



Top privacy issues for 2011

Insights on IT risk

17 March 2011

Presenter:

Jason Clifton, CA, CISA,
Senior Manager, Advisory

 **ERNST & YOUNG**
Quality In Everything We Do

Every organization that handles personal information — whether for consumers, customers, employees or business partners — faces a number of obligations related to privacy and the protection of that information. The current economic and social media environment has added a particularly complex challenge to the ability of companies to manage privacy and protect personal information.

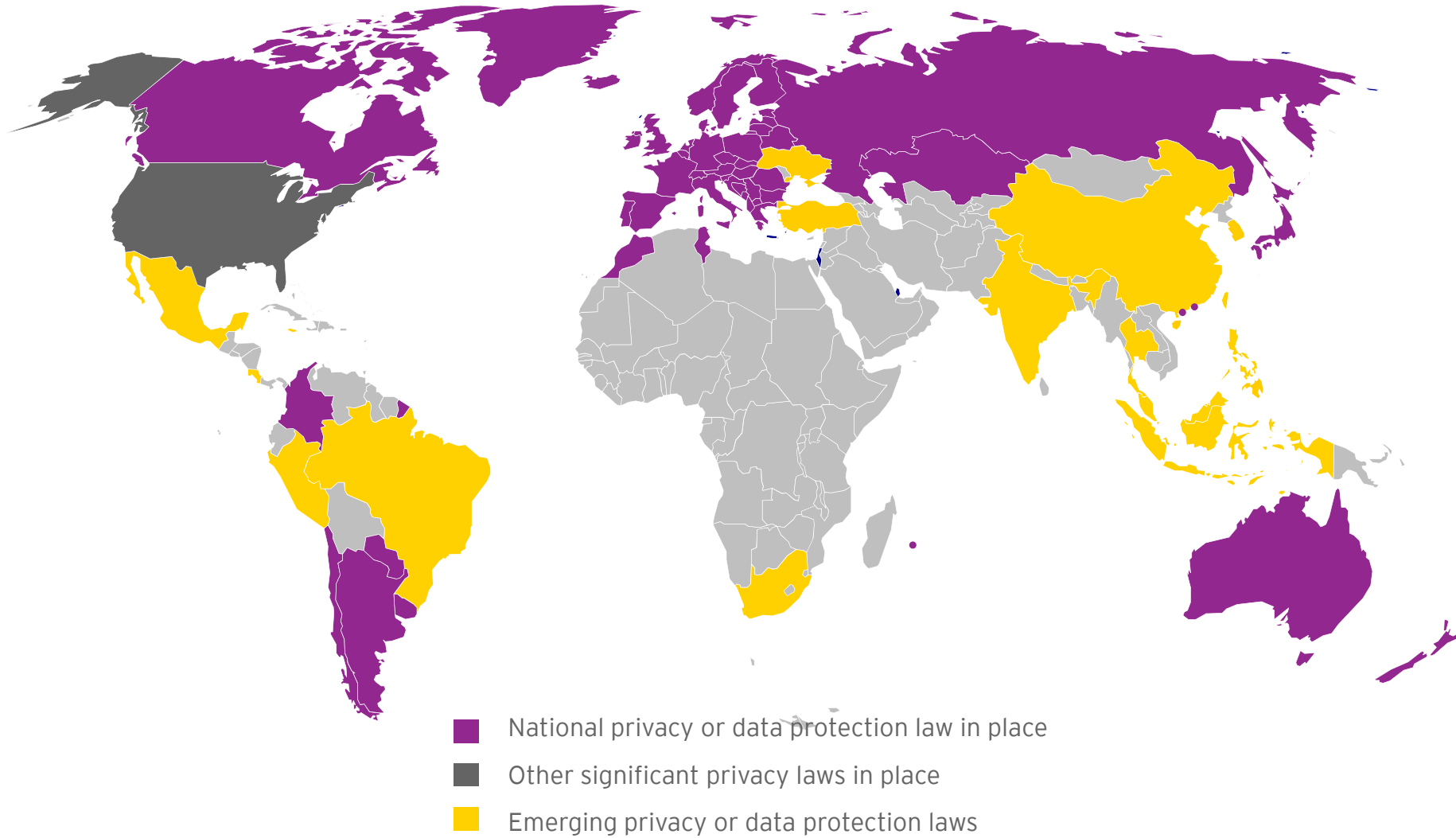
Introduction

- ▶ In Ernst & Young's 2010 Global Information Security Survey, 81% of executives interviewed indicate that managing privacy and protecting personal data is very important or important to their organization.
- ▶ Executives are investing more money to protect the privacy of personal information to respond to ever-increasing government regulation, enforcement and to stem the rising tide of risk.
- ▶ **But are they spending it in the right places?**
- ▶ With parts of the global economy still limping toward recovery, executives continue to ask this burning question as they search for the right balance between spending on privacy protection and taking appropriate levels of risk to manage costs.

Introduction

- ▶ While governments are stepping up regulation and enforcement, privacy protection lacks international cohesion.
- ▶ It is a compliance patchwork with levels of consistency that vary from country to country and industry to industry.
- ▶ With all of this then: **Do organizations have time to wait for global regulatory bodies to reach consensus?**

A global perspective is needed



Privacy: a quick working definition

In the most general terms, privacy is the ability to control **how you are identified, contacted, and located.**

“Privacy encompasses the rights and obligations of individuals and organizations with respect to the collection, use, disclosure, and retention of personally identifiable information”

From the American Institute of Certified Public Accountants (AICPA)

Regulations, laws and enforcement

- ▶ Historically, enforcement of information protection legislation has lacked teeth.
- ▶ Today's regulators plan on changing that by expanding their reach and imposing tougher penalties.
- ▶ The US Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 (the HITECH Act) is one such example.
 - ▶ Under the HITECH Act, state attorneys general can investigate and take action against organizations for failing to secure protected health information.
- ▶ In the EU, the European Commission is in the process of updating the 1995 EU Data Protection Directive.
 - ▶ Plans for strengthening enforcement include providing data protection authorities with the ability to investigate and sue organizations that do not comply.
 - ▶ In advance of the release of new regulations under the EU Data Protection Directive, several EU countries are busy intensifying existing enforcement policies.

Regulations, laws and enforcement

- ▶ The Federal Law on the Protection of Personal Data Held by Private Parties will impact US-based companies operating in other countries such as Mexico and Canada.
- ▶ The Payment Card Industry Security Standards Council, or PCI SSC is an open global forum, launched in 2006, that develops, maintains and manages the PCI Security Standards, which include the Data Security Standard (DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) Requirements.
 - ▶ Compliance and penalties are enforced by each of the payment card brands.

Additional breach notification requirements

- ▶ Breach notification focuses on stakeholder transparency, which has fundamentally altered how organizations approach privacy and data protection.
- ▶ Breach notification failures have resulted in reputation damage and attracted the attention of regulators.
- ▶ In Canada, an amendment to the Personal Information Protection and Electronic Documents Act (PIPEDA) is making its way through the regulatory process and includes breach notification obligations.
- ▶ In the EU, a breach notification regulation for the telecommunications industry will come into effect in 2011.
- ▶ The US Data Accountability and Trust Act requires any organization that experiences a breach of electronic data containing personal information to notify all U.S. individuals whose information is breached. The law requires that the Federal Trade Commission to also be notified.

Additional breach notification requirements

- ▶ To help with breach notification investments in data loss prevention (DLP) tools may be required to help monitor unintentional or intentional data leaks from within the organization.
- ▶ However, it takes more than the purchase of a DLP tool to achieve effective monitoring of personal information to prevent loss.
- ▶ Adopting these tools requires:
 - ▶ Appropriate consideration of the policy that will guide the extent of the tool's implementation (e.g., to stop a possible leak or just report it for a later investigation)
 - ▶ Cross-functional leadership support given its reach in the company.
 - ▶ Necessary staffing with right skills to implement it.

Governance, risk and compliance (GRC) initiatives

- ▶ From a technology perspective, the market for GRC tools continues to develop and offer risk management solutions, and more specifically, solutions for managing privacy.
- ▶ However, few vendors currently offer a full GRC solution, and even fewer offer sophisticated or easy to use modules for privacy management.
- ▶ This is partly due to the complex nature of the requirements and partly due to the difficulty involved in automating key privacy-related updates.
- ▶ GRC technology firms may still be finding their feet and some boutique software companies are trying to take advantage of the gap.
- ▶ In 2011, we expect technology firms large and small to produce new modules that will attempt to better integrate privacy into control monitoring.

Governance, risk and compliance (GRC) initiatives

- ▶ In 2011, we also expect to see progressive organizations take an integrated approach that aligns risk and strategic business objectives.
- ▶ This means shifting GRC investment to focus on the risks that matter, and looking across the enterprise to identify compliance control redundancies.
- ▶ As organizations endeavour to implement a risk transformation program to improve GRC performance, privacy professionals need to make sure they have a seat at the table to ensure that privacy concerns remain a top priority for risk leaders and an integral part of any comprehensive GRC solution.

Cloud computing

- ▶ According to a 2010 Gartner research publication, by 2014 less than 10% of companies will see privacy concerns as a reason not to join the cloud. (“Predicts 2011: Enterprises Should Not Wait to Find Solutions for Business-Critical Privacy Issues,” Gartner, 8 November 2010, © 2010 Gartner, Inc. and/or its Affiliates)
- ▶ The major attractions of cloud computing are cost and flexibility. As some global economies struggle to recover, organizations are looking for more ways to streamline operations and save money.
- ▶ But with cloud use comes responsibility.
- ▶ Organizations need to have robust vendor risk management, including third-party reporting capabilities that address data privacy risks.
- ▶ For example, cloud services located in different geographies raise regulatory challenges as personal information travels across jurisdictions.

Cloud computing

- ▶ Further, as more companies choose to use a third-party cloud provider in 2011, they need to outline specific requirements that enable them to meet their privacy regulatory obligations.
- ▶ Before moving data to the cloud, organizations should analyze their data and develop policies that address both the risks associated with sensitive data and regulatory requirements.
- ▶ Policies should include:
 - ▶ How soon the cloud provider needs to alert the organization of a suspected breach
 - ▶ Be clear about retention periods,
 - ▶ Where the data can or cannot be transferred,
 - ▶ Logging of access by cloud administrators

Mobile devices

- ▶ In 2011, we expect increased regulation that directly addresses protecting personal information on mobile devices, and the sensitive information revealed by geo-location tracking of mobile devices.
- ▶ **Geo-Location**
 - ▶ On the employee level, organizations can keep track of their workforce, comparing where their employees are versus where they are supposed to be.
 - ▶ On the customer level, organizations can offer marketing programs that are based on immediate location.
 - ▶ If organizations decide to use physical location to track employees customers, transparency is paramount.
- ▶ **Encryption**
 - ▶ Traveling data means understanding and adhering to state, federal and international privacy regulations that will vary from one jurisdiction to another.
- ▶ **Training and transparency**
 - ▶ Employees use personal devices for work - where should the organization draw the line in terms of infringement on personal privacy? What is being monitored?

Increased investment

- ▶ In 2011 we will see an increase in privacy and data protection investments that will focus on two issues:
 - ▶ Program initiatives.
 - ▶ Technical controls.
- ▶ Organizations will once again review their governance structure through a privacy and security lens.
 - ▶ They will launch new privacy programs, including updated policies, new procedures and awareness programs, training, data loss prevention (DLP) tools and will recruit talent accordingly.
- ▶ In terms of technical controls, 2011 promises more spending in this area as organizations rely more heavily on controls to manage personal information.

Increased investment

Questions to consider :

- ▶ Have you assessed your budget needs in light of the evolving risk and compliance landscape?
- ▶ Have you reviewed the necessary positions for effective governance over your privacy and data protection activities?
- ▶ Have you consulted with your organization's privacy professionals regarding the investment in technology to monitor the use (and possible abuse) of personal information?



More privacy assessments

- ▶ According to our 2010 Global Information Security Survey, 54% of participants are already using internal auditing to test controls as a means of controlling data leakage of sensitive information. In 2011, we expect that number to increase.
- ▶ The American Institute of Certified Public Accountants (AICPA) and Canadian Institute of Chartered Accountants (CICA) Privacy Task Force's Generally Accepted Privacy Principles (GAPP) describe a comprehensive framework developed to allow the auditing and development of privacy programs.
- ▶ The GAPP helps management develop effective policies to address privacy risks. They are gaining widespread recognition and use in the design, measurement, monitoring and auditing of privacy programs.

Service provider reporting standards

- ▶ In our 2010 Global Information Security Survey, 41% of participants indicate that service providers and outsourcing rank among their top five areas of IT risk.
- ▶ Organizations traditionally seek a Statement on Auditing Standards No. 70 (SAS 70) reports to get an independent assessment, although these reports are not normally intended or robust enough to address privacy, or even security for the most part.
- ▶ The AICPA is in the process of issuing new guidance on service organization controls (SOC) reporting (SOC 2, Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy), which will allow service providers to report on their privacy and security controls.
- ▶ This new report will provide transparency and insight into the privacy and security practices of service providers, permitting them to demonstrate that they have effective privacy and data protection practices in place.

Privacy by Design

- ▶ Instead of treating privacy as an afterthought, Privacy by Design offers a proactive and prescriptive response that is entrenched into the very fabric of the organization.
- ▶ Privacy by Design gained international recognition with the signing of the Privacy by Design Resolution at the 32nd International Conference of Data Protection and Privacy Commissioners.
- ▶ The resolution ensures that privacy becomes an essential component of privacy protection by embedding it into new technologies and business practices from the beginning.
- ▶ The resolution also encourages organizations to adopt Privacy by Design principles as a fundamental means of operation.

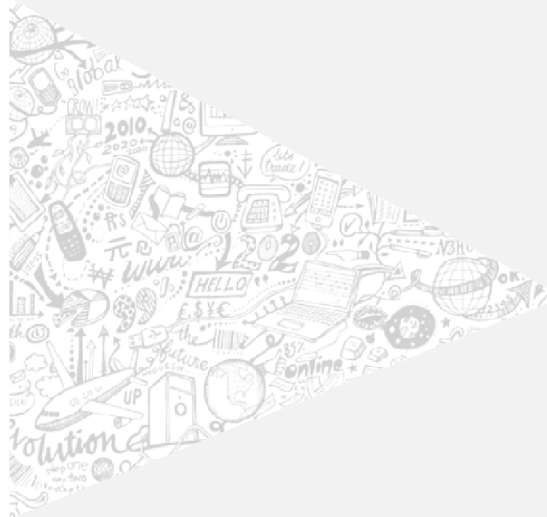
Social networking

- ▶ Despite the development and growth of privacy regulations, regulators find it difficult to accurately capture the particular challenges that come with sharing personal information on social networks.
- ▶ For example: The right to be forgotten has yet to be addressed.
- ▶ Companies need to be transparent about their expectations of employees' behaviour on social networking sites (as applicable to the organization) and whether such activities may be monitored and used to discipline them.
 - ▶ For example: Recruiters should have policies about whether and how to use social networks to mine for information on candidates and should communicate those intentions clearly when candidates come in for an interview.
- ▶ Merely disabling social network use in the workplace is not a sustainable solution.

Social networking

Questions to consider :

- ▶ Have you considered the possible privacy risk and compliance challenges before using social media sites for commercial purposes?
- ▶ Have you brought together your compliance and HR groups to discuss the approach and policies to follow regarding the personal information on social media sites of employees and job candidates?
- ▶ Have you clearly communicated your expectations to employees regarding their communication on social networking sites where they are identified with your organization, or otherwise interact with colleagues or customers?



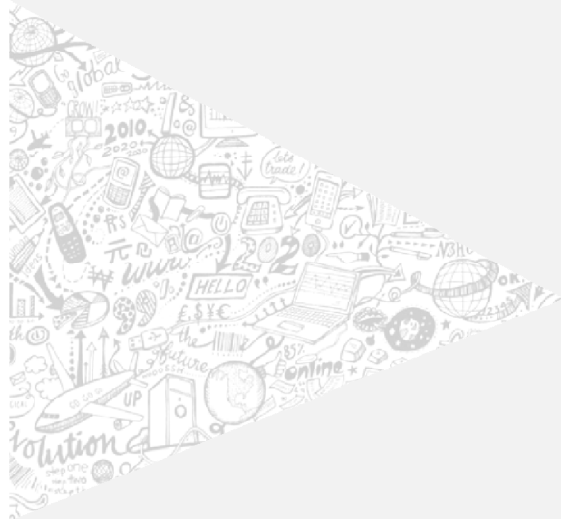
Evolving privacy professional expectations

- ▶ With the ever-increasing scrutiny on privacy protection, it is no surprise that the privacy profession is evolving well beyond the position of the chief privacy officer.
- ▶ Organizations with privacy offices are recruiting and training privacy professionals to focus on specific areas of the business.
- ▶ In 2011, organizations will increase their hiring of privacy professionals, reversing the head count loss privacy offices experienced during the economic downturn.
- ▶ Several organizations are improving the privacy function by merging information security, privacy and other functions (HR, legal, sourcing) into virtual information risk governance organizations, which take a more holistic approach to data protection.

Evolving privacy professional expectations

Questions to consider :

- ▶ Have you considered specific positions in your organization that can benefit from additional training and certification in privacy?
- ▶ Have you identified specific certification requirements for professionals handling personal information in marketing, IT, internal audit, compliance and legal in your organization?



Appendix A - Privacy framework

The privacy framework explains what an organization needs to do well to be able to effectively manage privacy risk and compliance.

The **business level performance layer** describes the organization’s use of personal information throughout its business processes and considers the infrastructure of systems and third parties.

The **risk management and compliance layer** defines the people, processes, and technology used to protect and govern the use of personal information throughout the organization.

Atop them both, the **governance layer** defines how all that is managed.

How will you do this?

- Informally or formally?
- Integrated with other risk and compliance efforts, or separately?
- At the corporate level, within the business units or at affiliates?



Ernst & Young LLP

Assurance | Tax | Transactions | Advisory

About Ernst & Young

Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 141,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

For more information, please visit www.ey.com.

© Ernst & Young LLP 2011 All rights reserved.
Confidential and Proprietary.

