MUNICIPAL *Interface*

NOVEMBER 2000

MANAGING PRIVACY A CHALLENGE IN DESIGNING TODAY'S SYSTEMS

By Commissioner Ann Cavoukian, Ph.D. and Mike Gurski, Senior PolicylTechnology Advisor Ontario Information and Privacy Commission

These days, it has become common knowledge that any asset, process or service that can be digitized is going to be delivered over the Internet. For information systems managers, this is fundamentally good news, if only at the job security level. For private citizens who end up having personal information posted to the Internet, the picture is not so rosy.

Take the case of the City of Hamilton, Ontario it was recently reported that, in the name of good customer service and an innate desire to use available technology, the City placed the names, addresses and tax assessment of every Hamilton homeowner on the Web.

Much to Hamilton's credit, after a spate of e-mails from irate citizens, the acting director of information technology services removed the names of the property owners from the posted data. No sooner had the City revised its position than the data miners, such as the local real estate board, complained that the City had unilaterally made formerly public information private. Some said that the higher costs for accessing the tax assessment roles will be passed on to their clients.

It goes without saying that municipalities need to rethink the impact of digitizing what, in analog form, is a public record but not easily accessible. The ability to analyze, manipulate and mine a database or link it to other databases is a strong business driver, not only for municipalities but for private sector interests that can profit from analyzing and profiling those databases, such as the real estate board.

Nevertheless, what happens to the privacy expectations of the private citizen, whose personal information is often at the nub of this migration to a digital world?

Security Does Not Equal Privacy

To answer this question, information system managers are at a distinct disadvantage. The privacy vocabulary and its terrain are often terra incognita — or worse, wrongfully equated with security. Security, with its attendant arms of data integrity, authentication, confidentiality and non-repudiation, is a necessary requisite for privacy. Weak or inadequate security on an information technology platform or a simple database can quickly compromise privacy. Examples of this abound on the Internet, where hundreds of thousands of credit card files with personal information fall into the hands of hackers or the just curious with a depressing regularity.

While security is under the control of the information systems manager or somewhere up the organizational hierarchy, the ultimate control over privacy should be in the hands of each individual.

Privacy Defined

Privacy is person-centric. Security is organ ization-centric. In security architecture, it is a question of who in the organization has or can authorize access. So how is privacy defined? In the context of personal information, privacy can best be defined as follows:

"Personal control over the collection, use and disclosure of any recorded information about an identifiable individual."

An organization is responsible for safeguarding personal information in its custody or control. When faced with what to do with personal information on the job, question what personal information needs to be collected. Too often, the ease of collection and the capacity of technology to store and manipulate ever-increasing amounts of data silence the necessary up-front analysis regarding what personal information an organization needs from its citizens to conduct business.

Just as important as restricting collection is the idea of active containment. This concept covers the notions of use and disclosure of personal information. The recent Human Resources Development Canada (HRDC) collection of files, or "Big Brother Database" as the media portrayed it, serves as a case study in managing privacy. It illustrates the public backlash that can occur if the up-front analysis remains unfinished, in terms of both restricted and indirect collection of personal information, and the use and disclosure of personal information.

One could argue, as HRDC did, that all the information was necessary for policy analysis, and that the information was legitimately collected under the auspices of other programs, some not even federal. All this is true. HRDC did not break any privacy protection legislation at the federal, provincial or municipal levels, according to HRDC. However, there are dissenting opinions that cite lack of consumer consent, indirect collection and unauthorized use as violations.

Whatever the legal status, it is clear that the public's expectations of privacy are higher than HRDC's privacy protective information management practices. The public's concerns regarding privacy and its expectations continue to climb, as recent surveys indicate.

From an information system manager's perspective, the challenge in an HRDC-like scenario is to continue to provide the necessary information, while at the same time dismantling the collection files or databases that the organization relied on.

Like the City of Hamilton, HRDC had as its goal better customer service. To provide good customer service, in 1998 Victoria and Richmond, BC, published their tax rolls on the Internet in compliance with Section 361 of the BC Municipal Act. By moving from microfiche to digital information, however, the municipalities ran afoul of the BC Privacy Commissioner. His report made a number of recommendations, including that members of the public must be restricted to searching for properties by civic address only. Setting restrictions on search keys has had far-reaching implications for municipal services in BC.

Tools for Managing Privacy

It becomes apparent that designing and implementing privacy-protective information technology is a complex task. Apart from understanding applicable privacy legislation and public expectations of privacy, the information system manager has other demands. He or she needs to assess the technology - whether purchased, developed or used — for its privacy-enhancing characteristics as well as its privacy- i nvas ive characteristics.

Technology is not neutral when it comes to protecting privacy. Technology needs to be designed using privacy and technology design principles at hand. As well, privacy-impact assessments need to be used prior, during and subsequent to deployment of a technology project.

Armed with a basic definition of privacy, information systems managers next need to ask the right questions. These questions stem from the Fair Information Practices, developed by the OECD. These practices set the international standard for data protection and form the underlying basis for current federal and upcoming provincial private-sector legislation in Canada, as well as being the foundation of the European Union's dataprotection standards and legislation.

The four key questions to ask are:

Why are you asking for this personal information?

- Specify the purpose for collection and limit the information collected.

How will the personal information be used?

- Define the primary use of the information and place limitations on uses.

Who will be able to use the information?

- Within the organization, third parties and the individual who provided the personal information.

Who is accountable?

- For accuracy, security, access by individuals, independent enforcement, and an open and transparent set of practices.

These questions, in company with the underlying Fair Information Practices, form the backbone of two of the most important tools for addressing privacy: privacy/technology design principles and privacy impact assessments. These tools have many benefits. For a start, as they already exist, there is no need to re-invent them. As well, each has been used in a number of setti6gs and found to work for technology projects, whether in the birth throes or as mature, fully implemented systems. An example of a set of privacy/technology design principles is the set developed by the Ontario Information Privacy Commission and the US Justice Department, available through the commission's Web site, www.ipc.on.ca. A privacy impact assessment provides a framework for addressing the privacy implications at both a policy and technology level. The Ontario government is in the process of doing more than 20 privacy impact assessments. An assessment generally has three components:

- A map of the information or data flows associated with a given business activity;

- A privacy analysis of the data flow that examines whether fair information practices are being adhered to and reviews technical compliance with relevant statutory requirements; and
- An analysis of privacy issues raised by the proposal, including a risk assessment and a discussion of the options available for mitigating any risks that have been identified.

There are other resources available to the municipal information-systems manager. Most likely, there is already a privacy expert on staff, your municipality's Freedom of Information and Privacy Co-ordinalor. As well, most provinces have a Freedom of Information and Protection of Privacy Commission that has oversight responsibility for privacy legislation covering the municipal sector and can offer guidance and advice to municipalities.

Privacy is an issue that information systems managers will be called upon to manage and be accountable for, along with the more traditional aspects of their responsibilities. Using the tools and resources mentioned in this article can help assure success in managing privacy.