

# PRIVACY MANAGEMENT:

## What Management Should Know

By Marc Vael

An international article brought to you from Belgium

### Introduction

In today's information age, privacy has become a significant asset, becoming more valuable as it becomes more scarce. As a result, the protection of privacy is becoming an important competitive differentiator for organizations worldwide, in industries from financial services to healthcare, to consumer and technology markets, to government, a variety of which have already installed chief privacy officers (CPOs) to lead their privacy efforts.

Faced with customer demands for privacy protection, as well as rapidly evolving regulatory efforts around the world, organizations are increasingly viewing privacy protection as a way to enhance trust as well as avoid costs, mitigate risks, improve customer satisfaction and, potentially, generate new revenues. The ability to assure customers of the privacy of their own information is fundamental to engendering their trust, which is fundamental to the building of any brand. Thus, organizations that approach privacy as a strategic issue, and their customers and their information as strategic assets, are aware of the idea that privacy can be good for business and information-sharing can be good for customers.

### Understanding Privacy And Its Difference From (Information) Security

Privacy can be defined as the protection of the collection, storage, processing, dissemination and destruction of personal and sensitive information.

Personal information can be defined as any information relating to an identified or identifiable individual. Such information includes, but is not limited to, the customer's name, address, telephone number, personal identity/social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records and similar information.

Sensitive information can be defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions,

religious or philosophical beliefs, trade-union membership, sexual preferences or information related to offenses or criminal convictions.

Privacy is not the same as (information) security, although the two are often confused. In fact, privacy and (information) security both address access and control over information about people and organizations in all forms of media, many of which are not electronically based, such as paper files. Information security focuses on ensuring that the correct information is protected against loss, misuse, unauthorized access, disclosure, alteration and destruction, as intended by the author. An information systems security environment enables information and transactions to stay private. But, having excellent information security does not mean that an organization has dealt with all the issues related to privacy. An organization can have information security without privacy, but privacy is impossible without information security.

### Understanding The Extent Of The Privacy Issue And Its Risks

At the heart of the problem is the gigantic amount of information about customers, vendors, alliance partners, employees and citizens at large that organizations and governments possess today in millions of databases. And the rise of the Internet has made personal information easier to obtain and much harder to delete. Organizations and individuals want to control who does and does not have access to their medical, financial, purchasing and other personal information. And, if access is needed, organizations and individuals would like to be able to specify for what purposes and to what extent access will be granted. They also want specific assurances that the information considered to be private is effectively kept private. Customers are particularly concerned about the privacy of online transactions, especially about whether they can trust organizations to safeguard their credit card data and other key information. Although trust is not the only reason people buy from an organization, without it, they will go elsewhere.

Privacy breaches can emerge and have emerged wherever information flows. Organizations encountering privacy breaches face a variety of substantial business risks such as:

- ▲ Litigation and enforcement actions
- ▲ Fines
- ▲ Disruption of business operations
- ▲ Data transfer injunctions
- ▲ In-depth investigations and audits by data protection authorities
- ▲ Negative publicity leading to reputation and brand damage
- ▲ Civil liability prosecution
- ▲ Criminal prosecution

Unfortunately, many organizations today still tend to underestimate the importance of privacy. Many organizations are also not aware of the rapidly evolving legislations and regulations on a global and domestic level. Until something happens to put them at risk, many organizations today still do not know how much or what kind of information they have, who exactly has (had) access to it, to what extent its use may be regulated or what penalties they may face for its mishandling. Moreover, many organizations believe that adherence to information security practices will automatically take care of their privacy protection. This behavior can have serious consequences. Therefore, Board of Directors, executive management (including CEO, CIO and CSO) and audit committees need to be aware that these privacy risks still exist today and must examine the existing information management practices in their own organization to identify the privacy risks and define proper mitigation strategies.

Managing privacy risks in a business environment, converting them into competitive advantage, requires an organization-wide approach encompassing an array of critical business, technological, legal and ethical considerations, such as:

- ▲ Customer expectations and demands;
- ▲ External regulatory and legal environment;
- ▲ Internal compliance and related testing and monitoring;
- ▲ Information technology systems (management and security);
- ▲ Internal business processes and change management;
- ▲ Third-party relationships, including vendors and alliance partners;
- ▲ Objective attestation that privacy policies are in place and effective.

A typical example is the "opt in" or "opt out" mechanism. U.S. and E.U. laws require mechanisms that enable individuals to stop the use of their information. How much individuals control the content of transactions, and how much organizations themselves do, has become the key question for all organizations. The debate is whether customers should be given the option to "opt in" or "opt out" of having their information shared with or sold to third parties (online, they opt in or out simply by choosing whether to buy and otherwise share information). Most of the online industry would prefer to tell Web site visitors that "personal information might be retained for internal purposes or even distributed to third parties" unless they exercise their right to "opt out" and thus prevent the information from being used for marketing purposes or by third parties. On the other hand, most customer groups want Web sites to request that customers always explicitly "opt in" before they are allowed to retain or distribute information on a visitor.

## Privacy Legislation

Many privacy legislations do exist today in the world. We will not elaborate on them in this article (on the Internet alone there are more than 300.000 dedicated websites on the subject). However, below are some highlights of privacy legislations with an impact.

Established in 1995, the European Community's Directive on Data Protection (**ECDDP**) created a framework for use of personal data while ensuring the protection of the fundamental rights of the individual to privacy. The directive (Directive 95/46/EC) establishes uniform European Union national privacy laws governing personally identifiable information, including both employee and customer information. The Directive sets out the data protection principles that, with few exceptions, prohibit transfer of personal data to a country outside of the European Economic Area unless that country ensures an adequate level of protection of that data. In July 2002, an updated version was approved on the processing of personal data and the protection of privacy in the electronic communications sector (Directive 2002/58/EC). Anno 2005 it is still the leading Directive for all E.U., but also many non-E.U. countries.

The Safe Harbor Accord for the European Commission's Directive on Data Protection is designed to bridge different privacy approaches between the European Union and the United States and provide a streamlined means for U.S. organizations to comply with the 1995 European Union Directive. By prohibiting the transfer of personal data to nations that do not meet European standards for privacy protection, the E.U. Directive imposed specific privacy related elements around the flow of information between E.U. and non-E.U. organizations. An organization that wants to do business with E.U. countries must establish and demonstrate compliance with privacy policies in keeping with the Safe Harbor basic privacy principles:

- ▲ **Notice:** The organization must provide individuals with clear notice of "the purposes for which it collects and uses information about them, the types of third parties to which it discloses the information and how to contact the organization with inquiries or complaints."
- ▲ **Choice:** Before any data is collected, the organization must give its customers the opportunity to "opt out" of any disclosure of their information to third parties or of a use of that information that is incompatible with the purpose for which it was originally collected. Also before any data is collected, the organization must allow its customers to choose whether to "opt in" to the sharing of their sensitive information (e.g., data related to such factors as health, race or religion).
- ▲ **Onward Transfer:** Unless it has the individual's permission to do otherwise, the organization may share information only with those third parties that belong to the Safe Harbor or follow its principles.
- ▲ **Security and Data Integrity:** The organization needs to ensure that the data they maintain is accurate, complete, current and thus reliable for use. It must also ensure the security of the information by protecting it against loss, misuse, unauthorized access, disclosure, alteration and destruction.
- ▲ **Access:** Unless it would be unduly burdened or violate the rights of others, the organization must give individuals "access to personal data about them and provide an opportunity to correct, amend, or delete such data."
- ▲ **Enforcement:** The organization must "enforce compliance, provide recourse for individuals who believe their privacy rights have been violated and impose sanctions on their employees and agents for non-compliance."

In 2005, this Safe Harbor Accord still creates a lot of commotion in organizations working with E.U. organizations.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is driven by the need to enable a mobile society to contain US medical costs, insure more US citizens, and enhance the quality of US healthcare. The

standards protect individually identifiable medical information, including demographic information, payment records and other identifiable data. Protections apply to oral, written, audio-visual and electronic information. Even though this Act applies solely to US-based hospitals, medical centers, health plans, clearinghouses and pharmacies, many non-US-based organizations are using this Act as inspiration for their internal privacy protection policies.

The effects of these complex privacy laws extend well beyond industry lines. A large manufacturer must comply with financial privacy laws when, for example, it issues credit cards in addition to selling heavy equipment. A large retailer is affected by medical privacy regulations because it has pharmacies in its stores. Another company that issues a private-label credit card is affected both by financial and health care laws if customers use the card in pharmacies. In addition, countries also face complex, conflicting regulations and customs, some provisions of which affect multinational organizations.

## Privacy Legislation And Its Impact In Belgium

National legislation still has a huge impact on the privacy and data protection within organizations. In Belgium for example, a specific data protection law exists already since December 1992 with a focus on the management of processing personal information and the audit thereof. It states that all organizations must take the appropriate technical and organizational security measures to protect personal data against accidental or unauthorized destruction, accidental loss, as well as against alteration of, access to and any other unauthorized processing of personal data. In other words, all organizations must prevent unlawful processing of personal data. The Belgian law implies the following principles for the collection, use and disclosure of personal information, combined with controls of individuals over how their personal information is handled:

- ▲ Accountability
- ▲ Identifying purposes
- ▲ Consent
- ▲ Limiting collection
- ▲ Limiting use, disclosure and retention
- ▲ Accuracy (data quality)
- ▲ Safeguards and security obligations
- ▲ Openness
- ▲ Limiting access
- ▲ Challenging compliance
- ▲ Notification of legal provision
- ▲ Supervision of compliance

Still some elements remain open for discussion in the Belgian legal environment, such as specific information security requirements (unlike in some other E.U. countries, e.g. Italy requires anti-virus and firewall devices), sanctions in case of non-compliance and the security obligations for electronic communications service providers and providers of software for electronic communications (such as e-mail, blogs, instant messaging, etc.).

Furthermore, aside the (Belgian) data protection law, various other legislation exists, such as the professional secrecy obligations (e.g. for lawyers, doctors, accountants) and intellectual property legislation (e.g. no patent protection is possible if information related to invention was previously disclosed to the public), which makes it not easier to determine a uniform approach. As an example, a special Collective Worker Agreement (CWA number 81) was created in Belgium in April 2002 dealing with the privacy protec-

tion in the workplace of electronic online communications from employees. Such rules are deemed necessary and required since monitoring techniques nowadays are highly efficient and easy to apply by organizations. In summary, monitoring is allowed in Belgian organizations in the following circumstances:

- ▲ The prevention of unlawful acts, libel and acts contrary to decency;
- ▲ The protection of economic, commercial and financial confidential interests of the organization;
- ▲ The maintenance of the technical performance of the computer system;
- ▲ The control of the respect of the terms of use of the computer system.

In this Belgian CWA, particular attention is given to the following basic concepts for monitoring whilst protecting the privacy of the employees:

- ▲ Finality: this implies compliance with a limited list of objectives, for which the controls on communication data are allowed
- ▲ Proportionality: this implies reducing the infringement of the privacy of the employee to a strict minimum (if unavoidable) and not allowing systematic individualization
- ▲ Transparency: this implies an openness around the monitoring policy (rights and obligations, limitations, sanctions, etc.), procedures, people and tools (conditions of use and limitations) involved towards all employees collectively via proper organizational channels (such as workers council, committee for prevention and protection, unions and intranets accessible to all employees) as well as towards every employee individually via employee and user policy, contractual agreement and general instructions

In essence, secret monitoring by an organization on its employees is never allowed and employees still have rights but also obligations whilst performing activities within an organization in Belgium. However, all this legislation has created and is still the basis for a lot of commotion, discussion and adversarial approaches, especially between management, unions, and employees. The technical implementation of these rules are not evident in this context.

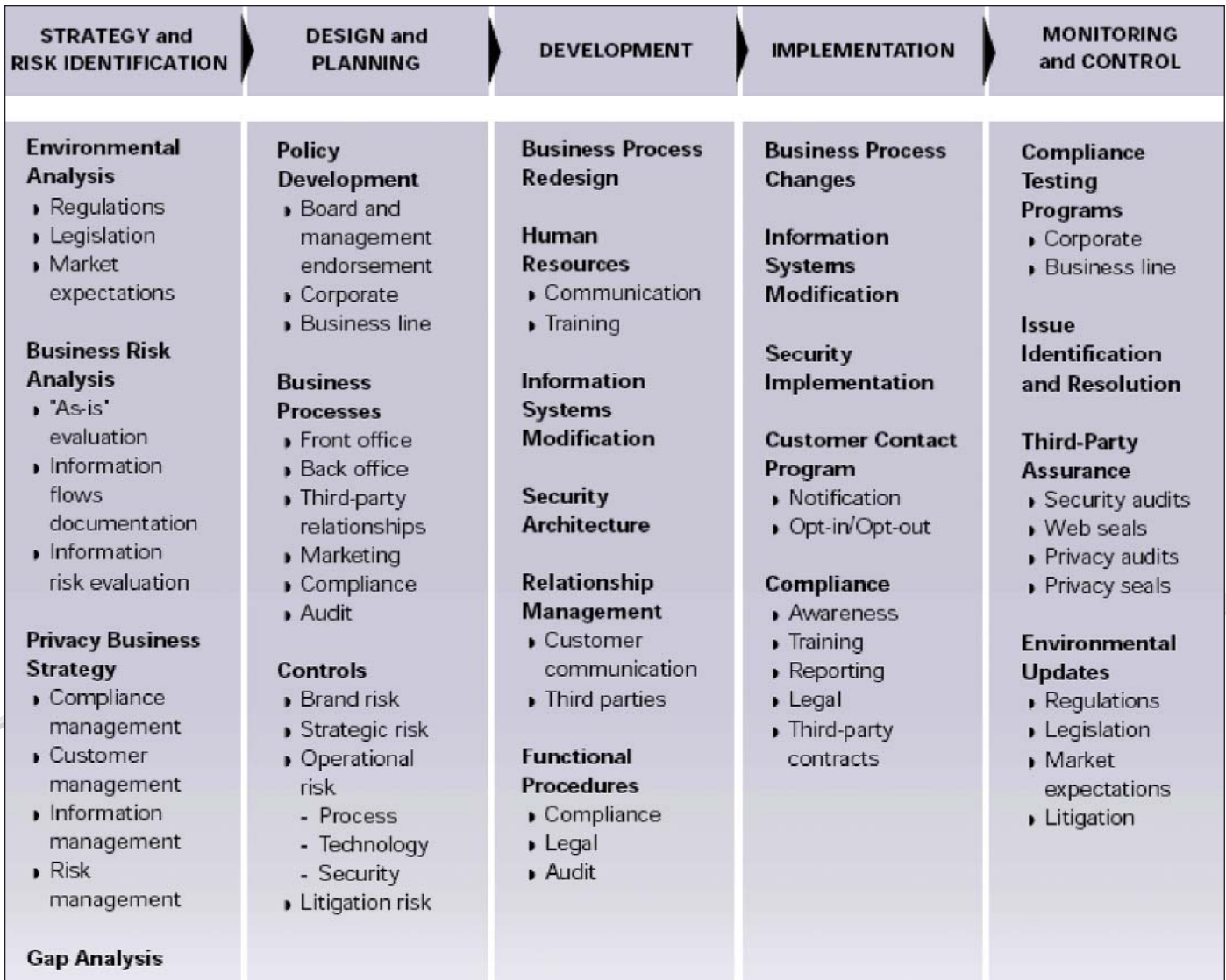
In practice, as one can imagine, this makes it not easy for any multinational organization to come with one "global privacy policy."

## A Privacy Risk Management Approach

An effective approach to privacy risk management begins with recognizing that it is not solely a technology-based issue. Rather, it is a strategic issue that encompasses the protection of a variety of assets, many of which are not electronically based. Although globalization and the Internet have increased the quantity of data and the speed and complexity of its flow, privacy issues affect paper records as well. Records of customer preferences are part of a covenant between a person and an organization, delineating how that entity will collect and use information about that person and how it will safeguard his or her privacy.

An effective privacy risk management program provides a mechanism for an organization to manage privacy risks in a manner consistent with its business needs, regulatory requirements, and marketplace expectations. Such a program:

- ▲ Discloses privacy principles;
- ▲ Addresses the collection, use and retention of customer information;



**Figure 1: Privacy management may be depicted as a “lifecycle” encompassing five phases**

- ▲ Ensures the security of the information maintained (confidentiality, integrity and availability);
- ▲ Identifies how customer privacy is maintained in business relationships with affiliated and non-affiliated third parties (such as vendors and alliance partners);
- ▲ Periodically tests for compliance with organization policies and regulatory compliance requirements;
- ▲ Monitors and evaluates the business implications of possible changes in laws and attitudes toward privacy.

The development of an organizational privacy policy is essential to increasing customer confidence and sustaining long-term relationships. A privacy policy creates a commitment with respect to the protection of personally identifiable information. This lets employees and customers know that the organization is dedicated to keeping personal information secure and using it only in accordance with individual privacy preferences and with relevant laws and regulations.

A good privacy policy contains at least the following components:

- ▲ Definitions
- ▲ Purpose of and access to databases

- ▲ Use of databases
- ▲ Penalties for misuse
- ▲ Security of Personal Data
- ▲ Access to Personal Data
- ▲ Modifications and Corrections of Personal Data
- ▲ Transfer of Personal Data
- ▲ Compliance with Policy
- ▲ Cooperation with Data Protection Authorities
- ▲ Additional Third-Party Rights of data subjects
- ▲ Dispute resolution process
- ▲ Complaints process
- ▲ Employment applicants
- ▲ Application of policy
- ▲ Compliance with national law
- ▲ Crisis management program (when incidents happen)

Each privacy policy statement must include:

- ▲ Responsible parties
- ▲ Required activities
- ▲ Permitted activities

- ▲ Prohibited activities
- ▲ Reporting requirements
- ▲ Known penalties for violation

Once a privacy management program and a privacy policy is put in place, the organization also needs to recognize that posting such a policy and then failing to live up to it may create a legal liability. Once developed and posted, a privacy policy must become part of the organizational culture.

Putting a privacy policy in place is a good step, but it is not the only step. An organization needs to identify where customer and other information is coming from, where it is circulated, where it goes and how it is used. Organizations need to know what they need; they need to avoid collecting information they do not need and they need to make sure vendors and other third parties follow the same rules. Moreover, organizations need to recognize and communicate that such efforts must be ongoing. To accomplish these goals, organizations must begin to manage privacy holistically, with an individual (chief privacy officer or CPO) or a team held accountable for the complete process. The appointment of a CPO represents a certain maturing approach to privacy. No one individual, however, can take sole responsibility for designing, developing and implementing the effort.

A privacy management program requires the collective expertise of a variety of departments and specialists, including professionals with knowledge, insight and experience with information risk management and business process analysis and redesign as well as with privacy regulations, legislation, litigation and the organization's own industry-specific needs. To varying degrees the team must also include business line managers, the IT manager, the security manager and members of the organization's legal, HR, marketing and internal audit department.

Such overall process of privacy management may be depicted as a "life-cycle" encompassing five phases.

## 1. Strategy and Risk Identification

Managing privacy as a business strategy helps an organization identify and mitigate its risks and leverage the substantial opportunities that such an effort may uncover. An organization needs to understand its environment fully, including the regulations and potential legislation that affect all of its markets as well as its customers' privacy needs. The analysis must encompass external customers and their customers as well as internal "customers," including vendors, employees and other stakeholders.

The organization then conducts a "business risk assessment" identifying and documenting all the data flows within the organization in all forms of media, electronic and otherwise. It needs to determine where the information originates, where it flows, how it is stored and how it is disseminated. This process usually uncovers the most obvious areas of exposure and begins to reveal more subtle risk and compliance issues. With this assessment of the "as is" state, the organization can develop a better informed, high-level privacy strategy, which encompasses its specific goals for management of compliance, customers, information and risk.

Setting a reliable strategy requires that the organization determine how it can better comply with relevant regulatory requirements and identify how best to manage information and its related risks. To meet these objectives, the organization can perform a gap analysis—comparing the "as is" state to the desired "to be" state set out in the privacy strategy, and then assess the risks and opportunities that arise. The gap analysis should attempt to achieve the following:

- ▲ Identify current privacy practices and the organization's adherence to privacy principles, industry practices and regulations.

- ▲ Identify missing or poorly executed privacy program elements that require remediation.
- ▲ Identify current versus desired practices and procedures over the collection, use, sharing and storage of personal information.
- ▲ Deliver specific recommendations, resources and timeline for completing the implementation of the desired privacy program.
- ▲ Conduct a post-implementation review after a reasonable time, following the implementation of specific recommendation.
- ▲ Deliver internal reports to executive management that detail current privacy practices.
- ▲ Conduct random reviews to determine ongoing compliance improvements.
- ▲ Generate periodic program health checks to assess program efficacy.

A gap analysis of the HR process, for example, would determine whether the organization's training program encompasses current privacy regulations and the organization's compliance policies.

## 2. Design and Planning

Once risks are identified and a strategy is set, the organization can focus on developing a proper privacy policy (and supporting procedures) that is both appropriate and workable for the organization supporting its strategy. Beyond the privacy policy, the organization must also create a plan that addresses privacy risk issues and communication of those issues at all levels of an organization, including front- and back-office operations, IT, marketing, audit, HR, security and third-party relationships. To do so, the organization must analyze the effects of the gaps identified in key processes and design the appropriate controls for the organization to mitigate associated risks. Controls are needed, for example, to ensure that access to certain information is limited to the people who have a defined need to know. The organization can use the privacy business strategy and the privacy policy to determine how current processes can be improved. An effective privacy policy reduces the risk of litigation and regulatory non-compliance, and at the same time builds trust and loyalty among customers and other stakeholders.

## 3. Development

During the development phase, the organization puts in place mechanisms for addressing the issues identified during design and planning. It establishes practices and controls to maximize compliance with the privacy policy, such as developing internal training programs in which employees learn about the importance of privacy and how to protect private information. Entities may also find that changes can or should be made to existing business processes and supporting systems. Some of these changes can generate tremendous additional value, for example, by integrating disparate customer databases residing in different divisions of the organization. During this phase, the organization should also review its technical architecture so that, for example, it can ensure that firewalls as well as authorization and encryption methodologies and mechanisms are in place to limit data access to only the employees who need it to perform a specific business function. By communicating these efforts internally and externally, the organization can remind and assure its stakeholders of its commitment to privacy protection. Such efforts can inspire new confidence in external stakeholders, who secure in the knowledge that their privacy is respected, may be more likely to choose the organization over its competitors.

## 4. Implementation

This phase entails implementing the changes in business processes, information systems and security measures that the entity has designed, planned and developed. Once the organization makes these changes, it may also want to initiate a "customer contact" program to raise stakeholder awareness and appreciation of how the organization is addressing privacy issues and of changes they should expect in how it operates. In addition, the organization must review its management reporting, legal and third-party contract practices to align them with its new privacy initiatives and guidelines.

## 5. Monitoring and Control

Monitoring and control of privacy-related processes and initiatives begin during the implementation phase and remain ongoing. Although these measurement efforts are particularly important for organizations in regulated industries, which undergo heavy scrutiny of privacy-related processes and procedures, monitoring and control are essential for any organization that invests in a privacy management program and expects to derive meaningful results from it. Issues arising during implementation are addressed and resolved during this phase. The organization must take into account how its privacy policy and processes are affected by changes in the business environment, including regulatory and legislative developments, market expectations and litigation.

To ensure that policy and processes are in place and working properly, the organization must consider conducting separate security and privacy audits. Internally, a privacy audit can provide a useful self-assessment of organizational compliance with laws and regulations. Externally, a privacy audit can help demonstrate commitment to privacy management as well as compliance with regulations and internal policies. It encompasses both on- and off-line privacy management, including business processes, implementation of policies and employee training. Data flows are examined to see if "gaps" in privacy have been effectively closed, and if new gaps have opened. When the organization communicates the results appropriately, a privacy audit can help build the covenant of trust with customers by providing a regular means of testing the enabling system and of verifying organizational compliance with its own privacy policies. The organization may also seek the additional benefit that derives from obtaining third-party assurance, such as a Web Seal, to demonstrate that it fulfills defined criteria in various areas of business, information security, information privacy practices and transaction integrity.

This five-phase approach helps organizations to manage privacy as a strategic issue subject to ongoing changes in technology and regulation.

The following essential components are required to implement a privacy framework within an organization today:

- ▲ Ensure board of directors/senior management commitment: an organizational privacy program must start at the top to ensure sufficient resources and continuity. View it as part of an overall risk management program.
- ▲ Appoint a dedicated chief privacy officer with sufficient resources, including employees and time: identify key persons in the various areas of the business to participate in the privacy framework.
- ▲ Understand why the organization currently collects, uses and/or distributes personal data: identify the organizational information needs and requirements to achieve its business ends. This could include, for example, sales, leasing, warranties and customer support.
- ▲ Review all information the organization currently possesses: is the current information consistent with the organization's actual needs? Does the organization have more personal information

than required? Have all customers consented to the collection of that information?


- ▲ Review all methods used by the organization to collect personal information: including review of the Web site, credit applications, contests, warranty registrations, contact databases, etc. Is the organization clear and up-front about why it is asking for the information?
- ▲ Review customers' consent to collect the information: Is the purpose for collection clearly articulated? Keep track of why the organization has collected the information and the consent to do so.
- ▲ Develop and enforce an organization-wide privacy policy: ensure employees and customers have access to the privacy policy.
- ▲ Educate and train all employees: including existing employees and new hires. Pay special attention to employees who interact with customers.
- ▲ Ensure all personal information is secure at all times.
- ▲ Ensure third parties and vendors comply with the organizational privacy policy: determine that they are able to provide at least the same level of protection that the organization requires.

## Conclusion

Privacy Management affords organizations the opportunity to build their perceived value with customers and other stakeholders by communicating their privacy policies in such a way as to create a covenant of trust. This covenant is a transparent, mutual understanding of who owns the information, who controls it and how information will be used. It can be a genuine competitive advantage, but it requires organizations to look beyond the demands and requirements of evolving regulations. Thus, while compliance with legislation and regulations may compel companies to review their privacy practices, if that is all they do, they will not be doing enough. In fact, they will likely be overlooking the full extent of the risks they could confront. They may be collecting and archiving much more information than they will ever use and spending more money than they should. Moreover, they may be neglecting an opportunity to use their privacy practices as a tool for building customer relationships and, ultimately, brand value in the global marketplace. A privacy management program helps organizations address these challenges and helps them create an important new covenant with stakeholders.

At the heart of privacy legislation, regulations and guidance is the challenge of balancing a customer's right to privacy with the organization's clear interest in using customer information to identify potential business opportunities, both inside and outside the organization. When organizations have their customers' trust, they benefit from those customers' increasing willingness to share increasingly specific information about their preferences as well as their satisfaction levels. Such information can enable organizations to understand, meet and eventually anticipate customer needs and desires more effectively. Thus, to design and implement an effective privacy management program, organizations must first invest in understanding what their customers want and expect. Organizations cannot determine how to treat customer information without knowing their customers' needs.

In the short term, most organizations must focus on compliance with relevant privacy laws and regulations. During those efforts they need to remember that long-term market differentiation will ultimately evolve from a concerted effort to brand the organization as privacy-conscious in keeping with identified customer expectations. Management need not to

view privacy laws as another regulatory burden. Rather, as custodians of increasing levels of customer information protection, they should take the opportunity to make privacy protection part of their strategic business plans. Organizations that make the commitment to the notion that ensuring privacy protection is good for business stand to benefit in the marketplace. Moreover, organizations must acknowledge that waiting to address the issue until after a privacy breach has occurred will almost certainly be an expensive approach with potentially serious consequences for the organization's reputation and bottom line. The organization that damages its reputation because of a privacy breach is likely to see decreased revenues and profits and be saddled with brand rebuilding to recapture its proper market share. That does not seem to be a risk worth taking. 

---

*Marc Vael is currently the National Information & Technology Security Officer and the Data Protection Officer at KPMG in Belgium.*

