PRINCIPLES FOR PROTECTING INFORMATION PRIVACY

Julie Gable, CRM, CDIA, FAI

When it's done well, information privacy protection is part of an organization's policy and procedural infrastructure, working in the background like a silent sentinel that few realize is constantly on alert. When it's done poorly, it makes headlines and ripples through an organization from the cubicles to the board room.

Media reports tend to make privacy protection synonymous with cybersecurity, and some resources, such as the EDRM's Information Governance Reference Model, take the position that while business, legal, and records and information management (RIM) stakeholders have input, it is IT's responsibility to manage the information protection environment.

Protection, though, is as much about policy and procedural issues as it is about technology activities. Anti-hacking and anti-theft measures, for example, can exist only as the result of well-defined policies that are made in response to laws governing collection, storage, transfer, retention, and disposition of private information and the assignment of privacy protection responsibilities.

The Push for Privacy

The states of Massachusetts and Nevada have enacted tough privacy laws, and members of the U.S. Congress are moving forward with cybersecurity legislation aimed at protecting private information. Meanwhile, privacy experts are advocating that individuals have the right to control the collection and use of their personal data, an idea embodied in many European laws. Organizations, therefore, find themselves squeezed between pressures from lawmakers and customers.

Privacy breaches are expensive for business. According to the Ponemon Research Institute's "2014 Cost of Data Breach Study: Global Analysis," the average cost for each stolen or lost record containing sensitive or confidential information is $145 (U.S.). Considering that Verizon's "2012 Data Breach Investigations Report" showed that 95% of the 174 million records compromised worldwide in 2011 contained personal information, the total cost is significant. What's worse is the potentially irreparable harm to customer confidence in the breached organization and its impact on future business.

Privacy breaches can be costly for careers, too. In some cases, high-level executives have lost their jobs, and in the high-profile incidents at Wyndham Worldwide and Target, sharehold-

ers brought lawsuits against their respective boards alleging that board members failed to take reasonable steps to maintain their customers' personal and financial information in a secure manner.

But, determining what "reasonable steps" are is a mammoth task in an environment that is a complex tangle of evolving state, national, and international information privacy laws, industry regulations, human behaviors, and physical and electronic systems.

- Centralized access controls
- Well-defined confidentiality and privacy considerations
- A defined chain of custody when appropriate
- Training for employees

Level 3 of the IGMM also notes that the organization will have defined, specific goals related to records and information protection. Finally, protection notes that an organization's audit program should have a process to "ascertain whether sensitive information is being handled in accordance with the outlined policies in the principle of protection."

One complicating factor in addressing protection for private information is that it will likely involve several functions.

Privacy Protection Principles

Two well-known sets of principles offer a starting point for making sense of what is required of organizations and knowing what to do and in what order: the Generally Accepted Recordkeeping Principles® (Principles) and the Generally Accepted Privacy Principles (GAPP).

Principle of Protection

One of the eight Principles from ARMA International, the Principle of Protection, notes that an information governance (IG) program should be designed to offer "a reasonable level of protection to information that is personal or that otherwise requires protection." The context for this principle says that the program must ensure that "appropriate protection controls are applied to information from the moment it is created to the moment it undergoes final disposition." It also specifically includes electronic systems as well as physical systems.

A look at the Principles' complementary Information Governance Maturity Model (IGMM) reveals that elements of protection considered "essential" (Level 3 of the IGMM) include:

- A formal, written policy for protecting records and information

One complicating factor in addressing protection for private information is that it will likely involve several functions. In large organizations, it's common to find compliance officers, privacy officers, legal counsel, and IT and RIM professionals involved. In smaller concerns, the task may fall predominantly on whomever has responsibility for RIM and/or IT. The key to progress in either situation is to find useful guidance that can provide a consistent understanding of concepts and reliable information on how to proceed.

GAPP

The American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA) developed GAPP to help organizations design and implement privacy programs based on sound privacy practices and policies that address obligations, risks, and business opportunities. Although it was designed by accounting organizations, GAPP's focus is not solely on financial services.

Just as the Principles are based on ISO 15489: 2001 Information and documentation – Records management – Part 1: General), GAPP is based on ISO 27002 *Information technology – Security techniques – Code of practice for information security controls.* Although ISO 27002 has much to say about specific technologies, GAPP is technology-neutral.

Among the useful features of GAPP are standard definitions of privacy, personal information, and sensitive information. GAPP defines *privacy* as "the rights and obligations of individuals and organizations with respect to the collection, use, retention, disclosure and disposal of personal information."

Personal information is further defined as information that is about or can be related to an identifiable individual, including such items as name, home, or e-mail address, identification number such as Social Security number or social insurance number, physical characteristics, and consumer purchase history. Refining the definition further is GAPP's inclusion of *personal information that is considered sensitive*, such as medical, health or financial information, race or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions, sexual preferences, and criminal offenses.

GAPP is also based on key concepts from such laws as the Organization for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and the European Union's Directive on Data Privacy (Directive 95/46/EC). (For a discussion of these, see "An International Perspective on Protecting Personal Information" by Cheri Buckles in the March/April 2014 issue of *Information Management*.)

GAPP lists 10 privacy principles. (See Sidebar: Generally Accepted Privacy Principles). For each of these, there are objective and measurable criteria to guide development and evaluation of an organization's pri-

vacy policies, communications, procedures, and controls. The practitioner's version of GAPP includes a chart showing each principle, the criteria involved in its development, illustrative controls and procedures, and additional considerations. In short, it outlines how to design a privacy program element so it measures up to the standard.

For example, Principle 1: Management notes that the entity must communicate its privacy policies and procedures. The practitioner's chart elaborates on how to do this in an acceptable manner. It specifies that privacy policies must be communicated at least annually to those internally responsible for collecting, using, retaining, or disclosing personal information, that changes in policy should be communicated shortly after approval, and that internal personnel must confirm initially and periodically their understanding of the policies and their agreement to comply with them.

The criteria are specific with good reason. The need to audit privacy practices is not lost on the accounting profession, traditionally the source of business auditors. How well a large organization is addressing its privacy risk is something about which most executives and board members will likely seek an objective opinion. In addition, organizations that provide outsourced services requiring personal information – such as payroll or retirement benefits – may want to have an audit professional attest to their privacy risk management practices.

Those who want to measure their own progress in privacy can also use the Privacy Maturity Model (PMM), a tool very like the IGMM; the PMM provides varying degrees of maturity for each of the GAPP principles. Access it at: *http://www.cil.cnrs.fr/CIL/IMG/pdf/10-229_aicpa_cica_privacy_maturity_model_finalebook_revised.pdf.*

The Generally Accepted Privacy Principles

Privacy Principle	The entity:
Management	Defines, documents, communicates, and assigns accountability for its privacy policies and procedures
Notice	Provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed
Choice and Consent	Describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information
Collection	Collects personal information only for the purposes identified in the notice
Use, Retention and Disposal	Limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. Retains personal information only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information
Access	Provides individual with access to their personal information for review and update
Disclosure to Third Parties	Discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual
Security for Privacy	Protects personal information against unauthorized access (both physical and logical)
Quality	Maintains accurate, complete and relevant personal information for the purposes identified in the notice
Monitoring and Enforcement	Monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes

Source: The American Institute of Certified Public Accountants (*www.aicpa.org*) and the Canadian Institute of Chartered Accountants (*www.cica.ca*)

The Principles and GAPP

Given the groundswell of support for legislation regarding privacy, IG professionals would do well to understand the relationship of the Principles and GAPP, even though privacy may not be part of their current mandate. Jason Stearns, IGP, CRM, director of information governance compliance at global investment management company BlackRock, noted how the Principles and GAPP are compatible in his presentation, "Records Management and Privacy

Concerns – A Marriage of Principles." Stearns has seen the difficulties that arise in trying to retrofit privacy requirements onto information management systems; he offers three examples.

The desire to … make the most of an existing resource may have to be tempered with the need to meet international data privacy … restrictions

Case Study: The Shared Database

A particular line of business in financial services designed a database in the Americas to track customer order history and account performance. The database was quite successful, and eventually other lines of business started to use it, several of which were outside the United States. Over time, retention requirements began to conflict:

- U.S. data had a six-year retention requirement, but data originating in another country had a 10-year requirement.
- France required that data about its citizens be disposed of once the relationship with the company ended.
- Co-mingling was permitted when the database was designed, but it was not permitted later.

Accommodating all the requirements became impossible. Client information was commingled in one set of database tables but not another, precluding the possibility of simply sorting the database by country. Stearns said that after examining the additional risk of long retention, the company chose to keep all the data for the longest required retention period, i.e., 10 years.

He also noted that this particular example became a cautionary tale of how not to do things. The desire to streamline and make the most of an existing resource may have to be tempered with the need to meet international data privacy retention restrictions going forward.

Case Study: Mining the Data

In another, related example, Stearns related that users of the same database in the United States wanted to send it to a third-party service to do data mining. The business unit had gone so far as to extract data and package it for transmission to the data mining company, being unaware that some countries have restrictions on data being moved. The cause of this potential misstep was lack of education and training about privacy law for those who collect and use data.

Luckily, the company had developed an electronic tool that steps users through the transfer process by asking questions about the type of data, where it originated, and where it is to be sent. Because answering these and other questions reveals whether there are restrictions based on state, national, and international laws, the violation was avoided.

The tool is just a first step, though. Even if no restrictions are found, specific permissions and approvals are still necessary to move the data. The usefulness of the online tool is that it can be updated easily and refined to include new regulations as they come into existence. While this does not fix the problem of what is stored in the database, it does help prevent violating trans-border data requirements.

Case Study: Boxes in the Bahamas

Many countries, notably Germany, the Bahamas, and Mexico, have restrictions on who can look at private data held in that country and on whether the data can leave the country. Stearns told of a case where the company had boxes of records stored in the Bahamas. Box descriptions were held in company-designed software running on a PC located in that country. When the decision was made to discontinue some operations there, Stearns discovered that although the company had the ability to view the box description data from a U.S. location, it was specifically prohibited from doing so by Bahamian law because of its possible privacy implications.

The irony is that boxes eligible for destruction could have been identified easily by just the records category, but again, this could not be done from a remote location. The only solution was to send a company employee to the Bahamas to complete the task.

Stearns noted that for many older systems, it is not even possible to eradicate stored data or to partition it according to country of origin. He strongly advises to invest in Privacy by Design when building a new system or doing a significant upgrade. [Editor's note: See this issue's cover story by Norman Mooradian, Ph.D., "Closing the Gap Between Policy and ECM Implementation Using Privacy by Design.]

"Having tools like the Principles for information governance and GAPP for privacy is an advantage," Stearns said. "They are based on international standards and the issues they address are important to preserving business advantage whether at home or abroad."

Not Once and Done

As with so many aspects of information management, protection is not "once and done" where privacy protection is concerned. Continuous improvement with the help of the IGMM and outside audits will be factors in assessing risks and making intelligent policy decisions going forward. **END**

Julie Gable, CRM, CDIA+, FAI can be contacted at juliegable@verizon.net. *See her bio on page 47.*