

Protecting PRIVACY

WENDY M. DUFF, PH.D., WALLY SMIELIAUSKAS, PH.D., CPA, CFE, AND HOLLY YOOS

AT THE CORE

THIS ARTICLE EXAMINES:

- the role of information professionals in privacy protection
- privacy legislation
- a privacy audit

In the May 1999 issue of *The Economist* bearing the cover title "The End of Privacy," the author of the lead article argues that the benefits of the new information economy, such as safer streets and better services and products, more than offset the costs of loss of personal privacy. However, the article also documents a growing concern about protection of personal information. This concern will only intensify as controlling the mounting volume of personal information available to third parties becomes more difficult. Further, the editor of *The Economist* argues that one would have to go to extreme lengths today

to preserve a level of anonymity common just 20 years ago. In fact, personal privacy may become one of the most endangered resources of the 21st century.

One means for helping to preserve the privacy of personal information is a privacy audit. Privacy audits are one way to monitor and influence the level of privacy protection maintained by organizations, governments, or systems. Reports by privacy auditors can assure individuals that organizations adhere to privacy standards and that those organizations that pledge to protect privacy actually do so. A records and information professional can play a key role in the privacy audit because privacy protection requires that organizations adopt recordkeeping and disclosure practices consistent with their own policies and legal requirements that affect them.

A new perspective on privacy protection focuses on (1) the roles of information professionals and auditors and (2) how they can collaborate to strengthen privacy. Broader organizational controls for protecting

privacy, notably the roles of privacy commissioners and organizational privacy policies, are also addressed in the following sections.

Privacy Defined and Legislative Framework

The right to privacy is a fundamental right that should be guaranteed to all individuals. *Privacy* has been defined as "the claims of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about themselves is communicated to others (Westin 1967)." The *loss of privacy*, according to a *Yale Law Journal* article, is the "extent to which we are known to others; the extent to which we are the subject of others' attention; and the extent to which others have physical access to us" (Gavison 1980). Even more simply stated, *privacy* is the "right to be left alone" (MacNeil 1992). Individuals differ as to the types of information they want to protect, because ultimately privacy is personal and subjective.

During the last 20 years, society has increasingly focused attention on

issues surrounding privacy. This trend seems to be a reaction to the dramatic decline in privacy as documented in *The Economist* article. These concerns arise over the quantity of information known about a person and the technological advances in accessing it via computerization, telecommunications, and monitoring. Citizens have voiced special concern over the government's use of information and, in particular, its ability to use computers to link or match data about individuals from multiple sources. This issue of privacy is one of the most important and complex ethical issues facing society today.

Many governments have passed data protection legislation to prevent misuse of personal information by government. The underlying principle of this legislation is that information that citizens must disclose to government should be protected – not used for purposes other than that for which it is collected – and not improperly disclosed to others. In Canada, for example, the federal government and some provincial governments have passed privacy legislation to protect citizens against the misuse of personal information collected by the government. In the United States, the Privacy Act of 1974 protects personal information captured in records held by government agencies. Some equivalent statutes have been passed at the state level as well. In Australia, the

Of course, issues of protecting personal information extend beyond personal information collected and maintained by government institutions. Efforts have been made in some jurisdictions to address the protection of personal information collected and maintained by private sector organizations. In Europe, for example, control of information by the private sector is regulated by the Organization for Economic Cooperation and Development's (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Organization for Economic Cooperation and Development 1981) and the Council of the European Union's (EU) *Convention for the Protection of Individuals with Regard to the Processing of Personal Data* (Council of the European Union 1981). In addition to these instruments, the European Union has also enacted the *Data Protection Directive* that attempts to harmonize data protection laws throughout the EU. The *Directive* requires EU members to enact complementary legislation and "imposes an obligation on member states to ensure that the personal information relating to European citizens is covered by law when it is exported to, and processed in, countries outside Europe" (Electronic Privacy Information Center and Privacy International 2000).

In Canada, comprehensive privacy protection legislation for the private

and, potentially, segments of the provincially regulated private sector as well. This Act, Bill C-6, is modeled on the Canadian Standards Association's *Model Code for the Protection of Personal Information* developed in 1996 and based in large part on the OECD *Guidelines*. The primary objective of the Code is to assist organizations in developing and implementing policies and practices to be used when managing personal information (Canadian Standards Association 1996).

In Australia, rather than introduce federal privacy legislation that would apply to the private sector, the Prime Minister directed the Privacy Commissioner to develop voluntary codes of conduct for the private sector. In 1998, the Privacy Commissioner released these voluntary codes as National Principles. The Principles detail guidelines for the fair handling of personal information. In 1998, the federal government announced its intention to introduce "light-touch" legislation that would apply to the private sector and be based on the National Principles. Under the proposed legislation, those in the private sector will be allowed to develop their own codes for protecting the privacy of personal information, including its collection, storage, use, and disclosure. If organizations fail to develop their own codes, the legislation provides default privacy rules (Attorney General [Australia] 1999). In the meantime, some pieces of legislation protect personal information in specific industries or functions, such as telecommunications, medical research, and credit reporting.

In the United States, no privacy law applies to the private sector generally. Such federal legislation has been broadly debated, but few initiatives have moved forward into law. However, piece-meal legislation applies to specific sectors, functions, or areas of information such as financial records, educational records, telephone records, and credit reports at both the federal and state levels.

**...Information that citizens must disclose
to government should be protected...
and not improperly disclosed to others.**

principal federal statute, the Privacy Act of 1988, contains 11 Information Privacy Principles that apply to the records of federal government agencies. Australian states also have privacy laws that apply to government records.

sector may be forthcoming. The Canadian federal government has introduced the *Personal Information Protection and Electronic Documents Act*. This legislation would extend privacy legislation to segments of the federally regulated private sector

Within the context of regulatory environments, perceptions of privacy are often culturally and politically bound. As noted in an article in *CA Magazine*, in Europe privacy is generally viewed as a basic human right, while in the United States, privacy tends to be viewed more as an economic good that can be sold or exchanged (McKendry 1996). For example, in the United States, one individual launched a court case against a company that sold his name to another company for marketing purposes. This individual argued not that his privacy had been violated but that the company had violated his property rights by selling his name. Thus far, in Canada and Australia, privacy seems to fall somewhere in between these two extremes, although the sale of names via marketing lists remains common practice (McKendry 1996).

This discussion of privacy legislation and codes provides a context for understanding privacy audits as discussed in the balance of this

organizations outside of the EU fail to meet the standards of personal information protection established in the EU's *Data Protection Directive*, they may not be able to conduct certain types of business within Europe. Reducing such information risk is a primary objective of auditing. For example, accounting auditors reduce (to an acceptable level) the chance that a financial statement is incorrect (Robertson and Smieliauskas 1998).

Risk management is a process that manages inherent risk, including fraud, noncompliance with laws, regulations, costs, competition, and change, by identifying

- potential risk
- potential impact of that risk on an organization or organizational unit
- controls that reduce the risk
- quality of the controls
- possible impact of any residual risk

Documentation, including policies, standards, and processes, is an essential component of an organization's control structures.

The risk of these organizational controls failing to manage inherent risks is referred to as "control risks." Control risks can occur from flaws in the design of the organizational controls and/or failure of the controls to operate as intended. To reduce the risk that invasions or breaches of privacy will impact negatively on an organization, an auditor must identify the types of personal information that are confidential, the processes associated with this type of information, the controls connected to these processes, and the possible outcomes if information is not protected.

The word "auditor" originates from a Latin word meaning "to hear"; in ancient times auditors listened to the oral reports of responsible officials (stewards) to owners or those having authority. They confirmed the accuracy of the reports. Over the centuries the role of auditors as verifiers of official reports evolved to include that of written records.

Controls are essential to protecting privacy. Controls include the development of a privacy policy and the creation of procedures and other documentation for carrying out the policy. Training is necessary to ensure that all staff members understand the policy and procedures. The privacy audit then determines whether the organization is in compliance with the policy. The degree of inherent and control risks related to the privacy of personal information determines whether the control system is effective enough for privacy objectives to be met.

Auditing as a profession arose out of the need for accountability in what can be best described as a "three-party accountability relationship." In a three-part accountability relationship, at least three parties with distinct social roles are always involved. One party is the **user** of

Documentation, including policies, standards, and processes, is an essential component of an organization's control structures.

article. An organization's legislative and policy environment is a key component in a privacy audit's assessment of acceptable risk.

Risk Management and Audit

Organizations face many different types of risk, and an auditor must evaluate each relevant type the organization faces. Auditors define *risk* as anything that will prevent the enterprise from meeting its objectives. Organizations may risk possible litigation, loss of business, and loss of reputation if they do not protect the privacy of their customers and staff. For example, if government

Risk management does not wholly eliminate risk because the cost of implementing controls sufficient to eradicate **all** risk is rarely justified. Therefore, the main objective of risk management is to reduce risk to a manageable level. Changes in an organization's structure or environment impact the level of risk. Therefore, the assessment of risk is a continual process.

A control structure reduces risk to a manageable level because it reduces the probabilities of errors or irregularities. Control includes an organization's resources, its processes, systems, culture, and other things that help it meet its objectives.

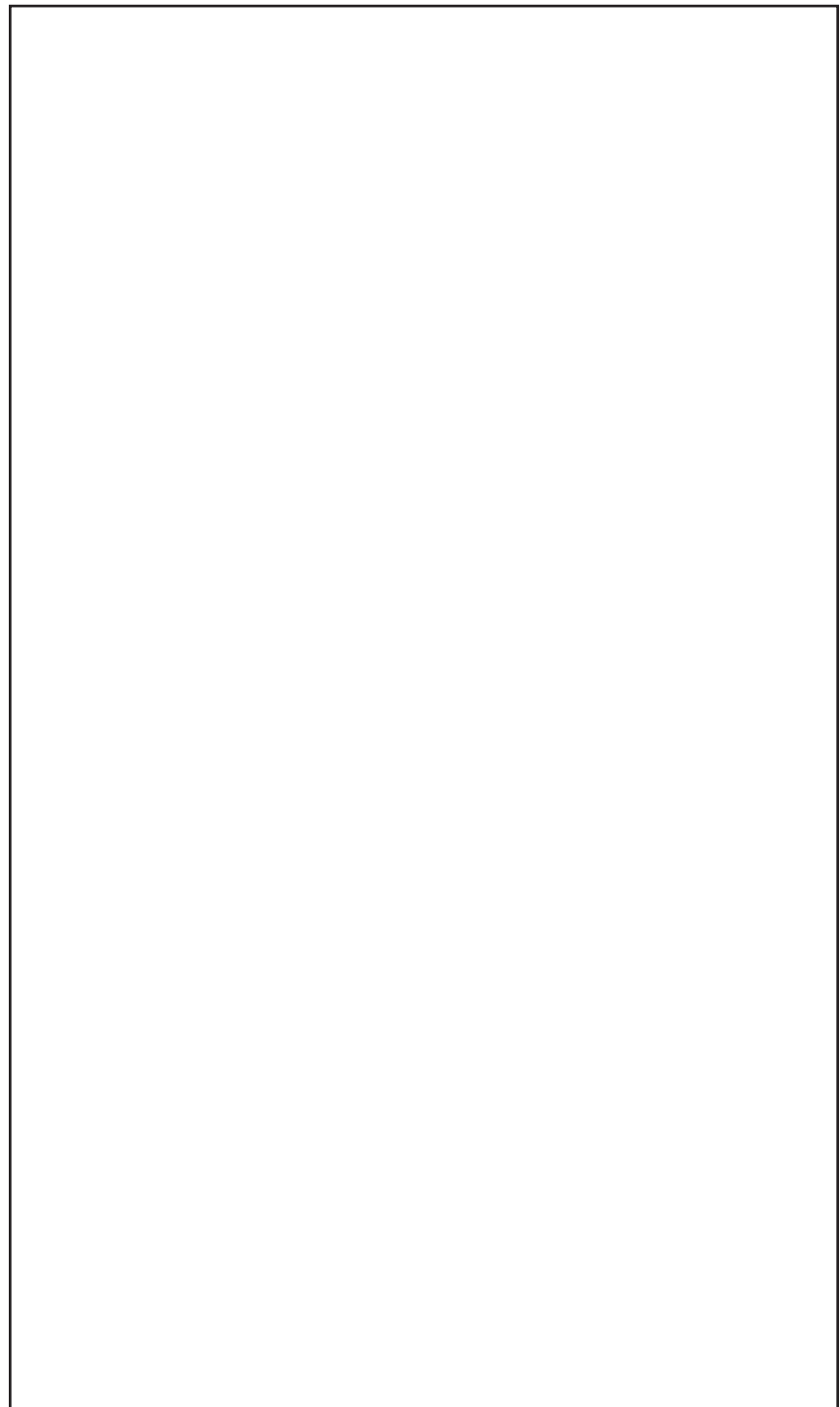
some information (e.g., records) who relies on the accuracy of this information (i.e., the risk with using the information is low). A second party is the **preparer** who has the responsibility for preparing this accurate information (e.g., managers, accountants, or records analysts employed by management to act on their behalf). However, experience has shown that the user can't always rely on the preparer of the information for its accuracy, especially if the preparer is in a conflict-of-interest situation. For example, a common type of conflict of interest arises when the information is about the preparer's performance, which creates a potential bias in the information. In such circumstances, an independent third party may be needed to verify the accuracy of the information to the user. The third party serves the role of the **auditor**.

In modern society, the primary role of auditors has been to facilitate economic accountability of management to owners (investors, taxpayers, and other providers of capital). This accountability of management to owners is achieved through the use of annual financial statements prepared in accordance with standardized and generally accepted accounting principles. The auditors' role is to verify conformity with these principles. In essence, auditors are required because the users of financial statements do not sufficiently trust management to prepare accurate financial statements and cannot prepare them themselves. For example, inflating earnings so that they can get a higher bonus may be in managers' self-interest. Similar problems can arise in other contexts whenever a responsible party is put in charge of other people's money or other resources. If the risk of bias or deception is high (i.e., information risk is high), then three-party accountability is demanded, and the auditor is called in. Three-party accountability relationships tend to increase as the complexity of society and social relationships increases.

For this reason, as information risks have increased the importance of auditors has also grown.

Usually audit criteria (e.g., relevance, reliability, neutrality, and completeness) will need to be tailored to the objectives of a particular audit engagement. That is, they must be relative to the particular accountability relationship that is the

subject matter of the audit engagement. For example, criteria for the effectiveness of healthcare services are quite different from those, for example, of a fire department. In many aspects of the engagement, the auditor must exercise professional judgment to tailor evaluative criteria and standards to a specific engagement. For example, auditors are



developing more efficient ways of conducting traditional financial statement audits through knowledge of the auditee's competitive environment and related strategic plans. In other engagements, the auditor may need to develop innovative criteria unique to the engagement. In such situations, intimate knowledge of the auditee organization and its accountability needs become particularly important.

Evaluative criteria also need to be invoked in the conduct of privacy audits. Here, privacy objectives are operationalized by suitable criteria or code that must be met such as the Canadian Standards Association's *Model Code for the Protection of Personal Information*, as discussed.

A privacy audit is merely an extension of audit practices to the realm of personal information. As with other types of audits, the privacy audit is primarily a verification that a system of privacy controls is in place and functioning. The level of controls required is in turn a function of the risks that the privacy goals will not be met. The combination of inherent and control risks determines the effectiveness of the system designed to meet privacy objectives.

Auditors are increasingly extending the scope of their work to new subject areas such as privacy audits involving the collection and use of private information on commercial Web sites. Such privacy audits facilitate the growth of electronic commerce by providing assurance to customers on privacy and security concerns.

With respect to privacy audits in traditional organizations, a key control is the organization's record-keeping system; in particular, records professionals and their duties related to information used by the organization. The records analyst can and should be a key component to preserving privacy of all types of information in large organizations. Privacy audits, therefore, tend to focus on testing the controls and evaluating the effectiveness of this function.

A primary objective of a privacy audit is to evaluate the overall effectiveness of controls in meeting the privacy objectives. Therefore, the most important part of an auditor's report concerns overall effectiveness of controls in meeting the privacy objectives. Audit reports, however, also may list various findings, particularly weaknesses, to assist management in improving adherence to its privacy policy. The focus on weaknesses tends to make auditees defensive and feel threatened when being audited. So, the auditor must have good interview and interpersonal skills and attempt to develop a balanced evaluation that considers not only control risk but also inherent risk along with the costs and benefits of various controls.

Therefore, auditors need to be knowledgeable about the auditee and concerned about being overly alarmist in dealing with sensitive subject matters such as personal privacy. An illustration of the importance of these issues is given in the next section.

Some organizations have used privacy audits as a tool to assess compliance with privacy laws and policies and to evaluate accompanying risks. For example, the office of the Australian privacy commissioner conducts privacy audits of government agencies and organizations to assess structures and controls implemented by management to ensure that records containing personal information are maintained in accordance with Australia's Privacy Act. After such an audit, a draft report outlining findings and recommendations is prepared. The subject of the audit then submits a formal response. The final audit report is composed and formally submitted to the privacy commissioner (Australian Privacy Commissioner 2001). These reports reveal weaknesses in the implementation of the Privacy Act, including problematic trends. The office of the privacy commissioner also offers training seminars to government agencies to

clarify the obligations of agencies under the Privacy Act (Office of the Federal Privacy Commissioner 1999).

A Case Study

Scope

From July 1998 to September 1999, the authors conducted a privacy audit of personal information of faculty and staff collected and maintained by a large Canadian university. The audit had two objectives: (1) to assess whether the university's goals regarding the protection of faculty and staff personal information were effectively met during the period May 1, 1995, to April 30, 1999, and (2) to determine whether the existing level of protection provided by the privacy policy was appropriate.

The project team members included a professor from the university's Faculty of Information Studies, a professor from the university's School of Management, and a records analyst from the university's Archives and Records Management Services Department.

Choice of Subject

The university selected for the audit project is a large Canadian institution with approximately 53,000 students and 6,000 faculty and staff. The organizational and physical structure of the university is complex and supports a wide variety of programs spread over three separate campuses.

The university was a desirable case study subject for several key reasons:

- The project's team members were already familiar with the university's administration and could readily identify stakeholders in the management of personal information, and team members could also use established personal and professional contacts within the university to gain access to those with responsibility and to facilitate cooperation.
- The university had recently implemented the human resources

module of an electronic enterprise information system, and this event marked a fundamental change in the technology used to manage personal information. Therefore, an investigation of the university's management of personal information was timely.

- The university had an access and privacy policy in place, and the university's Policy on Access to Information and Protection of Privacy outlined how personal information could be collected, used, and disclosed. The policy also provided for the appointment of Freedom of Information and Privacy Protection officers

sector. The exact scope of the bill was unclear, but it could potentially apply to Canadian universities not currently covered by provincial access and privacy legislation. These proposed changes to the surrounding legislative environment could have a direct impact on the management of personal information within the university if they become reality.

- The project's team members believed that the university culture, as an academic research institution, has fostered a greater awareness of privacy issues among its populace than other types of organizations. For

engagement letter and the project in general. Once the scope and nature of the project were defined, the team developed a questionnaire to act as a guiding instrument when conducting interviews with university staff. While scheduling and conducting interviews, the project team undertook a formal comparison of the university's privacy policy with the elements of the Canadian Standards Association's model privacy code encapsulated in Bill C-54 (Canadian Standards Association 1996).

The project team's first step was to approach the university's privacy commissioner to define the scope and nature of the audit. The commissioner was particularly interested in learning how well the privacy policy was working from the perspective of university employees. The commissioner had played a key role in creating the policy, and no specific monitoring of the effectiveness of the policy had been instituted since its inception in 1995.

In consultation with the privacy commissioner, an engagement letter was drafted that identified the objectives of the engagement and authorized conducting the audit. The engagement letter also defined the purpose and scope of the audit, terms of reference, detailed procedures, and assistance required. The engagement letter was important for soliciting the support and cooperation of the university administration and planning for the audit.

With the terms of the engagement set out in the engagement letter, the project team scheduled meetings with key senior university administrators involved in managing faculty and staff personal information at the university. These meetings included senior personnel in the human resources, internal audit, and information systems areas. The project team used these meetings to refine the scope of the project and provide these key senior administrators with the opportunity to provide input into the nature of the project and the engagement letter. It was also a key

...the university culture, as an academic research institution, has fostered a greater awareness of privacy issues...than other types of organizations.

who would work with a university Freedom of Information and Privacy commissioner to handle access requests and resolve disputes. The university's privacy policy provided an important benchmark for the project team to use when evaluating how the institution was managing the personal information of its faculty and staff. Moreover, the policy had not been actively monitored since its introduction, and little assessment of its success or failure was available.

- In 1999, the Canadian federal government had introduced Bill C-54, the Personal Information Protection and Electronic Documents Act (although it was later reintroduced as Bill C-6, at the time of the audit it was Bill C-54 and is referred to as such throughout this case study), which proposed applying privacy standards for personal information to segments of the private

example, the university has developed guidelines for protecting the personal information of humans used as subjects in academic research. University faculty wishing to undertake research involving human subjects must apply to the university's ethics committee for approval. The approval process includes an assessment of research aspects, such as access to records and security of data. The project team felt that a heightened awareness of privacy issues may help bring to light any potential problems or issues.

Process

The privacy audit consisted of a number of related components. One of the first activities was to engage in preliminary discussions with the university's privacy commissioner. In concert with this discussion, the project team held informal meetings with key senior university administrators to provide input into the

means to solicit the support and cooperation of these administrators. Informal discussions at these meetings also helped the project team better understand the management of personal information at the university. Discussions focused on relevant university policies, common procedures, and possible problem areas. Existing documentation for related procedures was identified and obtained. Possible problem areas identified during these meetings proved to be invaluable when developing the audit's interview questionnaire.

An interesting finding of the study regarding audit procedures is that questionnaires prepared by privacy auditors in other contexts were much too detailed and procedural for this audit. These more traditional questionnaires took up too much valuable administrator time, especially given the lack of pre-existing formal controls in the auditee organization. A briefer, pointed questionnaire that was more people-oriented and focused on the staff that would make the difference in determining the effectiveness of the policy was much more effective. The authors' familiarity and knowledge about the organization being audited probably made this approach feasible. Many auditors do not have as intimate a knowledge of their subject matter. Nevertheless,

An audit questionnaire was used to interview university administrative staff from a broad cross-section of university offices. The project team interviewed administrators from both central and decentralized administrative offices and from both the downtown and suburban campuses. The questionnaire covered topics such as accountability for protecting personal information, purposes of collecting personal information, the limitation of use and disclosure of personal information, and the retention of personal information. Interview questions also dealt with issues of identifying personal information, safeguarding personal information, and providing access to an individual's own personal information.

The project team conducted the interviews in a manner that would best provide them with accurate and unbiased data. For example, the project team made a conscious effort to keep a low profile during the privacy audit. The team did not want to raise awareness of privacy issues in advance of conducting interviews for fear of influencing interview results. For the same reason, the project team maintained an informal atmosphere during interviews to encourage honest responses. The team did not want to appear as assessors who would be reporting procedural failings of staff members to their

policies and procedures were in place and implemented while more junior staff reported differently. Even where staff claimed that privacy of faculty and staff personal information was well protected within the university, probing questions regarding details of privacy administration often revealed potential problems.

At every possible occasion, the project team sought to identify and obtain copies of relevant documentation. However, the project team soon became aware that little documentation that detailed procedures for managing personal information of faculty and staff existed. Of the documentation that did exist, by far the richest was found in the internal audit and human resources areas. Because so little documentation existed, the interview component of the privacy audit became increasingly important.

This change was an important departure from traditional audit practice in which oral evidence is not treated as very reliable. However, the project team found, consistent with some of the newer audit approaches being developed, that oral evidence cannot only be made reliable but also indispensable in obtaining the types of information not normally documented. People's attitudes, expertise, and trustworthiness may be critical when formal procedures to assure adherence to a policy are lacking. For example, the project team found that even when senior staff members were unaware of the policy, their intuition – probably based on many years of a shared culture within the university – was largely in conformity with the policy. In retrospect, this revelation is not surprising because the shared culture was largely reflected in the policy in the first place. Thus, what at first appeared to be a major flaw of the system proved in practice not to affect implementation of the policy. From an archival perspective, oral evidence in the form of inquiries and interviews provide a type of meta-record of the effectiveness of

**...in-depth knowledge of a client
is critical to the effectiveness and efficiency
of all audits.**

the experience illustrated the importance of such knowledge to the point the authors could confidently change the audit approach. As noted earlier, the auditing profession is increasingly recognizing that in-depth knowledge of a client is critical to the effectiveness and efficiency of all audits.

managers. The team also interviewed staff at various levels within the university and discovered that often staff at different levels had differing perceptions of how well privacy was protected within the university. For example, senior administrators often reported that awareness of privacy

the functioning of an information system such as that associated with personal data.

The university's Internal Audit Department had undertaken an implementation audit of the human resources module of the university's

The comparison chart revealed, for example, that the university's policy does not require that the purpose of collection be identified in advance, documented, and communicated.

After completing the formal interviews, the policy comparison, and

management professionals. Some recommendations were developed via an analysis of practices invoked by offices to address similar functions or problems. For example, the university requires that division heads sign an accountability report to confirm that they are in compliance with financial management policies. The audit report recommended that this concept be applied to confirm compliance with privacy policies as well.

The recommendations concern raising awareness of the privacy policy, implementing the privacy policy, addressing risks posed by technological changes, and the role of Internal Audit. Perhaps the key recommendation was to develop further general documentation practices and procedures, including an annual accountability report acknowledging awareness of the policy and listing policy implementation procedures that are submitted by division heads to the privacy commissioner, training and awareness, ongoing monitoring, and other general documentation and procedures. The report noted that the records analyst could be charged with developing many of these procedures under the approval of the privacy commissioner. If accepted, this responsibility could be an important new role for the records analyst.

Project Benefits

The privacy audit project successfully met the goals of the project team. The academic team members concluded that the audit process could be a quite valuable function for information management professionals. Audit has been practiced for many years in other organizational areas and, therefore, has fully developed methodology and procedures for use. Bringing audit practice into the records management realm means that records professionals have the benefit of a fully developed model as well as the credibility and authenticity that the audit process brings.

**The privacy audit report contained...
recommendations for improving
the management of faculty and staff
personal information at the university.**

enterprise system. The project team reviewed the working papers generated by Internal Audit during their system implementation audit to determine whether Internal Audit included consideration of privacy concerns in their audit of the system and whether the human resources system and surrounding procedures were in compliance with the university's privacy policy.

Concurrent with the development of the formal interview questionnaire, the project team undertook an analysis of the university's privacy policy by comparing it to other privacy policy standards. Such a comparison allowed the project team to determine whether the university's privacy policy was more, or less, stringent than other privacy standards. The standard selected for the comparison was the Canadian General Standards Board's *Model Privacy Code* that, incidentally, had been incorporated into the federal government's Bill C-54. The project team compiled a chart that detailed each element of the privacy model code and compared it to the university's policy. The chart made note of differences, evaluated their significance, and speculated as to their potential impacts. The elements examined matched those included in the interview questionnaire such as accountability, purpose of collection, limiting use/disclosure/retention, accuracy, safeguards, and openness.

the review of Internal Audit working papers, the project team met to compose the privacy audit report with its several recommendations. Structured according to common audit practices, the audit report detailed the audit objectives, criteria, and responsibilities of management and the audit project team. The report detailed weaknesses and strengths discovered during the audit and included general conclusions. The bulk of the audit report described the audit findings, with each finding followed by a recommendation.

The draft audit report was forwarded to the original senior administrative stakeholders for comments, corrections, and rebuttals. A revised draft report was then forwarded to the university's privacy commissioner for informal comment and criticism. The project team then finalized the report and formally submitted it to the university's privacy commissioner.

The privacy audit report contained a number of recommendations for improving the management of faculty and staff personal information at the university. Most often, these recommendations were developed through the observations of the project team, and best practices were identified through interviews with administrative staff. Some recommendations came from the expertise and experience of the audit project team as audit and information

Analyzing privacy issues in a case-study environment substantially heightened team members' understanding and appreciation of the difficulties inherent in maintaining the privacy of personal information. The role and impact of different contextual factors, such as new technologies, organizational culture, administrative structure, and other factors, became very clear when examined in a real-world environment.

The project also did a great deal to promote each member's understanding of the audit and information management fields and the relationship – and possible partnership – between them. Regular team meetings became a forum for discussion and debate on topics relating to the two fields. In essence, these meetings evolved into an informal knowledge-sharing exercise with each team member contributing to each other's understanding.

The privacy audit also gave value to the university generally and to the university's privacy commissioner specifically. The audit identified and evaluated the university's policies, procedures, and practices surrounding the management of personal information and made note of areas of weakness and best practice. Associated risks were identified, described, and evaluated, and appropriate recommendations were developed.

Moreover, the audit provided opportunities to promote the university's own information and records management programs. Many of the recommendations in the final audit report discussed how adherence to developed records management policies and procedures could help protect the privacy of university faculty and staff personal information. Meetings and interviews with the university administration to conduct the privacy audit also supplied the project team with opportunities to promote the role of the university's records management program. When appropriate, the team could refer

university administrators to relevant policies, procedures, services, and products developed through that program.

Furthermore, the privacy audit helped the records analyst establish a network of senior administrative contacts, including officials from the Human Resources, Internal Audit, and Information Systems Departments. The benefit of having established contacts with these individuals will extend beyond the parameters of the privacy audit itself.

Additionally, the privacy audit provided the records analyst team member with limited access to the university's enterprise system. Under the auspices of the privacy audit project, the records analyst was provided with access to the "sandbox" enterprise system from which system functionality could be deduced. System training was also provided along with supporting systems information such as user access profiles. This information was not only essential to the privacy audit but is also essential to the analyst's regular duties.

Finally, the privacy audit team suggests that from their foundational efforts the privacy audit may be used as the basis of further study and research. Opportunity to conduct similar privacy audits exists in other environments, and lessons learned from this study will make a useful contribution to them.

Of course, the privacy audit was not without significant challenges. Primarily, the project team struggled with finding a common language for discussing the privacy audit both among themselves and with other stakeholders. Team members and stakeholders had unique perspectives to bring to the project, which, while enriching the process, made consensus difficult to achieve.

Conclusion

The privacy audit was a great learning experience in several respects. First, privacy audits can be

very important in monitoring the effectiveness of privacy policies to protect personal privacy. Second, a key formal control in implementing privacy protection is the issuance of regular accountability reports prepared with the help of information and records management professionals. Third, information management professionals must play a part in the privacy control system. Fourth, the knowledge of the entity and subject matter is essential in conducting the audit, especially in evaluating the less formal controls.

In this audit the informal controls were sufficient for protecting the personal privacy of employees in the organization. The authors' knowledge of the organization audited, as well as oral evidence based on interviews and inquiries, was critical to evaluating the competence and trustworthiness of the staff that allowed the informal controls to function so effectively. However, this situation may be unique to the university environment used in this case study that continues to maintain a number of long-term senior employees. Many organizations experience significant staff turnover at all staffing levels. This turnover weakens the informal controls and consequently requires strengthening of compensating formal controls so that privacy objectives continue to be met in the future. In this study, the organization is expected to undergo significant staff turnover as a result of a wave of retirements expected for the "boomers" hired in the 1960s. Consequently, the formal controls must become better developed and will become increasingly important in maintaining privacy objectives.

The real measure of success for the privacy audit will be whether the university's privacy commissioner chooses to accept and adopt the project team's recommendations as outlined in the privacy report. He included a copy of the privacy report in his final report to the commissioner, but he has not formally accepted or

rejected the recommendation. By coincidence, the report was submitted to the commissioner's office just as a new privacy commissioner was taking on the position. The project team eagerly awaits the new commissioner's response. **U**

ABOUT THE AUTHORS: *Wendy M. Duff, Ph.D.*, is an assistant professor in the Faculty of Information Studies at the University of Toronto, Ontario. She has been in the information management field, specializing in records management, electronic records, archives management, and metadata, for 20 years. She is a member of ARMA International and the Association of Canadian Archivists. Duff received her doctorate from the University of Pittsburgh. She may be reached at duff@fis.utoronto.ca.

Wally Smieliauskas, Ph.D., CPA, CFE, is a professor of accounting at the University of Toronto School of Management. He has been in the accounting field, specializing in information systems audit and accounting information systems, for 32 years. He is a member of the American Accounting Association and the Canadian Academic Accounting Association. The faculty of the School of Management at the University of Toronto presented him with an award for outstanding contributions to the MBA in accounting. He has authored textbooks in the auditing area and received a research award from the Peat, Marwick, Mitchell Foundation. Smieliauskas received his Ph.D. from the University of Wisconsin-Madison. He may be reached at smieli@mgmt.utoronto.ca.

Holly Yoos is a senior records analyst with University of Toronto, Development and University Relations. She has a master's degree in archival studies and six years information management experience. Yoos' specialty is in information system development and implementations. She is a member of ARMA International and AIIM International. Yoos may be reached at holly.yoos@utoronto.ca.

REFERENCES

- Attorney General (Australia), *Further Consultation on National Privacy Legislation*. News release, 30 November 1999. Available at http://law.gov.au/aghome/agnews/1999newsag/657_99.htm (accessed 5 March 2001).
- Australian Privacy Commissioner. *Privacy and the Private Sector*. Available at www.privacy.gov.au/private/index.html (accessed 5 March 2001).
- Canadian Standards Association. *Model Code for the Protection of Personal Information*. Etobicoke: Canadian Standards Association, 1996. Available at www.media-awareness.ca/eng/issues/priv/laws/csacode.htm (access 12 March 2001).
- Council of the European Union, *Convention for the Protection of Individuals with Regard to the Processing of Personal Data*. Strasbourg, France: Council of Europe, 1981.
- Electronic Privacy Information Center and Privacy International. *Privacy and Human Rights 2000: An International Survey of Privacy Laws and Developments*. Available at www.privacy.org/pi/survey/index.html (accessed 5 March 2001).
- Gavison, Ruth. "Privacy and the Limits of Law." *Yale Law Journal* 89 (January 1980): 241-471.
- MacNeil, Heather. *Without Consent: The Ethics of Disclosing Personal Information in Public Archives*. Metuchen, NJ: Scarecrow Press, 1992.
- McKendry, David. "Peep Show." *CA Magazine* (September 1996): 19.
- Office of the Federal Privacy Commissioner. *Eleventh Annual Report on the Operations of the Privacy Act for the Period 1 July 1998 – 30 June 1999*, 61.
- Organization for Economic Cooperation and Development. *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Paris: OECD, 1981.
- Robertson, Jack C., and Wally J. Smieliauskas. *Auditing & Other Assurance Engagements*, 1st Canadian Ed. Toronto: McGraw-Hill, 1998.
- Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.