



 **ERNST & YOUNG**

*Quality In Everything We Do*

# Privacy Landscape

2008



# The Privacy Landscape for 2008

Every organization that handles personal information – whether for consumers, customers, employees, or business partners – faces a number of obligations to the participating parties related to privacy and the protection of that information.

Since 2001, when Ernst & Young published our first annual update on privacy concerns and the top issues organizations would face in the year ahead, one thing became clear – many issues are persistent and don't neatly expire at the end of a year. Even more alarming is that these issues are becoming increasingly complex and more integral factors in a company's ability to do business well. While privacy in earlier years may have been considered more of a marketing hook, focused on meeting customer preferences, privacy today is associated with the potential for abuse – inappropriate access to or exposure of information resulting in identity theft and fraud. The prevalence of such issues has attached a keen sense of urgency to privacy, thereby moving it up the list of business concerns on a global scale.

## Persistence and Complexity: Two Critical Business Risks

### Privacy Persists as a Compliance and Business Risk

Beyond the ethical responsibility of privacy, compliance with laws and regulations has become a key driver for privacy management initiatives all over the world. National data protection laws are well established in Europe, Canada, and some Pacific Rim countries. Russia and Dubai enacted new laws in 2007, and legislation is being considered in other countries key to the global economy, including India, China, Korea, and Singapore. These laws are far-reaching and have had a significant impact on how personal information is processed.

In the United States, although there is no overarching privacy law, a complex arrangement of federal laws and even more complex state laws govern the use of personal information in different industries and contexts. For an organization that operates across state lines or national boundaries, complying with these laws and regulations can pose significant challenges and a range of business risks.

**Compliance Risk:** The risk related to not complying with relevant laws and regulations or even the contractual obligations over personal information is accelerating with the increase in regulator inquiries, audits, and other enforcement actions. The penalties for noncompliance, even the settlements without admission of wrongdoing, routinely cost companies millions of dollars. With media continuing to shine the spotlight on privacy, any violations or other incidents that emerge can mean damage to the enterprise brand and reputation. Such attention is even more likely with the increasing requirements for breach notification, whereby an organization must inform individuals if their personal information is lost, even if the actual risk of harm is perceived to be low.

### Convergence in Compliance

As the business risks related to privacy become increasingly important, the process of managing compliance with privacy and data protection standards is becoming more integrated with such existing compliance initiatives as records management, intellectual property protection, data governance, and information security (e.g., compliance with the Payment Card Industry's requirements), all of which share common goals and compliance methods. This trend is clearly evident in Ernst & Young's 2007 Global Information Security Survey. Survey respondents cited the combination of privacy and data protection third on their list of top issues that have the most significant impact on information security practices, following only the related drivers of complying with regulations (namely the internal controls requirements of the Sarbanes-Oxley Act and similar laws) and meeting business objectives.

Some companies are bundling privacy compliance duties with another set of corporate compliance functions, such as those for ethics, code of conduct management, and sales and marketing. In these cases, common policies, processes, and tools are needed to make the convergence of these compliance functions effective.

Organizations are increasingly aware of the need to address privacy as part of their overall IT risk management and compliance effort and not as a stand-alone issue. That includes the formal governance and life cycle management of IT processes and their role in meeting business goals and objectives. Processes and assurance related to enterprise IT must be managed effectively to comply with corporate and external mandates, and they must address risks to operations as well as to brand and reputation. Then, as an integrated business initiative, privacy becomes an enterprise-wide responsibility, shared by legal, compliance, and the business units.

## Top Ten Privacy Issues – Be Prepared

For an organization addressing privacy as a critical business risk, there are some key issues that need to be considered and questions that should be asked by management and the C-suite. Depending upon the responses, the organization can determine how vulnerable it may be to privacy breaches or issues of noncompliance and what actions it should take to meet these inevitable challenges.

### 1. Information is Power: Recognizing the Need to Identify and Classify Data

#### Identifying and Classifying Information

A well-developed privacy program begins with inventorying the personal information an enterprise holds, identifying the business processes that handle personal information, and classifying the information based on sensitivity and impact if the system is compromised, breached, or otherwise misused. Although keeping track of where and how information is governed requires ongoing maintenance, having accurate categories, classifications, and definitions of data protection controls can mean both short- and long-term benefits.

While many organizations have data classification policies in place, they may not be serving their purpose if policies and procedures are outdated (created prior to the emergence of the current privacy risks), overly broad (containing limited high-level categories with only general security requirements associated with them), or inaccurate in designating risk thresholds among specific data elements. As organizations take action around the management requirements of records, they can help further identify and classify information and can bring about important points for decision-making related to privacy, information security, records management, and intellectual property protection.

To determine whether your company is prepared, have you:

- Inventoried your personal information across all systems, databases, and repositories of data for manual processes?
- Recently reviewed and updated your data classification policy to ensure it addresses relevant privacy regulations and risks?

### 2. Less is More: Sanctioning the Use of Personal Information

#### Data Minimization

Limiting the collection, use, disclosure, and retention of information that requires protection not only helps limit privacy risks to the organization and maintain privacy regulations, it also provides an opportunity for businesses to demonstrate their commitment to data protection.

It is a trend for organizations to explore opportunities to eliminate, truncate, redact, or obfuscate personal information in three key ways, starting with reviewing their systems in the context of data transfer (as personal information is stored in portable media devices



or is communicated electronically such as in e-mail messages). Next, organizations should review how personal information is applied specifically to particular data elements that are relevant to the business (e.g., Social Security numbers, credit card numbers). Finally, in the context of disclosures to third parties, as organizations should require transparency around the purpose of the disclosure, whether the third party already has the information and whether the act of disclosure will expand the circle of potential exposure.

To ensure success of data minimization efforts, have you:

- Identified opportunities to limit the collection, use, disclosure, and retention of personal information through information minimization?
- Looked to limit personal information that is stored on portable media devices or sent via e-mail?
- Identified specific data elements that should be minimized across the organization and in communications with third parties?

### 3. The World in Your Palm: Personal Information That Travels via Portable Devices

#### Portable Media Devices

Personal information is routinely processed, transmitted, and stored in an increasing array of media and devices. Terabytes and petabytes of information about customers and employees are written to disk or tape, pushed to laptop computers, and transmitted through e-mail systems to handheld devices. Loss or theft of this equipment and media is the foremost trigger for security breach notification – one that may be avoided if leading safeguards would become more common practice.

One of the first places to start is with defining clear policies and procedures for chain of custody over portable media containing personal information. Technology solutions exist today to help minimize the exposure of personal information in portable media and devices. For example, not all employees who frequently travel and require access to personal information need fully functioning laptops. Laptop-style “thin clients” that have no memory are gaining attention where high-speed network connections are commonly found. Network-based backup is another available solution that can help limit the use of traditional tapes and disks, which have been at the center of so many vanishing acts leading to breach notifications in recent years.

Using portable storage devices also complicates the issue of data retention. Organizations need to balance the benefits associated with keeping personal information, including where it is stored and how available it is, against the risks associated with protection – or the lack thereof. The issue becomes even more complex when the personal information in question is not subjected to any regulatory retention requirement or a clear definition of how long it can or should be kept. Organizations should seek out and minimize extraneous personal information from portable media. Indeed, the leading practices of the future will likely include limiting the use of such devices altogether.

When it comes to portable media devices, have you:

- Established policies or guidelines over the use of personal information with portable computing and media?
- Considered network-based backup solutions to reduce the amount of personal information being transferred with portable media?
- Reviewed your retention policies for the consideration of portable media devices and provided guidance to employees on how to stay on top of retention limits?

## 4. To Decode or Not Decode: The Evolving Use of Encryption

### Maturing the Use of Encryption

Personal information is vulnerable to theft or other loss whether it is “at rest” in a computer, on a tape, or on a USB memory device, or “in motion” as it is communicated in an e-mail message. Personal information protection has been gradually extending to cover data wherever it is and wherever it is going. The practice of encrypting portable devices, portable media, and computer communications (including e-mail messages and their attachments) is becoming commonplace among organizations. While this may have been a cutting-edge idea or a leading practice just a year or two ago, in 2008, the encryption of data at rest and in transit should be standard operating procedure.

Organizations that have yet to do so should pilot and implement laptop, e-mail, and portable media encryption solutions for the devices and exchanges that involve personal information. Common tools for the encryption of e-mail attachments should be provided to the business units that routinely handle personal information and should be made mandatory when personal information is transferred to third parties over otherwise unprotected methods.

For many organizations, the use of encryption is not new. In fact, it has been part of the protection of specific systems and processes that have given rise to a wide patchwork of encryption tools, technologies, and solutions. Eclectic as they are, each adds to the increasing challenge of encryption key management and brings technical limitations in applying them across different systems and operations. For many such organizations, it is no longer the mere addition of encryption – the benefit of enhanced protection over personal information – that is the goal, it is more consistent and effective use of encryption technology.

For many organizations, encryption will come to mean maturing and streamlining the use of existing procedures and solutions, identifying specific tools and applying them consistently, upgrading from folder-based to full-drive encryption of portable media for better coverage, and using encryption technology less reactively, on an issue-by-issue basis, but rather more holistically, with an eye on the organization’s broader compliance and risk management needs.

With an eye on encryption, have you:

- Identified encryption solutions for portable media and communications containing personal information?
- Identified opportunities to manage those solutions more effectively so encryption can be more commonly available and cost-effective?

## 5. The Three-Legged Stool: Enforcing Strict Standards With Vendors and Business Partners

### Managing Third Parties

Sharing personal information with vendors and business partners is commonplace and a necessity in today’s global market environment. Less common are effective programs that consistently apply and monitor how privacy is managed once personal information leaves the organization.

Leading companies have developed vendor risk management processes that account for privacy, including performing due diligence during the selection process, putting controls in place, both contractually and for the secure transfer of the information, and building a solid basis of confidence that the vendor can protect the personal information and govern its use.



However, even those leading organizations may still be struggling to define privacy and data protection requirements for business partners – whether, for example, joining forces in conducting clinical trials or conducting behavioral targeted marketing across the organization’s Web sites. Causing that struggle is likely the fact that the ability to dictate requirements does not exist in these alliances the way it might in a traditional client-vendor relationship. Business partners aside, many organizations have learned hard lessons on the path for vendor management – lessons that still impact their operations today.

Challenges arise as outdated language in evergreen contracts leave companies with fewer options for getting vendors to meet new requirements and carry their costs; vendors of significant size doing limited business with the client organization are less pressured to accept new requirements and use their legal resources to resist them; and small vendors with their limited resources struggle and are sometimes unable to meet expectations of advanced technical controls. Managing third parties effectively requires bringing not only procurement to the table with compliance executives but also legal, marketing, and any other business unit that interacts and shares personal information. Information security is an important part of this discussion in defining reasonable expectations that can be effectively met by third parties of different sizes.

When dealing with third parties, have you:

- Identified what personal information is exchanged with third parties and how it is secured and used by the third parties?
- Defined privacy and data protection requirements for third parties, along with a process that involves periodic and ongoing assurance around the controls that the third parties have put in place over the personal information?

## 6. On the Road Again: Personal Information and the Telecommuter’s Way-of-life

### Working Away

Whether from home, the road, or a coffee shop, more organizations support an increasing number of teleworkers. Though that may mean increased convenience, it also means increased exposure, bringing the enterprise into uncontrolled territory and using networks and computing devices that may not have been provided by or be protected by the organization. Extending security to this arrangement, protecting personal information processed in these often portable devices, and training people who work in these environments in the safe handling of personal information pose significant challenges.

When considering those who work remotely, have you:

- Equipped mobile and telework devices with security features, including virus protection, spyware protection, firewalls, and encryption solutions?
- Trained mobile and teleworkers on protection of personal information in these environments?

## 7. In Case of Emergency: Having a Plan for the Worst Case Scenario

### Incident Management

As a corollary to the broader security issues raised, the need for effective and timely management of privacy events and incidents remains a critical issue for all organizations. Potential compromises occur frequently, even in the best run organizations. Therefore, formal, effective, and repeatable processes to determine the nature of an event and the steps to take in response are essential. Maturity in incident management involves not only responding to events but also alerting the individuals who may be affected by the security breach.

In some cases, deadlines are mandated not only by the speed of business but also by regulation; failure to meet those deadlines becomes a violation of law. In other cases, inappropriate reactions to events may open the organization up to more damage than is warranted by a situation. Deliberate processes managed by cognizant executives are a must.

In assessing your organization's incident preparedness, have you:

- Established a process to manage events and incidents involving personal information?
- Tested the process and shown it to be effective?

## 8. It's a Small World: Developing Privacy Procedures for Home and Abroad

### Globalization and Harmonization

One of the by-products of today's business trends is that data, including personal information, is spread seamlessly across the globe. Accelerating business models and their globalization of businesses, markets, and workforces require a harmonization of systems and processes. That means organizations must tackle privacy risk management and compliance across jurisdictions to keep their businesses growing. Such privacy regulators as the Federal Trade Commission, state attorney general offices, national data protection authorities, and financial and telecommunications regulators have become more active with inquiries, audits, and enforcement activities – sometimes in response to employee and customer complaints and other times as part of a proactive initiative.

It used to be that privacy was the roadblock to global data. Today, privacy compliance steps can be the enabler of global markets and global business effectiveness. Management can ask what steps it needs to take to make a certain global process a reality. Although this does not mean that just any transfer or use of personal information will be warranted, it does imply that legitimate activity and transactions can take place with the proper policies, procedures, and controls.

If your business is global or becoming more so, have you:

- Cataloged cross-border transfers of personal information within the corporation and among third parties?
- Addressed the legitimacy of all such transfers?

## 9. Building a Better Mousetrap: Keeping Pace With Technology to Manage Privacy

### Monitoring Tools and Capabilities

After policies are written, controls are developed, and training is administered, information professionals can sit back and relax. Or can they? Any organization has some form of activity that can be considered to be monitoring adherence to policies and the effectiveness of controls. If nothing else, the internal audit department is likely to pass through most business units at one point or another and flag possible issues. However, the questions to be asked are whether the existing monitoring solutions address the main risks the organization is facing and whether they'll be considered reasonable if challenged.

In past years, we have addressed the need for monitoring due to the growing risk of the insider threat – a representative of the company misusing information due to lack of awareness or on purpose. Now, we bring up monitoring in the context of effectiveness – the effectiveness of a privacy program, the effectiveness of joint or overlapping compliance activities, and the effectiveness of balancing privacy risk and business value.



As one form of monitoring, various tools for addressing and preventing data loss or data leakage are available today for organizations to monitor activities on computers, databases, and networks. However, there is not one solution that will address all needs when it comes to monitoring use of personal information enterprise-wide. When looking for technical solutions, it is important to understand what existing capabilities – logs, queries, or other controls – are built into the existing processes and technologies. Whether leveraging available solutions or purchasing new ones, the question of maintenance – the ability to ensure consistent monitoring operations and review of possible findings – is just as important. Last but not least, the presence of national privacy and data protection laws is an increasing challenge for multi-national companies. Faced with a plethora of privacy laws, labor laws, and trade union and works council agreements, organizations are in a constant exercise to balance the privacy of the information they hold and the privacy of their workforce.

When it comes to monitoring the use of personal information, have you:

- Developed a risk-based plan for monitoring the use of personal information?
- Identified gaps in capabilities for monitoring certain operations and the tools that the organization can obtain to close those gaps?
- Reviewed your monitoring activities for compliance with relevant regulations?

## 10. The Buddy System: Including Internal Audit in Privacy Management

### Improving Internal Audit Capabilities

As privacy is increasingly an area of risk for the organization and an area of interest for audit committees, boards, and senior executives, internal audit departments should reflect upon their existing expertise in this area. Internal audit departments need to understand the practical principles of privacy management, so these departments are informed, their findings are accurate, and their suggested solutions can be implemented. Leading international associations for auditors, including those specifically serving internal audit professionals, have been developing audit criteria, guidance, and other resources that can be used for helping organizations assess and meet their risk and compliance goals when it comes to privacy protection.

While professional advisor input and executive interest in privacy have made it clear to many internal audit departments that privacy is an area where they are required to be more active, it is not evident that these departments have resources available to execute on this task and provide meaningful results. Awareness of the existing audit criteria and guidance is a good starting point. Beyond that, organizations need to educate their internal audit personnel on the topic of privacy and make them regular members in information compliance discussions and committees.

To maximize internal audit's effectiveness, have you:

- Made sure that the necessary resources are available to assess the organization's privacy risks?
- Trained internal auditors about privacy risk and compliance?

## Looking Forward

These issues deserve more than a check-the-box exercise. Each one should be addressed as part of the comprehensive and deliberate management of privacy risk and compliance. Founded on policy and governance, an effective program relies on controls, monitoring, compliance activities, and other assurances to help make sure an effective operation is in place.

More than ever, privacy is becoming a mainstream business issue, and, as the Ernst & Young survey indicates, security and compliance remain the primary drivers for privacy in 2008. We are also starting to see the trend back to marketing and customer databases that both drove the topic at the turn of this century and fueled the privacy debate throughout the emerging Internet economy. With the increasing use of interactive technologies, accelerations in customer relationship management systems, and emerging techniques for online behavioral tracking and advertising, we expect the resurgence of marketing as one of the key drivers in privacy concerns in the new year.

As these and other issues become increasingly prevalent and as effectively managing privacy risk and compliance takes on significance of global proportion, Ernst & Young can help.



ERNST & YOUNG LLP

[www.ey.com](http://www.ey.com)

© 2008 Ernst & Young LLP.  
All Rights Reserved.  
Ernst & Young is  
a registered trademark.

SCORE Retrieval File  
No. DY0006