An International Perspective on Protecting Personal Information

Records and information management professionals have a key role to play in safeguarding the privacy of personal information. The challenge is keeping up with rapidly changing, intrusive technologies and in step with the legislation that often lags behind them.

Cherri-Ann Beckles

The need for privacy as a public policy arose and augmented in the second half of the 20th century with the emergence and use of information and communications technologies (ICTs) to collect, store, and share *personal data*, which is defined by the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* as "any information relating to an identified or identifiable individual (data subject)."

With profound changes in the advancement and utilization of technology and a shift from manufacturing to providing knowledge-based services, ICTs became central in both the public and private sector, facilitating the widespread distribution of information – including personal data – that could be stored, manipulated, and exchanged more easily than ever before. The expansion of state powers and the institutionalization of information over the last 50 years through more complex technology-based recordkeeping systems gave rise to the need to control access to and the use of personal data.

Records and information management (RIM) practitioners, who are likely to deal with vast amounts of personal data captured in records, have a key role in ensuring compliance with privacy and data protection legislation and policies relevant to recordkeeping within their jurisdictions. They must be proactive in managing information privacy in all recordkeeping systems by becoming conversant with relevant legislation and designing RIM program policies and procedures that ensure that their organizations' records are secured against the unwarranted disclosure and abuse of their internal and external customers' personal data.

Defining Privacy

There is no universal consensus on the meaning of privacy, which encompasses diverse concerns, including the right to be left alone; the right to be free from government surveillance,

intrusive police, or other searches, wiretapping, or persistent journalists; and the right to be allowed to make private personal decisions.

The definition of privacy changes according to space (location) and time. Universally, notions of anonymity and security are often associated with privacy. However, the definition that is most relevant to RIM is that privacy is the right for a "living and identifiable" individual to have some control over the collection, storage, and disclosure of his or her personal information held by governmental agencies, financial institutions, medical facilities, educational institutions, and other public and private entities.

In many jurisdictions, privacy is considered a fundamental human right. Yet, it is evident that privacy is not an absolute right and may be denied for what may be considered a greater purpose. For example, with the increase in terrorism on a global scale, the call for improved national security in some jurisdictions has led to what some consider a sacrificing of privacy. However, it is in the interest of governmental agencies to collect personal information about citizens' earnings and income for tax collection purposes and to collect census data so they can make strategic decisions and improve services for the citizenry.

Although there is this need to collect and use personal data, the "right to privacy" as outlined by the Universal Declaration of Human Rights of 1948 is generally accepted and respected across the globe, and RIM practitioners are key players – in many instances on the frontline – in protecting that right.

Relationship to RIM

When exploring the relationship between informational privacy and RIM, it is clear that the rapidly changing technological environment has had a profound impact on both pursuits. This resulted in privacy becoming a public issue and RIM developing as an organizational response to deal with these changes.

Recordkeeping systems had evolved over time, moving from manual, paper-based systems to highly networked, automated systems. By the 1970s, the proliferation of minicomputers and the computerization of organizations, including the introduction of word processing and data processing machines, meant that vast amounts of information, including personal data, was being created, received, manipulated, distributed, and stored electronically.

In spite of this automation, the widespread use of carbon paper and the photocopier resulted in sustained and exponential growth in creating and distributing paper records. By the late 1980s, organizations were working in hybrid recordkeeping environments, with electronic records adding a new dimension to the need to control records.

Another significant development in recordkeeping took place in the 1990s with the advent of the World Wide Web and the Internet, resulting in the ease of moving information seamlessly across local and wide area networks. Personal data became even more vulnerable to unwarranted distribution and possible abuse by unauthorized people.

Another major development was on the horizon in the new millennium. It took the form of the widespread use of e-mail, instant messaging, and social media, including Facebook, Twitter and LinkedIn, via portable digital assistants, smart phones, and tablets. More recently, cloud computing has led to the remote hosting of organizational data, usually by independent service providers.

These new modes for creating, capturing, and storing data have had unimagined and serious implications for managing records' privacy, as evidenced by the increasing occurrences of privacy-related lawsuits against high-profile governmental and private entities around the globe for failing to comply with privacy legislation.

RIM practitioners, according to legislation in some jurisdictions, are considered "data processors" working on behalf of "data controllers" (employers). Therefore, RIM practitioners should not ignore their role as privacy advocates and the promoters of more stringent regulation of recordkeeping privacy.

Key Privacy Principles

One of the greatest challenges of managing information privacy on a global scale has been disparity among countries' national legislation and enforcement. This led to concerns about the risks incurred by allowing the free flow of information across borders.

As part of the first global initiative to safeguard personal data, the Organisation for Economic Co-operation and Development (OECD) sought in 1980 to harmonize its member states' national privacy legislation by setting out seven baseline principles for the legal drafting process.

The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OCED *Guidelines*) generally seek to address data quality, specification of the purpose and limitations on collecting personal data, required security safeguards, openness, individual participation, and accountability. The principles embodied in the OECD *Guidelines* state that personal information must be:

1. Collected fairly and lawfully
2. Used only for the purpose specified during collection
3. Adequate, relevant, and not excessive to that purpose
4. Accurate and up-to-date
5. Accessible
6. Kept secure
7. Subject to disposal after the purpose is completed

The OECD's principles are not binding, and in some jurisdictions, they have not been implemented in law. However, they have been the basis on which many information privacy laws have since been written, and they can serve as a guide to RIM practitioners regardless of their location.

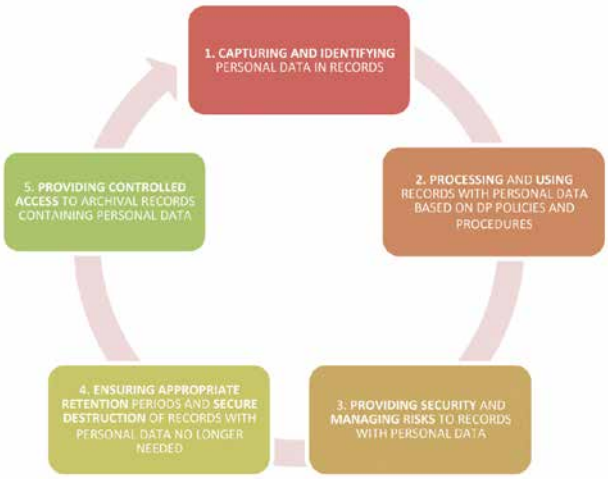

Figure 1: Lifecycle Management of Privacy for Recordkeeping

Key RIM Considerations

Records containing personal data form a significant part of any organization's informational assets and are usually found within the manual and automated systems managed either directly or indirectly by RIM practitioners. Their main activities in regulating privacy/data protection may be summed up in the following three points:

1. Ensuring that data protection responsibilities are clearly identified and assigned
2. Providing RIM services with clearly written policies and procedures that define how personal data is to be processed
3. Ensuring that when obtaining personal information, their methods of collection, storage, destruction and provision of access complies with data protection legislation
4. Following are some specific steps RIM practitioners can take. (See also Figure 1: Lifecycle Management of Privacy for Recordkeeping.")

Identify Sensitive Data

RIM practitioners must be aware of which records contain *sensitive personal data*, which the UK Data Protection Act of 1998 defines as "personal data consisting of information about the racial or ethnic origin of the 'data subject,' his political opinion, his religious beliefs or beliefs of a similar nature, whether he is a member of a trade union, his physical or mental health or condition, his sexual health and the commission or alleged commission of criminal offences."

This type of recorded information is predominately found in records in organizations' human resources,

Key National Privacy Legislation

Privacy acts generally govern how personal information is collected, used, stored, and disclosed. Following are some of the most-often encountered ones for select countries.

Australia: **The Privacy Act 1988:** *www.oaic.gov.au/privacy/privacy-act/the-privacy-act.*

Canada: **Personal Information Protection and Electronic Documents Act:** *http://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html.*

China: **Consumer Rights Protection Law:** at *www.wipo.int/edocs/lexdocs/laws/en/cn/cn174en.pdf.*

European Union member countries: **EU Directive 95/46/EC:** *http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf;* **Safe Harbor Data Privacy Framework:** *http://export.gov/safeharbor/*

New Zealand: **Privacy Act 1993:** *www.legislation.govt.nz/act/public/1993/0028/latest/DLM296639.html.*

United States: **Electronic Communications Privacy Act – Title II Stored Electronic Communications Privacy Act:** *www.law.cornell.edu/uscode/text/18/part-I/chapter-121*; **Fair and Accurate Credit Transactions Act:** *www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf;* **Family Educational Rights & Privacy Act:** *www.ed.gov/policy/gen/guid/fpco/ferpa/index.html;* **Health Insurance Portability & Accountability Act:** *www.hhs.gov/ocr/privacy/index.html; www.hhs.gov/ocr/privacy/index.html;* **USA Patriot Act:** *www.justice.gov/archive/ll/highlights.htm*

(See also the article in this issue "Protecting Information Privacy Per U.S. Federal Law" by Virginia Jones.)

finance, and administration sections. Some organizations, such as educational, medical, or judicial institutions, have a higher concentration of records containing personal data because of the nature of their business. Records management programs in these types of institutions need to put additional measures in place to ensure the security of any sensitive personal data.

Leverage Classification Schemes

RIM practitioners, particularly those working in highly centralized systems, seek to develop omnibus classification schemes to arrange records into categories that facilitate quick retrieval and comprehensive control. Classification schemes that group record series containing personal data in logical, functional categories, could be used as the foundation on which sound data protection strategies are built.

Know Legal Requirements

Additionally, RIM practitioners need to re-examine and rethink their formulation of records retention and disposition schedules, bearing in mind the requirements of privacy principles and/or legislation that relate to the retention of personal data. Careful attention must be paid to the provision of access to records containing personal data to ensure that this information is safeguarded from unauthorized use. Measures such as redaction and/or pseudonymization as well as encryption to anonymize personal data in records should be employed wherever necessary when dealing with requests to reproduce records. (See sidebar "Key National Privacy Legislation.")

Enhance Security

RIM practitioners should also seek to ensure the physical and intellectual security of the records within their care. Physical records should be protected in their storage areas, especially in instances where they are transferred for deposit in records centers and archival repositories, relocated to a new site, or sent for destruction.

Comply with Codes of Ethics

Some jurisdictions have either written or considered formulating a code of practice to guide RIM practitioners in managing privacy in their RIM programs. Notably, guarding personal data is not only a legal issue for RIM practitioners but an ethical one; therefore, it should not be overlooked or ignored. The *Code of Professional Responsibility for Records Management* as developed by ARMA International states that "records and information managers [should] affirm that the collection, maintenance, distribution and use of information about individuals is a privilege in trust: the right to privacy of all individuals must be both promoted and upheld."

The International Council on Archives in its *Code of Ethics for Archivists* states that "archivists should respect both access and privacy, and act within the boundaries of relevant legislation." Hence, the responsibility of the RIM practitioner to understand privacy legislation and adopt measures to protect personal data held within public and private organizations is unquestionable.

Develop a Good Communications Strategy

A good communications strategy is critical for sound data protection

management in RIM programs across all organizations, especially large and dispersed ones. Many breaches have occurred across jurisdictions as a result of human error or malicious intent by staff members. Training and orientation of staff in matters relating to privacy/data protection in RIM programs is absolutely crucial to maintaining a well-ordered, well-functioning, enterprise-wide program while reducing the risk of breaches. RIM practitioners should work with human resource experts to incorporate training and awareness about data protection legislation, policies, and procedures in the training programs for staff at every level of the organization.

Step up to the Challenge

Because RIM practitioners are at the heart of the organization as it relates to how its informational assets are managed, safeguarding records and information should be at the center of their work. They must recognize and accept that their role is weightier than ever before, as privacy/data protection legislation will continue to lag behind fast-developing, intrusive technology. Establishing forward-thinking, adept RIM programs inclusive of well-planned data protections policies, procedures, and measures should enable their organizations to stay ahead of the ever-changing compliance landscape. **END**

Cherri-Ann Beckles can be contacted at cherri-ann.beckles@cavehill.uwi.edu. *Her bio is on page 47.*