordination, and unauthorized access (Computer Science and Telecommunications Board, For the Record: Protecting Electronic Communications Board, Jan./Feb. 1999, pp. 43-48), the authors suggest most organizations are aware of the problem of unauthorized access, though not all have developed a privacy policy and guidelines for employees to follow (see the “Privacy Policy Guidelines” sidebar); however, these don’t guarantee against unauthorized access. Beyond these threats, the unauthorized use of personal information by organizations is most common. A significant issue to consumers, unauthorized use makes them targets for unsolicited marketing actions, statistics, and data mining efforts. In “Basic Intrusion Protection: The First Line of Defense” (Dennis Steinauer, Stuart Katzke, and Shirley Radack, IT Professional, Jan./Feb. 1999, pp. 43-48), the authors suggest most organizations are aware of the problem of unauthorized access to personal data, but few have established an effective security program for their systems. Most organizations have developed a privacy policy and guidelines for employees to follow (see the “Privacy Policy Guidelines” sidebar); however, these don’t guarantee against unauthorized access despite the awareness of heightened security needs, most organizations are facing a shortage of security skills.

---

**Table 1. Privacy constructs and definitions.**

<table>
<thead>
<tr>
<th>Dimension</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collection</strong></td>
<td>Concern that extensive amounts of personally identifiable data are being collected and stored in databases</td>
</tr>
<tr>
<td><strong>Unauthorized secondary use (external)</strong></td>
<td>Concern that information is collected for one purpose but is used for another, secondary purpose after disclosure to an external party (not the collecting organization)</td>
</tr>
<tr>
<td><strong>Improper access</strong></td>
<td>Concern that data about individuals is readily available to people not properly authorized to view or work with this data</td>
</tr>
<tr>
<td><strong>Errors</strong></td>
<td>Concern that protections against deliberate and accidental errors in personal data are inadequate</td>
</tr>
</tbody>
</table>

PRIVACY AND IT

organizational practices that stand to affect privacy. Nor can they discount their customers’ concerns.

Given the increasing attraction of organizations and consumers to e-commerce applications, the privacy debate will continue to raise both security and data management issues. The future IT professional will not only need technical competency but an understanding of multinational, interorganizational, multidisciplinary (functional), and “people” (employee) practices.

Although you can view information privacy along several dimensions as discussed earlier, it is profoundly affected by IT functions such as e-commerce, database management, security, telecommunications, collaborative systems, and systems implementation (change management). Despite these interconnections, technology continues to remain ahead of the law—a trend compounded because organizations continue discovering new uses for technology. The growing use of IT in business will continue to trouble consumers and organizations across the globe if IT professionals fail to address their customers’ privacy concerns.

Julia Brande Earp is an assistant professor of management information systems in the Department of Business Management at North Carolina State University in Raleigh, North Carolina. Contact her at julia_earp@ncsu.edu.

Fay Cobb Payton is an assistant professor of management information systems in the Department of Business Management at North Carolina State University in Raleigh, North Carolina. Contact her at fay_payton@ncsu.edu.

Resources

- http://ecommerce.ncsu.edu/isp/All the Internet security and privacy research and articles conducted by the authors for North Carolina State University are posted here on the “Internet Security and Privacy Project of NCSU.”
- http://www.mgt.ncsu.edu/people/Earp.html: Learn more about Julia Earp’s research.

Data Communications, March 1999, pp. 37-50. Technologies and techniques such as firewalls, intrusion detection, and authentication can provide effective protection only when implemented correctly and consistently.

No single security method for protecting an internal computer network is unconditionally guaranteed. This is why people need to realize that a combination of proven policies, procedures, devices, and awareness is necessary to promote a secure networked environment. The computer network must be protected from external as well as internal threats.

Beyond security measures, IT professionals cannot discount the role of individual employees’ concerns about organizational practices that stand to affect privacy. Nor can they discount their customers’ concerns.

A though you can view information privacy along several dimensions as discussed earlier, it is profoundly affected by IT functions such as e-commerce, database management, security, telecommunications, collaborative systems, and systems implementation (change management). Despite these interconnections, technology continues to remain ahead of the law—a trend compounded because organizations continue discovering new uses for technology. The growing use of IT in business will continue to trouble consumers and organizations across the globe if IT professionals fail to address their customers’ privacy concerns.

Julia Brande Earp is an assistant professor of management information systems in the Department of Business Management at North Carolina State University in Raleigh, North Carolina. Contact her at julia_earp@ncsu.edu.

Fay Cobb Payton is an assistant professor of management information systems in the Department of Business Management at North Carolina State University in Raleigh, North Carolina. Contact her at fay_payton@ncsu.edu.

Training You Can Trust

From the IEEE Computer Society and five partner universities

Continuing education courses based on software engineering standards.

Computer Society 2000 Authorized Training Centers
- California State University, Sacramento
- New Jersey Institute of Technology
- Oregon Graduate Institute
- Southern Polytechnic State University
- University of Strathclyde

Course descriptions and registration information are available at computer.org/education/sestrain.htm

Software Engineering Standards-Based Training

Training Done Right