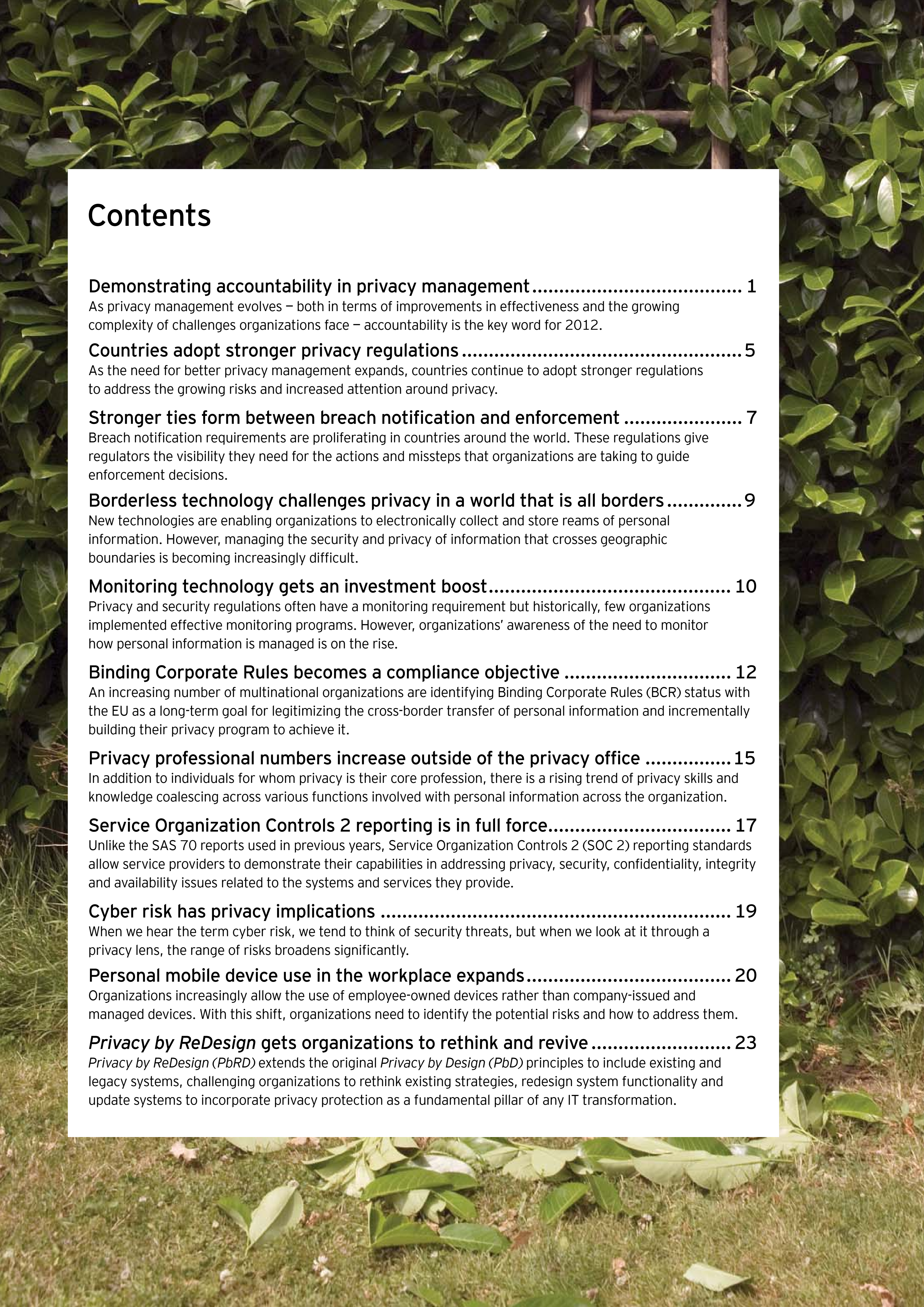
Insights on IT risk
Business briefing

January 2012

Privacy trends 2012

The case for growing accountability

Ernst & Young
Quality In Everything We Do



Contents

Demonstrating accountability in privacy management

In researching the privacy trends for this long-standing annual publication, our privacy professionals analyzed many of the issues our clients are facing across industries and geographies. We noticed a common theme among the trends that have emerged from our analysis — **accountability**.

As privacy management evolves — both in terms of improvements in effectiveness and the growing complexity of the challenges organizations face — accountability is emerging as a fundamental component of handling personal information. In particular, regulators and executives are looking to organizations to be more accountable for their actions.

We are seeing this phenomenon across all ranges of the spectrum. On an individual organizational level, accountability is taking form in:

- Adopting *Privacy by Design (PbD) and Privacy by ReDesign (PbRD)*
- Redefining the role of the privacy professional
- Embracing the concept of BCR
- Improving internal monitoring, including the use of data loss prevention (DLP) tools

At higher levels, governments are taking steps to regulate the use of personal information, and industry groups are exploring self-regulation to stem the tide of increased government action. On the government side, in 2011 in the European Union (EU), the European Commission (EC) amended its Electronic Communication Directive to give consumers more control over their personal information. As part of its overall strategy to update EU data protection rules, the new EC directive requires EU member states to compel electronic publishers to get permission from users before tracking their online behavior through cookies.

To avoid greater regulation, organizations in the retail and consumer products industries and GS1, a supply chain standards organization, are working with privacy commissioners to voluntarily set guidelines that address the privacy implications of using radio frequency identification (RFID) technology in their operations. Retailers across Europe are increasingly using RFID tags — electronic tags that use radio frequency to transfer data attached to an object for identification or tracking purposes — to improve supply chain efficiency. By increasing accountability in the form of self regulation, the industry is working to demonstrate that RFID tags can be used without compromising European consumers' personal privacy.

To achieve greater accountability, many organizations will have to rethink their approach to privacy within the context of their broader IT strategy. As organizations undertake IT transformations to upgrade and align legacy networks, systems and applications, privacy needs to be embedded as a fundamental pillar of the transformation process rather than an afterthought that is bolted on.

As regulators become increasingly interested in organizational accountability, now is not the time to wait for laws to dictate action on privacy. Laws may take years to implement but the consequences of a breach — or lack of accountability — can be immediate, visible and costly.

Dr. Sagi Leizerov

Americas Leader of Privacy
Advisory and Assurance Services
Ernst & Young

Escalating tension around privacy calls for more accountability

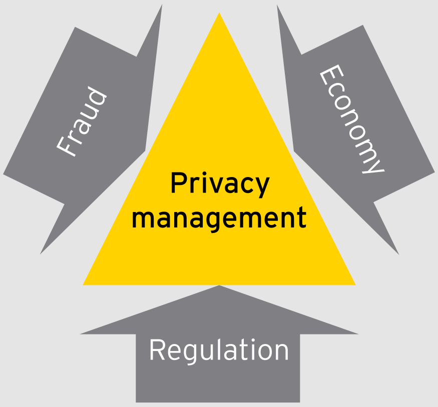
During the last decade, significant changes in the approach to privacy have escalated the tension between individuals and organizations. This tension appears in two distinct areas: the market's redefinition of privacy management; and technology's redefinition of privacy invasion.

Redefining privacy management

Three influencing factors have changed how organizations around the world manage personal information.

1. **Fraud.** Identity theft and privacy breaches are just two examples that highlight abuses of information that have garnered increased attention. Multiple instances of individuals, organized criminals or sovereign nations illegally accessing personal information for criminal or political purposes have pushed organizations to become more vigilant in securing the personal information they collect. Attempting to avoid the need to notify individuals of a possible breach of their personal information (as required by many breach notification regulations) is also an important influencer.
2. **Economy.** Although fraud is on the rise, economic uncertainty in global markets still leads many organizations to do more with less. Economic circumstances reshaped privacy programs, forcing them to function with fewer resources. Although this trend is turning, it will take a few years for the damage to privacy governance from the global economic crisis to disappear.

3. **Regulation.** For many organizations, the prolific increase in privacy regulation has turned privacy management into a never-ending compliance exercise. Regulatory compliance places a significant burden on resources within the organization, leaving little time and resource capacity to focus on the privacy risks that regulations do not cover.

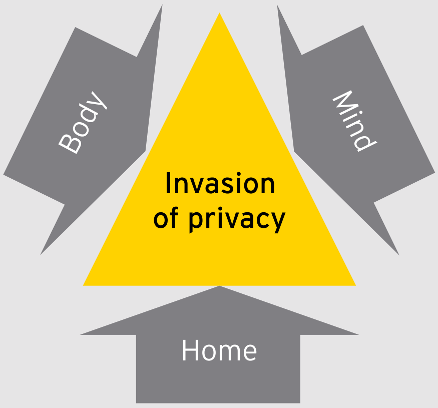


Redefining invasion of privacy

Historically, people have always had some notion of privacy. The basic concepts of privacy to which most people could always relate are: the privacy of our body; the privacy of our thoughts (our mind); and the privacy of our home.

Technology has shifted these boundaries for individuals and the organizations with whom they interact. In today's environment, organizations no longer collect only commercial personal information such as transactions, purchase histories or preferences. Technology is enabling organizations to reach past our personal privacy boundaries in the name of information gathering.

- **Body.** Facial recognition and airport scanners are two examples of technology undermining our control over the privacy of our bodies. Facial recognition relieves us of our anonymity in the world and airport scanners can lay bare our entire bodies for inspection. This kind of technology could create an uncomfortable relationship between individuals and organizations that can lead to a permanent breach of trust if used improperly.
- **Mind.** There was a time when we shared our thoughts only with those whom we spoke or corresponded. Today, on the web, we share our thoughts with the world sometimes by choice, other times without us knowing. Through Facebook, Twitter, blogs and other social media we make a conscious choice to express ourselves, often with limited control over how our comments will be further exposed. Our thoughts are also shared inadvertently, through search engine queries, activities on certain websites and by organizations that use cookies or super cookies that surreptitiously collect our actions and reactions to the content on the screen.
- **Home.** At one time, the biggest and boldest privacy solution was the invention of the door. Today, doors do little to protect our privacy. Smart grids can track our energy consumption with surprising detail that allows others to discover and infer personal details of our lives. Thermal imaging also has the ability to track movement within the home by tracking body heat. Often fodder for action and spy movies, we see police or armed forces using thermal imaging cameras to track their enemy. That technology can also be used in real-world circumstances again, without us knowing.



Governments globally are racing to introduce privacy regulations to safeguard our personal privacy. Unfortunately, regulations are sometimes too broad to have any meaningful impact, and they are almost always one or more steps behind every new innovation that could compromise our privacy.

Rather than placing the onus on regulation, it is time for both organizations and individuals to be accountable for privacy. Organizations need to be accountable for the information they collect or intend to collect from individuals. They need to be open and transparent about what information they are collecting, and they need to validate that the data they do collect is securely protected. However, the onus cannot be entirely on organizations. Individuals also need to be accountable for their information in how they use technology and interact with organizations. They need to increase their knowledge about what they are sharing and with whom they are sharing so that they can make informed decisions and maintain control of the privacy of their bodies, thoughts and homes.

As markets continue to redefine privacy management, and as technology continues to push the boundaries of our privacy, regulators and individuals are looking to organizations to be more accountable for the personal information they collect. But it is also important that individuals be accountable for their own actions. Ultimately, for the tension to ease and trust to endure, accountability over the protection of personal information needs to be everyone's responsibility.

Sandy Hughes

Global Information Governance and Privacy Executive, Procter & Gamble

Past Chairman, International Association of Privacy Professionals

Leading by example with accountability

Accountability has always been a key element of Procter & Gamble's (P&G) Global Privacy Program. As one of the first companies to sign on to the EU-Department of Commerce Safe Harbor certification, we used those principles and the OECD and Fair Information Practices as the basic foundation to design our Global Privacy Program. For example, as required for Safe Harbor, we have in place robust program oversight, accountability measures and audit schedules, as well as ongoing program monitoring and reporting that we extend to other operational areas of the company.

Having regulators more interested in accountability doesn't change how we as a company approach privacy, but it can help to drive consistency in accountability practices across companies thus elevating the trust consumers have in all of us within an industry. Self-regulation guidance such as the SEC Elements of an Effective Compliance Program, the FTC Online Behavioral Advertising Principles and the EU RFID Privacy Impact Assessment Framework, all of which have been developed under the auspices of regulators, help organizations to know what regulators are looking for should there be legislation and/or enforcement action and what companies should have in place to prove accountability in the case of an unfortunate mistake that results in a breach.

The increased focus on accountability presents a great opportunity to bring to the forefront those companies that have been doing the right thing and provide leading practices as role models for other companies who may not have the same resources to improve the compliance and efficiency of their programs and thus trust among the consumers we share.

Countries adopt stronger privacy regulations

As the need for better privacy management evolves, countries continue to adopt stronger regulations to address the growing risks and increased focus on the collection and use of personal information. Countries that have no privacy regulations are realizing the urgent need to address the issue. Countries with existing privacy regulations are updating laws in an attempt to keep pace with technological advances to address a rapidly changing landscape and emphasize accountability.

Many of the countries that are adopting privacy regulations — in Asia and Latin America in particular — are competing for outsourcing jobs. In 2011, India, a sizable outsourcing destination, adopted new privacy rules. India's Information Technology Rules 2011 impose significant limitations on how businesses can handle personal information. Under the new rules, organizations that collect personal information will be required to provide notice to the individuals from whom they are collecting it. The new rules also mandate organizations to take all reasonable steps available to secure personal information, offer a dispute resolution process when issues arise and publish or otherwise make privacy policies available. India's privacy rules cover any personal information collected in India or transferred to the country.

In 2012, we expect to see Singapore implement a new legal framework for consumer privacy protection that includes requiring informed consent from individuals for the disclosure and collection of personal information.

In Latin America, countries that currently have data protection laws or are drafting them are mainly following the European data protection model. However, without an integrated regional legal system, such as that in the EU, the laws that countries are drafting and adopting contain significant differences. For organizations operating in multiple Latin American countries, this inconsistency will prove challenging.

In 2010, Mexico, another significant outsourcing destination, adopted a broad privacy regulation that focuses on the private sector. The Federal Law on the Protection of Personal Data Held by Private Parties is expected to come into force in 2012. Other privacy laws that could be enforced in 2012 include those passed by Peru and Costa Rica in 2011. Colombia is in the process of passing privacy legislation and Brazil is strengthening existing regulations to more closely follow the EU model.

Many of the countries that adopt privacy regulations for the first time still need to prove that these regulations will be enforced. This could be a challenge for new data protection authorities in those countries if their governments do not provide them with the requisite resources to enforce the laws. There are also challenges related to awareness: the lack of awareness of people regarding their new privacy rights and the lack of understanding by the companies that operate in these countries of their new obligations.

As countries increasingly push for greater accountability, organizations need to understand how the increase in privacy regulations impacts their business. The diversity in privacy requirements across countries makes it more difficult for responsible players to comply. As multinational organizations expand their geographic footprints, geographic boundaries are becoming increasingly irrelevant. However, the regulatory variations make compliance a consistent and evolving challenge. Harmonizing privacy regulations across jurisdictions is critically important. Unfortunately, harmonization is not a trend we expect to see in 2012.

Questions to consider

- Have the privacy regulations in the jurisdictions in which you operate changed in the last year?
- If you outsource to countries with new or updated privacy regulations, have you considered what impact that may have on your operations in those countries?
- If you are off-shoring to countries with new or updated privacy regulations, have you considered the impact of those regulations on your local employees?

Lisa Sotto

Partner and Head of the Global Privacy and Information Security Practice, Hunton & Williams LLP

The move toward a more comprehensive privacy regime in the US

In the past year, there has been explosive growth in the development of privacy laws around the world. For example, in 2010, Mexico enacted a comprehensive privacy law and drafted regulations in 2011 to implement the law. New laws were enacted in South Korea and Peru, with Colombia following close behind. Also in 2011, India issued controversial new privacy regulations. In Taiwan, there has been more of an evolution than a revolution as the country is amending and expanding existing requirements. We expect this global trend to continue and even accelerate in 2012.

The US is out of step in its regulation of privacy, although there are efforts underway to more closely align the US's position with that of other countries. While others are moving toward more comprehensive regimes, the US continues to regulate privacy by industry or data type. For example, we have a law to protect the privacy of children but only if those children are under 13 and the information is provided online. There are individual privacy laws for various industry sectors. Health care and financial services are key examples. The sectoral regime in the US is not a model that any other country is following. Where other countries are developing comprehensive, omnibus laws, the US regime remains fragmented and piecemeal.

We don't expect Congress to achieve consensus in 2012, but it may move toward a more comprehensive approach in the next three to five years. Certainly, it's in everyone's interest to do so, particularly as new technologies continue to emerge. It seems as though each new innovation, like cloud computing or location-based services, prompts regulators to consider legal protections anew. But we would cease to innovate if we had to chase each new development with legislation. Ultimately, the US will need an overarching framework to address in a uniform manner new technologies as they are developed.

One way companies are responding is to look inward. Some businesses are choosing to implement *PbD* and other accountability regimes. They are embedding privacy into new products and services so that the issue is considered right from the start.

Stronger ties to form between breach notification and enforcement

In June 2011, the University of California at Los Angeles (UCLA) Health System agreed to a $865,500 settlement with the U.S. Department of Health and Human Services (HHS) for violating the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules. UCLA Health System employees were accused of improperly accessing protected health information of high-profile celebrities and other patients. HHS further concluded that the UCLA Health System itself had not sanctioned or otherwise taken action against the employees that had committed the privacy violations.[1]

The UCLA Health System enforcement was the third major action the HHS had taken in 2011, bringing enforcement totals for the first half of 2011 to more than $6 million. Since 2003, the HHS and the Office of Civil Rights (OCR) has investigated and resolved over 14,105 privacy violations. We expect that number to increase in the years to come as the HHS plans to audit and enforce violations under the Health Information Technology for Economic and Clinical Health (HITECH) Act, which addresses breach notification.

The US is not the only country stepping up its enforcement of privacy violations. Breach notification requirements are emerging in countries around the world — from Brazil, Uruguay and Mexico in Latin America, to Germany in Europe and Japan in the Asia-Pacific region. As they do, regulators are increasingly using their enforcement functions to give force to breach notification violations.

In 2012, we expect to see a tighter relationship forming between breach notification regulations and enforcement actions. Many proposed and newly enacted breach notification regulations omit the requirement to notify the individual — initially or at all. Instead, the focus is on notifying the regulator. This gives the regulator the power to decide what next steps are needed (including a notification to the impacted individuals) and appropriate enforcement actions.

In the EU, the EC is considering updating the ePrivacy Directive and has conducted public consultations with telecommunications and internet operators. The EC wants to introduce new rules to give greater definition to existing legislation that better guides organizations on the circumstances and procedures for breach notification. The EC is focusing specifically on telecoms and internet operators given the amount of personal data these organizations collect and the higher risk that breaches might occur.

Last year, we commented on planned amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA), which included breach notification requirements. Among other updates, the amendments give Canada's Privacy Commissioner more discretion over the complaints that cross her desk, as well as increased availability of resources to investigate privacy complaints. The Privacy Commissioner will also have additional powers to share information of investigations among counterparts, nationally and internationally.

Many privacy advocates applaud stronger regulations that give privacy commissioners and regulators more power. However, critics wonder whether concentrating decision-making power with the regulator, as is the case with new breach notification requirements, will distort how organizations address privacy risk and compliance. Some worry that it will give organizations incentive to only address areas that lead to breaches, while ignoring other privacy-related considerations, such as limiting the collection of personally identifiable information and providing clear notices.

In 2012, we expect to see more empowered regulators and privacy commissioners increase the number of audits they conduct and use reported breaches as the direction those audits take. These audits will likely be broader in scope than the incident or breach that triggered them in the first place.

Questions to consider

- Have you identified the different repositories, both structured and unstructured, that your organization uses to store sensitive personal information?
- Do you understand what your regulators would expect you to demonstrate in a privacy audit?
- Are you correcting root causes when remediating a breach? Or are you limiting your actions only to the weakness identified?

[1] Hunton & Williams LLP, "HHS Announces $865,500 Settlement with UCLA Health System for HIPAA Violations," *Privacy and Information Security Law Blog*, 8 July 2011, http://www.huntonprivacyblog.com/2011/07/articles/hipaa-1/hhs-announces-865500-settlement-with-ucla-health-system-for-hipaa-violations.

Kirk Nahra

Partner, Wiley Rein LLP

A health care perspective: breaches are immediate, enforcement incremental

In 2012, we expect US health care companies to see incremental increases in enforcement based primarily on security breaches related to the HITECH and HIPAA standards. What health care companies may be more worried about in the coming year, however, are the immediate, negative news stories, lawsuits and overall client dissatisfaction that could result from a breach.

From a compliance and enforcement perspective, 2012 is likely to be a transition year. We expect new rules to come out at the end of 2011 or beginning of 2012 but compliance won't be required until July 2012 at the earliest (and likely later). It may then take a year of understanding the rules, determining where changes need to be made and updating privacy and security standards to adhere to the rules. In other words, it could take three years from the time the law was passed (in 2009) to the government having final regulations that companies follow.

In the meantime, breaches keep occurring. In health care, in particular, breaches are a huge challenge because there are so many ways patients could be impacted. The biggest risk involves inappropriate internal access to information. Health care companies use immense amounts of data and that data is becoming more important as the sophistication of health care increases. More people need access, but giving more people access generally creates several issues. These may include people who are supposed to have access to data who misuse their access. The case of hospital workers snooping on celebrity medical records is a great example. Then there are the people who look at data for which they have interest. These people may sneak a peek at a family member's records (usually for "good" reasons) or those of a former love interest (often for "bad" purposes), which may not appear problematic but is both unlawful and completely inappropriate. Even worse are situations where internal access is used to commit identity theft or health care fraud.

In all of these instances, unauthorized access may be difficult to prevent on the front end (since employees typically need access to data for their jobs), but companies need to have back-end systems with appropriate monitoring systems that enable the companies to track how employees are using private information.

When a breach occurs, a company's best defense is to act quickly. In many cases where the breach is small, companies can take steps to make sure nothing bad happens. If a company knows about the breach and can fix it quickly, the organization can greatly minimize or eliminate the impact of the breach. Minimizing the potential harm is enormously important. Companies cannot prevent everything but a quick response can reduce the risk.

Borderless technology challenges privacy in a world that is all borders

Many countries have regulations that apply specific restrictions over the flow of information to other countries with different privacy protections. The EU set the bar with EU Data Protection Directive 95/46/EC — a privacy regulation model that can now be found outside the EU, including jurisdictions in Latin America. However, like the EU, inconsistencies among countries in the application of their privacy regulations present persistent challenges.

Even as regulations reinforce geographic borders, businesses are using technologies that systematically erase those borders. Global collaborative applications that allow employees to share data, cloud computing, centralized network architecture, centralized web filtering and call centers that "follow the sun" are all excellent examples of technology solutions that increase opportunities for businesses to save money and improve their performance but require that personal information crosses international borders. Two additional trends have fueled the increasing use of these technologies: cost cutting in response to the global economic crisis, and an underlying emphasis on collaboration at work and in our personal lives. These two trends have increased the number of compliance and privacy risks organizations need to address to remain accountable for the personal information of their customers.

Technology has enabled organizations across all sectors and jurisdictions to electronically collect and store reams of personal information. But as business demands more integrated IT solutions, managing the security and privacy of information that crosses geographic boundaries becomes increasingly difficult. Regulators will always be in a position of having to react to the challenges new technologies present. It is this conflict between privacy regulations and technological developments that underscore the importance of accountability within organizations to address privacy not on a location-by-location, regulation-by-regulation basis but in a comprehensive manner.

Organizations should be more proactive developing forward-thinking privacy management strategies that balance existing regulatory requirements with technological developments. Organizations also need to understand the nature of their IT architecture and the possible impact of the new technological solutions that they choose to adopt. In some cases, even simple controls and training can go a long way to increase compliance and contain risk.

Questions to consider

- Does your privacy impact assessment process address the cross-border transfer of personal information and related regulatory limitations?
- Does your network architecture design route data from different countries to a central location?
- Have you identified solutions that holistically address compliance needs and limit the risk of inappropriate access and exposure of personal information across the organization?

Monitoring technology gets an investment boost

Monitoring how employees handle the personally identifiable information that organizations collect from their customers, vendors, contractors, external partners and others with whom they interact is still a significant area of weakness. In Ernst & Young's *2011 Global Information Security Survey*, only 30% of respondents indicated that their organizations have implemented a process to monitor and maintain privacy-related controls.

Privacy and security regulations often have a monitoring requirement but historically few organizations implemented effective monitoring programs. Many IT systems maintain logs but mining these logs for data that can help with privacy monitoring is often costly and inefficient. Governance, risk and compliance (GRC) tools are excellent for monitoring security controls and presenting monitored information but they are less effective at monitoring privacy-related controls and data.

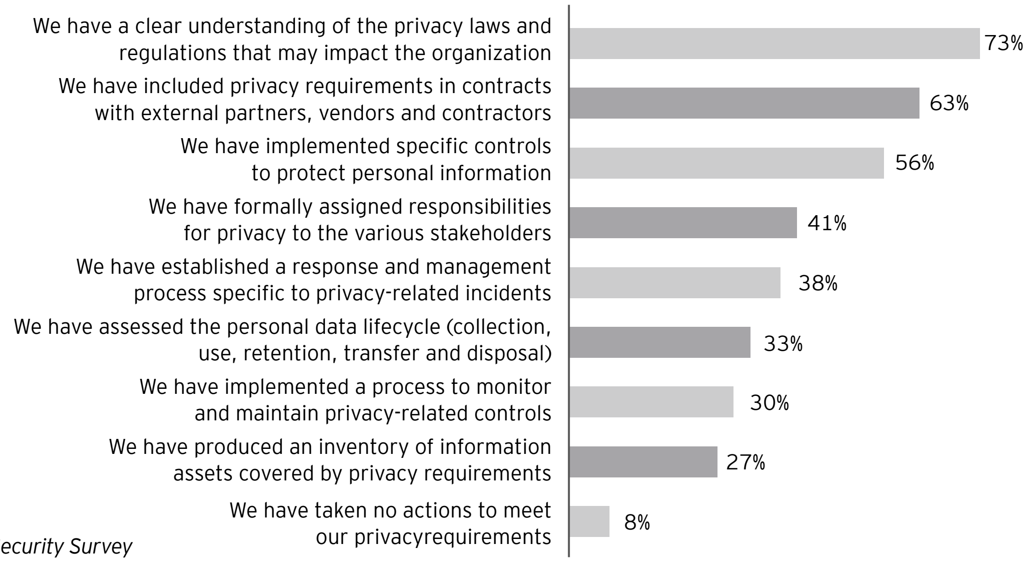
However, organizations' awareness of the need to specifically monitor how personal information is managed is on the rise. An increasing number of organizations are implementing DLP tools tracking, global collaborative applications that allow employees to share data and other tools that track network folders. Furthermore, organizations are implementing applications that monitor use patterns on databases. Many of these technologies are increasingly becoming common business practices rather than leading practices.

In 2012, there are two factors that we expect will drive organizations to increase their investment in privacy monitoring tools:

1. Demonstrating greater accountability through monitoring of the personally identifiable information they collect.
2. Mitigating breaches that could harm the organization's reputation and brand.

However, we do not expect to see a convergence of information security and privacy monitoring systems in 2012. Privacy monitoring will likely remain a feature that needs to be added to existing IT infrastructure for the next few years.

Which of the following statements can be made by your organization regarding privacy?



Ernst & Young's *2011 Global Information Security Survey*
Shown: percentage of respondents

Questions to consider

- Have you identified whether privacy regulations require that you monitor personal information use?
- Have you assessed the new monitoring tools available for the systems and applications you commonly use for processing personal information?
- Have you budgeted for increased investment in monitoring technologies to address privacy risks and compliance requirements?

Binding Corporate Rules become a compliance objective

An increasing number of multinational organizations are identifying BCR status with the EU as a long-term goal for legitimizing the cross-border transfer of personal information. BCR is a set of internal guidelines, similar to a Code of Conduct, that establishes policies for transferring personal information within the organization but across international boundaries.

Increasingly, organizations are considering their use of model contracts and Safe Harbor as temporary measures intended to address European requirements until their privacy program is robust enough to obtain BCR status.

The EU initiated BCRs in 2003. For early adopters, the process of obtaining BCR status took as long as 35 months. Under today's process, the average timeframe for achieving BCR status is eight to 13 months. "Prior to 2008, when the process was more demanding, only two organizations achieved BCR status," admits Florence Raynal, Head of the Department of European and International Affairs for Commission nationale de l'Informatique et des libertés (CNIL). "However, since 2008, 17 organizations have adopted BCRs. Another 29 applications are in process and should be completed by 2012."

Obtaining BCR status is not easy, but for many multinationals it can yield the following benefits:

- Endorsement of an existing data privacy compliance program
- In-house awareness of privacy issues
- Elimination of contracts for each transfer
- Mitigation of risks from data transfers to third countries
- Consistency in data protection strategies and practices within the organization

Early adopters of BCR status included GE and Philips. More recently, multinationals Hewlett Packard, International SOS and Bristol-Myers Squibb have all successfully adopted BCRs.

In 2012, we not only expect to see more organizations seek BCR status, we also expect to see more organizations designing their privacy programs in a manner that will support achieving BCRs as a future objective.

Questions to consider

- Is your organization transferring EU personal information to multiple countries outside of the EU and the US?
- Does your growth plan involve an increase in the number of entities and countries to which you will be sending EU personal information?
- Does it make sense for your privacy program to follow consistent policies, controls and monitoring?

Four steps to achieving BCR status

To be approved for BCR status, organizations must complete the following steps:

1. **Designate a lead authority.** A lead data protection authority (DPA) needs to be designated to the organization. This authority usually resides where an organization is headquartered in the EU. The lead authority will coordinate the EU cooperation procedure among other European DPAs.

2. **Draft BCR procedures.** With the help of the lead authority, the organization drafts its BCR procedures. These procedures must meet the requirements established in the working papers adopted by Article 29 Working Party. The organization then submits the draft to the lead authority, who will review and offer comments.

3. **Circulate the BCR to relevant DPAs.** Once the lead authority is satisfied with the draft, it will begin the EU cooperation procedure by circulating the BCR to the relevant DPAs, as well as to those authorities that are not under mutual recognition.

4. **Close the EU cooperation procedure.** Once the BCR has been finalized by all DPAs, the process is considered complete. The organization can then request authorization of transfers on the basis of the adopted BCR by each national DPA.

Florence Raynal

Head of the Department of European and International Affairs,
Commission nationale de l'Informatique et des libertés (CNIL)

BCR instills values that make privacy real

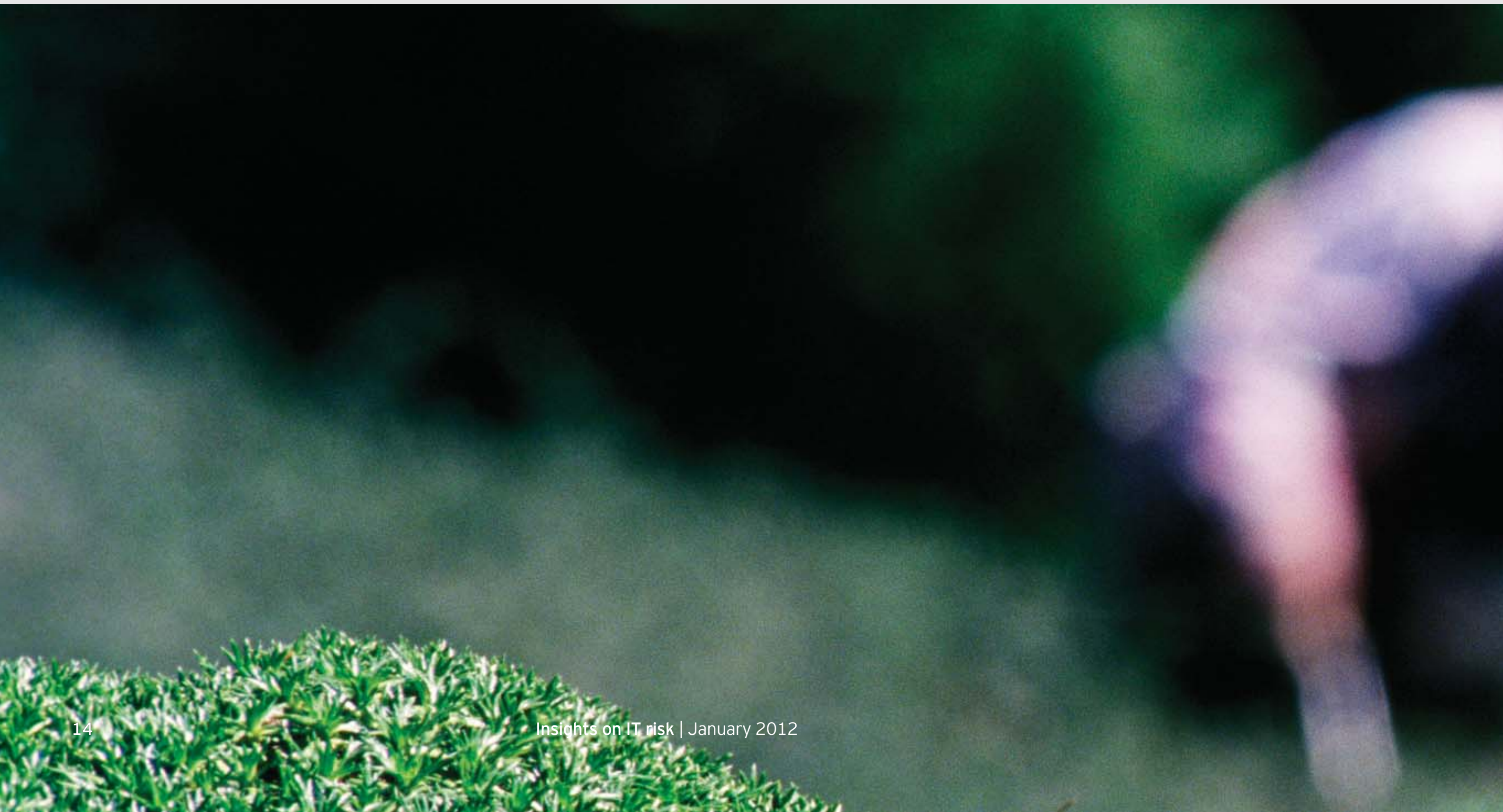
BCR is an efficient tool for compliance. It helps companies make privacy effective and real by instilling values around privacy into the daily life of the company. It also helps them to put in place global policies, internal mechanisms, training of people and systems of cooperation with DPAs. Companies like having these types of policies. In fact, many companies feel it is the only practical solution out there.

As a lead DPA, CNIL has seen tremendous growth in the amount of interest from companies wanting to achieve BCR status. Before 2008, only two companies had adopted BCR. Since 2008, 17 companies have successfully achieved BCR status — seven of which CNIL has served as the lead DPA. There are currently 29 BCR applications in process, 10 of which we are handling. We expect the 29 applications to be adopted in 2012.

We are all trying to process applications as quickly as possible but the processing speed doesn't only depend on the DPA. It also requires considerable coordination within the organization. Nevertheless, we have done much to accelerate the process. Two years ago, the EU instituted a mutual recognition procedure that simplified the process considerably. Prior to 2009, every DPA had to be consulted as part of the application process. Now, when the lead DPA does the work, it represents the work of 20 DPAs that accepted to be part of that system of mutual recognition. The other DPAs recognize the work the lead DPA has done and will not redo it.

With every application we gain experience. Our people are more knowledgeable and DPAs are more comfortable in knowing what to ask from organizations. We develop good relationships with the candidates. Our direct involvement engenders better communication. It is also a good way for the company to know what the DPA expects and which compliance mechanisms need to be put in place.

We are currently in the process of developing BCRs for third-party service providers. We expect it could be an especially good tool for cloud computing and we expect this new framework to be available in 2012.



Privacy professional numbers increase outside of the privacy office

The definition of privacy professional is changing. Privacy is a multidisciplinary subject that requires knowledge of the organization's different functions, as well as an understanding and collaboration with other information stakeholders. In addition to individuals for whom privacy is their core profession, there is also a rising trend of privacy skills and knowledge coalescing outside the privacy office. HR, security, IT, internal audit, marketing, records management and other functions increasingly have some percentage of their role dedicated to privacy.

Many information stakeholders within organizations increasingly understand their need to be at least conversational — if not fluent — when it comes to managing privacy in their function. Collaborating on privacy management is generally a result of cost of compliance failures, as well as the need for greater efficiencies. However, the result is a redefinition of the role of privacy professional in organizations today.

In terms of full-time privacy officers, true to the expectation we articulated in *Privacy trends 2011*, organizations have increased their hiring of dedicated privacy professionals, reversing the headcount loss privacy offices experienced during the economic downturn. As described in more detail overleaf, according to J. Trevor Hughes, President and CEO of the International Association of Privacy Professionals (IAPP), the IAPP has 9,200 members in 70 countries, an increase of approximately 50% in the last two years alone. However, for many of these new members, privacy is not their primary profession nor does it appear in their titles.

Questions to consider

- Have you identified key information stakeholders that play a supporting role in managing privacy risk and compliance?
- Are you providing access to privacy resources, knowledge and certification to professionals who take part in the daily implementation of your privacy program?

J. Trevor Hughes

President and CEO of the International Association of Privacy Professionals

The evolution of the privacy professional

The IAPP is a community of privacy professionals that has seen first-hand how the face of the privacy professional has changed over the years. With 9,200 members in 70 countries we are not a large organization by many standards, but we're also only 10 years old. However, in the last 24 months — arguably the worst economic stretch since the Great Depression — our organization has grown by roughly 50%. On January 1, 2009, we had 5,000 members. By the end of December 2010, we had 7,500 members. When almost every other department was cutting resources, privacy was receiving significant investment.

In addition to an increase in numbers, the IAPP is also attuned to the role the privacy professional plays within an organization. Many organizations have a core privacy function. In larger organizations, there is typically a privacy leader and a small team to support the maturing privacy function. What we are also seeing, however, and this is where I think our membership has expanded the most, is the liaison or champion who doesn't identify as a privacy professional but whose role does include organizational privacy.

Today, the biggest growth area for privacy is in corporate risk management. Increasingly, employees who touch data need to know more than what their fundamental privacy training taught them in the past. HR, marketing, IT and project management professionals all need to know enough about privacy and data protection to avoid the simple mistakes and identify and raise the privacy issues they see within the organization. From that perspective, there are many tens of thousands of privacy professionals who will emerge in the future. They may not identify themselves as privacy professionals but their knowledge and skills will be commensurate with the entry-level privacy professionals we see today.

As the accountability for privacy and personal information protection rises in importance within an organization, so too does the role of the privacy officer. While today's privacy professionals don't have a strong center of gravity within the enterprise, we expect that to change in the years to come. From a regulatory perspective, policymakers are recognizing that laws are not enough — they can't address all of the issues, nor can they address them in a timely manner. As such, the privacy professionals of the future will have more operational involvement. They'll have strong business management skills and deep privacy knowledge. And they'll be tasked with the implementation of principles such as *PbD*, BCR and other comprehensive privacy programs that instill privacy values as much as meet compliance requirements. Privacy professionals will be in the thick of it, which is where they need to be.

Service Organization Controls 2 reporting is in full force

Even an organization with the most robust internal privacy practices and controls cannot comply with its privacy commitments if its service providers do not have similarly robust practices and controls. Many organizations require their service providers to implement privacy practices and controls. However, it is often difficult and costly to verify that key service providers are complying with their commitments. As a result, organizations have asked their service providers to obtain an independent assessment of their privacy and security practices. Previously, organizations seeking such an assessment were making do with reports performed in accordance with Statement on Auditing Standard No. 70 (SAS 70 reports), even though these reports were not intended to address privacy or security.

In 2011, the American Institute of Chartered Public Accountants (AICPA) issued a new framework on service organization controls – *Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2).* Performed in accordance with AT Section 101, SOC 2 reporting replaces the SAS 70 reports but retains their reporting style. SOC 2 reports provide independent assurance based on the Trust Services Principles and Criteria. It offers organizations the opportunity to provide assurance on a wider range of service provisions than simply financial reporting.

SOC 2 reports enable service providers to be transparent and accountable to their clients by demonstrating their capabilities in addressing privacy, security, confidentiality, integrity and availability issues related to the systems and services they provide.

Organizations that outsource can use the SOC 2 reports to be accountable to their shareholders and other stakeholders by improving governance and oversight of service providers.

Each SOC 2 report will contain the following information:

- Independent service auditor's opinion
- Management assertion
- Description of the systems providing the in-scope services
- Description of the controls delivering each of the in-scope criteria based on the principles selected
- Description from the independent auditor of the tests performed and the results of those tests

SOC 2 reporting takes place in three phases:

1. Auditors conduct a risk assessment to identify controls gaps.
2. The reporting organization remediates areas of concern, implementing controls to close the gaps.
3. Auditors conduct the audit performing tests on controls in place and issuing a report based on the results.

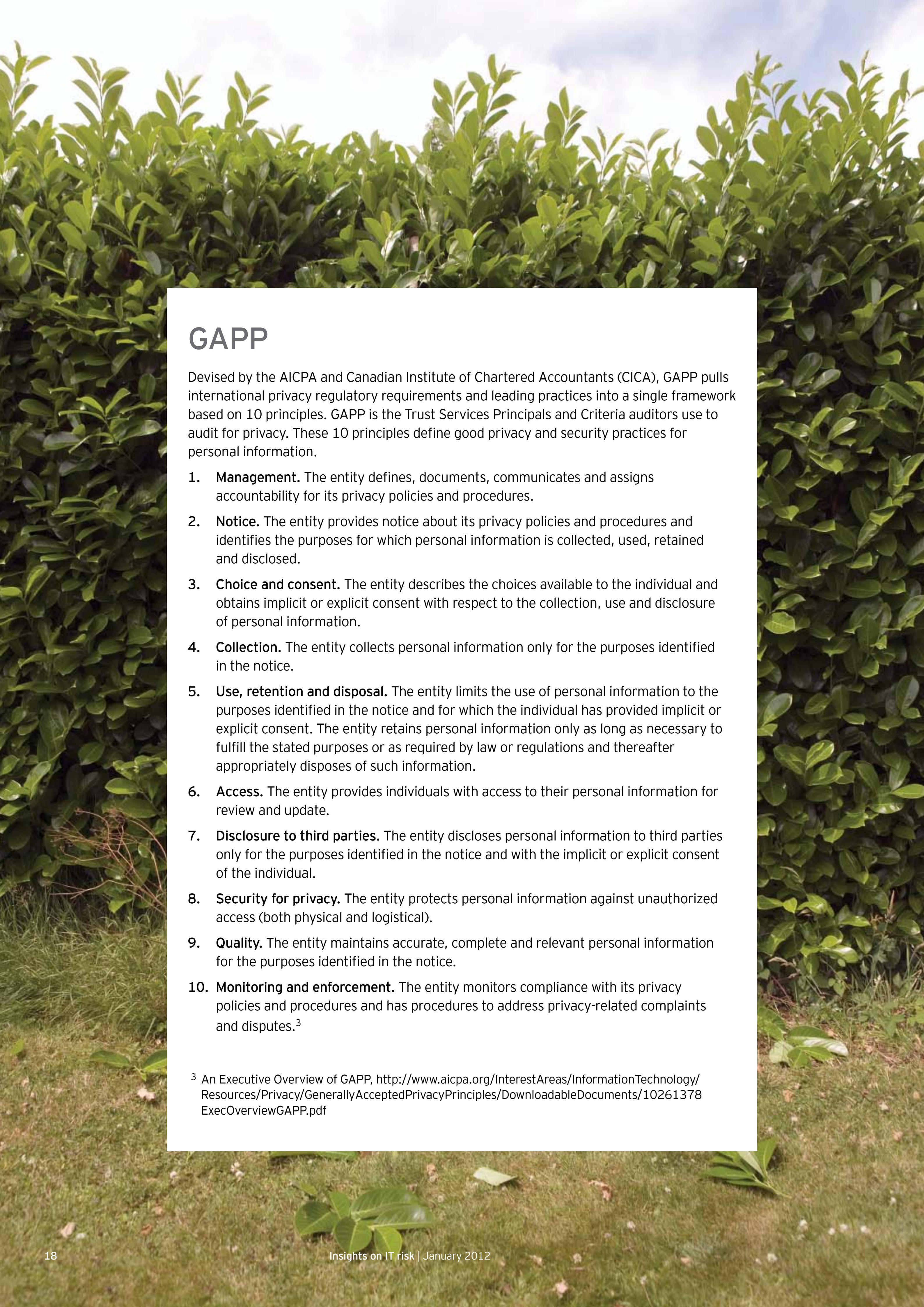
The SOC 2 framework is being mapped to other frameworks (e.g., ISO 27001, and the Cloud Security Alliance – cloud control matrix) for consistency and efficiency of testing. In a recent roundtable Ernst & Young hosted in London, one participant indicated that "the mapping is key" to show how work is done for a SOC 2 report to provide assurance across multiple certifications.[2]

Given that 2012 will be the first full year for SOC 2 reporting, we expect auditors to identify a number of deficiencies during the first phase of the SOC 2 work as organizations attempt to implement controls that address Generally Accepted Privacy Principles (GAPP). As a result, we anticipate that many organizations will use 2012 as a remediation year and that more widespread SOC 2 reports will appear in 2013.

Questions to consider

- Have you relied on your service provider's SAS 70 report as a privacy and security monitoring mechanism?
- Have you discussed with your service provider which controls you expect to see covered in the SOC 2 report regarding the use of your personal information?

[2] Ernst & Young, *SOC 2 – Assurance's silver bullet?*, July 2011.



GAPP

Devised by the AICPA and Canadian Institute of Chartered Accountants (CICA), GAPP pulls international privacy regulatory requirements and leading practices into a single framework based on 10 principles. GAPP is the Trust Services Principals and Criteria auditors use to audit for privacy. These 10 principles define good privacy and security practices for personal information.

1. **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information only as long as necessary to fulfill the stated purposes or as required by law or regulations and thereafter appropriately disposes of such information.
6. **Access.** The entity provides individuals with access to their personal information for review and update.
7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logistical).
9. **Quality.** The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.
10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.[3]

[3] An Executive Overview of GAPP, http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/10261378ExecOverviewGAPP.pdf

Cyber risk has privacy implications

High-profile security failures have made privacy protection a top-of-mind issue for many organizations. In several cases, hackers have gained access to online networks and systems, stealing personal customer data, such as names, addresses, passwords and credit card information. The financial costs of these breaches are often significant, ranging from tens of thousands to millions. The damage to a company's brand and its reputation often costs far more.

When we think of cyber risk we tend to think of security breaches, but when we look at it through a privacy lens, the range of risks broadens significantly.

New technologies have fostered an explosion in mobile application (app) development. Apps give organizations the opportunity to interact directly with consumers. In 2012, we expect to see more organizations developing apps for tablets and mobile devices. Interacting directly with consumers and gaining insight into their behavior will be enticing. Many organizations that want to gain every advantage possible already track behaviors and preferences without considering the privacy implications. Aligning the use of new technologies with an existing privacy program and previously published privacy notices will be a significant challenge for many organizations in 2012.

Social networking, particularly for business, presents similar privacy issues. As we discussed in our *Privacy Trends 2011* report, some organizations already have a presence on social networks to promote products and services and to communicate directly with customers. In doing so, they need to be transparent about why and how they are collecting the personal information customers provide.

How organizations use personal information that employees, or potential employees, share on social networking sites also remains an issue and will be for the foreseeable future. Organizations need to clearly articulate their expectations of employee behavior on social networking sites, and any steps they take to monitor that behavior. The sensitivities associated with the use of social networking sites in the workplace, both with employees and customers as users, is a top privacy concern for organizations large and small in 2012.

The proliferation of new technologies has fundamentally shifted how organizations interact with their customers. Just as organizations seek to develop direct relationships with their customers through the development and use of apps, they also seek advantage through the use of super cookies. Super cookies, also known as "flash cookies," are designed to track user preferences and browsing histories. Unlike typical cookies, however, they are incredibly difficult to detect and remove. Often, they secretly collect user data that reaches beyond the limitations of common industry practice, and beyond previous policies articulated in stakeholder contracts and notices. Obviously, the use of such cookies presents serious privacy concerns. Organizations need to be accountable to their customers by being transparent about the information they are collecting and how they are collecting it. Not disclosing the use of super cookies will be seen as a breach of trust by many users and could result in significant harm to the reputation and brand of the organization.

Although governments are showing increased interest in addressing cyber security concerns, it is unlikely we will see agreement on comprehensive reforms or legislation in 2012. As such, organizations themselves will need to be accountable for defining the parameters of their privacy program. As enticing as data mining through apps or cookies may be, organizations should resist the temptation for the sake of their brand and reputation as trusted corporate citizens.

Questions to consider

- Have you assessed the potential for using social networking sites and web apps for improving your interaction with customers?
- Do you currently have human capital privacy policies, including recruiting policies? Have you analyzed their applicability to different web technologies?
- 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?

Personal mobile device use in the workplace expands

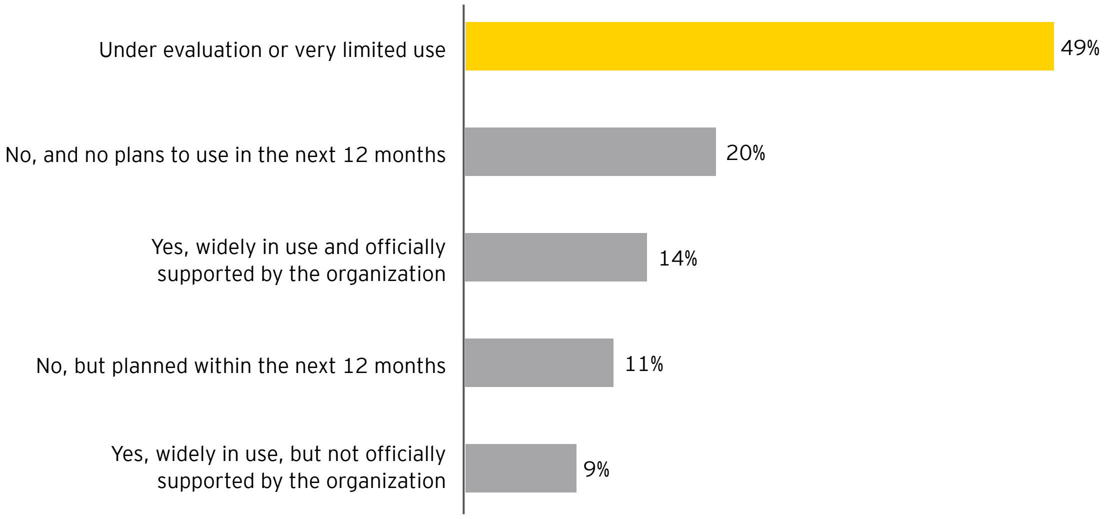
As the functionality overlap among laptops, smartphones and tablets expands, organizations are increasingly allowing the use of employee-owned devices instead of providing devices with a preconfigured system. In Ernst & Young's *2011 Global Information Security Survey*, more than 80% of respondents were either planning to, evaluating or widely using tablet computing.

With this shift in ownership, however, organizations need to identify the potential risks and develop effective strategies that address those risks. In the same survey, the adoption of tablets and smartphones ranked second-highest on the list of technology challenges perceived as most significant, with more than half of respondents listing it as a difficult or very difficult challenge.

Policy adjustments and awareness programs are two measures organizations are using to help address the risks posed by the evolution of using portable media at work. Many organizations are also using tracking and monitoring tools, which are more concerning from a privacy perspective. Organizations need to be careful about how they monitor an employee's personal device that is also being used for work purposes. Controls exist to address security issues, such as encrypting the part of the device where company information is processed. However, monitoring controls that determine an employee's compliance with security policies need to be balanced with the need to adhere to privacy policies.

Ultimately, one of the most effective means of driving privacy accountability within the organization is to make employees aware of and understand their personal responsibilities when using newer technologies or accessing corporate information. This awareness goes beyond high-level policies to pragmatic examples of activities that are permitted and prohibited when using social networks, laptops, tablets or smartphones. A concrete "dos and don'ts" list is the most effective means of communicating the policies and enabling responsible use.

Does your organization currently permit the use of tablet computers for business use?



Ernst & Young's *2011 Global Information Security Survey*

Questions to consider

- Do you allow your employees to use their personal mobile devices for work purposes?
- Have you reviewed your privacy policies recently to ensure they reflect your organization's use of mobile devices?

Caroline Winn

Vice President of Customer Services,
Customer Privacy Office,
San Diego Gas & Electric (SDG&E)

Integrating *Privacy by Design (PbD)* into San Diego Gas & Electric initiatives

SDG&E protects customers' right to privacy by ensuring their personal information is kept confidential. We know that with the advent of smart grid technologies — especially smart meters — that we are collecting more customer information than ever before. The subject of privacy can be complicated and yet is important to our customers. Our employees follow policies and procedures to help ensure they comply with privacy and confidentiality laws. We have taken the opportunity to work with the Information and Privacy Commissioner of Ontario, Canada to examine how *PbD* principles can be integrated into the way we conduct business. SDG&E has been working with Dr. Ann Cavoukian's team to integrate *PbD* into specific company initiatives with positive results thus far, and we look forward to continuing this work together.

PbRD gets organizations to rethink and revive

In 2009 Dr. Ann Cavoukian, the Information and Privacy Commissioner of Ontario in Canada introduced *PbD*, a model to embed privacy into new system implementations.

PbD is based upon seven foundational principles for protecting personal information:

1. Being proactive and preventative
2. Making privacy the default setting in IT systems
3. Embedding privacy into IT system design and architecture
4. Taking a positive-sum rather than a zero-sum approach
5. Embedding privacy from end to end within an IT security system
6. Providing visibility and transparency
7. Respecting user privacy[4]

Since its introduction, several organizations, including the U.S. Federal Trade Commission and the European Commission, have endorsed the *PbD* principles. In 2010, at a meeting of Data Protection and Privacy Commissioners in Jerusalem, participants unanimously adopted the *PbD* Resolution, which pushes regulators globally to adopt *PbD* principles.

However, *PbD*'s focus is on embedding privacy protection from the beginning. For large organizations with existing and legacy systems that are already operational and pervasive throughout the enterprise, embedding privacy from the beginning is not feasible. As a result, in May 2011, Dr. Cavoukian and Dr. Marilyn Prosch, an Associate Professor with the W.P. Carey School of Business, introduced *PbRD*.

In *PbRD*, Dr. Cavoukian and Dr. Prosch extend the original *PbD* principles to include existing and legacy systems.

PbRD principles challenge organizations to:

- **Rethink** existing mitigation strategies, systems and processes with a view to finding new privacy-focused approaches.
- **Redesign** system functionality to achieve better standards of privacy protection, without losing sight of business objectives.
- **Revive** systems through an IT transformation that incorporates privacy protection as a fundamental tenet.[5]

Rethinking, redesigning and reviving legacy systems to improve privacy protection will not only help organizations meet compliance objectives, but also achieve cost savings and improve business performance.

Working with Dr. Cavoukian and Dr. Prosch, Ernst & Young developed a complementary publication, *A path to making privacy count,* that details the implementation of *PbRD* in large-scale IT transformation projects. In the report, we describe the steps organizations need to take to address their evolving risk and compliance needs in an existing IT environment — an environment that often involves a patchwork of legacy systems and rigid technological components. Our discussion addresses the relevant considerations for network, applications and infrastructure layers and provides a five-step process for transforming an organization's IT environment with privacy and security in mind.

Privacy alone is rarely a pivotal motivator of IT transformations. However, when an organization decides to undertake an IT transformation, integrating privacy objectives is critical. In 2012 we expect more organizations to introduce *PbRD* into their IT transformation projects. By effectively managing the risk that privacy issues can pose, organizations can generate additional value and improve performance by safeguarding their reputations and their brands.

Questions to consider

- Is your organization processing personal information in an IT environment that comprises a patchwork of older and newer technologies with varying degrees of effective controls to protect data?
- Will you be able to improve your IT environment's privacy and data protection capabilities by implementing new technologies or will you need to find solutions that work with your organization's existing technology and architecture?
- Has your organization considered implementing *PbRD* as part of its IT transformation?

[4] Cavoukian, Ann, Ph.D., *Privacy by Design*, August 2009/January 2011, http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

[5] Cavoukian, Ann, Ph.D., Prosch, Marilyn, Ph.D., *Privacy by ReDesign: Building a Better Legacy*, May 2011.

Conclusion

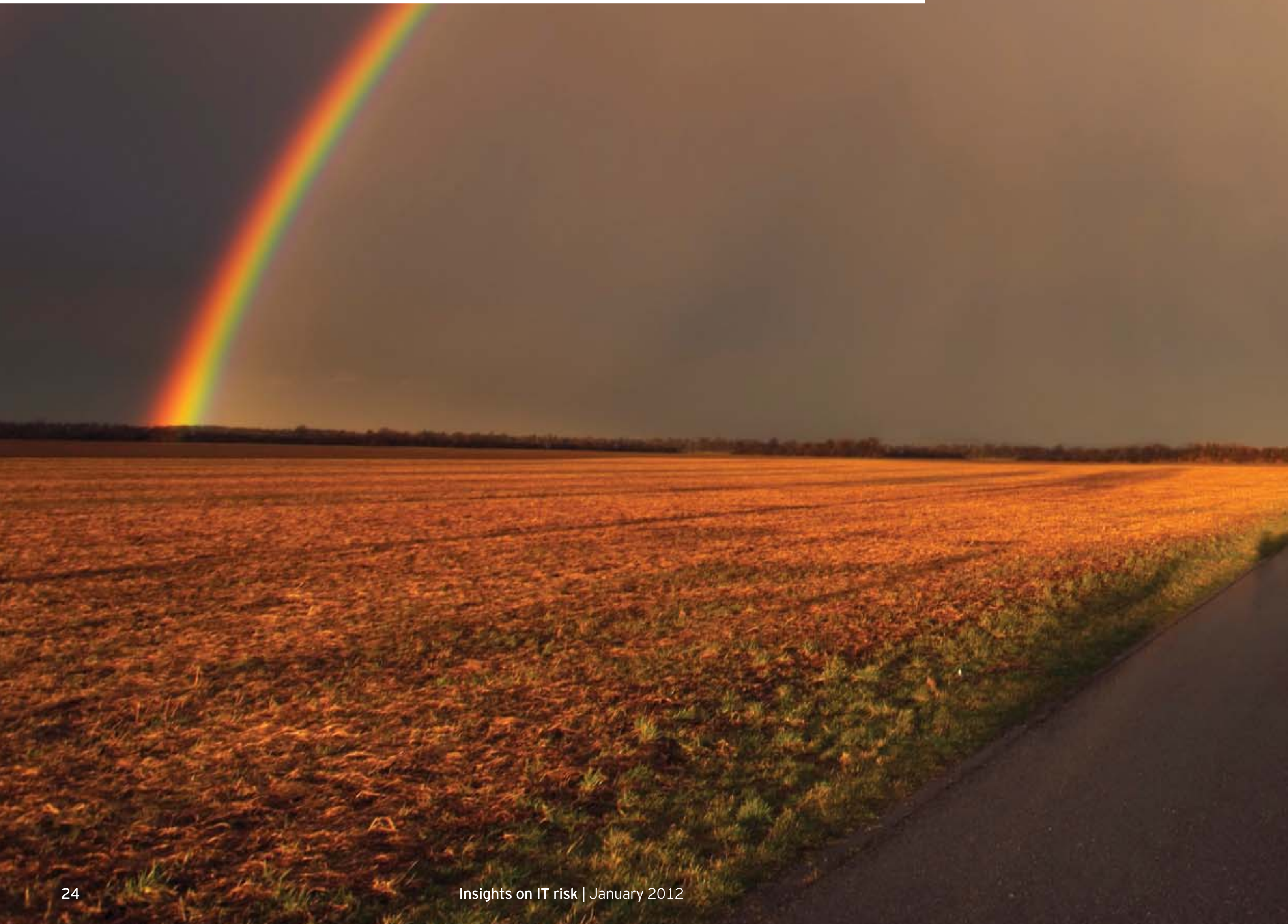
In 2012, the key word is **accountability**. This theme appears in every trend we have identified. It is a fundamental component of handling personal information that organizations need to recognize and address.

As quickly as governments are taking steps to regulate privacy, industry groups are exploring opportunities for self-regulation to limit an increase in government intervention. Ultimately, however, it is the organizations themselves that need to take action.

To achieve greater accountability, many organizations will have to rethink their approach to privacy. From implementing more effective monitoring tools to seeking BCR status or implementing *PbRD* as part of a large-scale IT transformation, accountability can take many forms.

What we do know is that 2012 is not a time for organizations to take a wait-and-see approach to accountability. It may be enticing to set aside privacy in favor of data mining for competitive advantage, or to save money by not undertaking robust privacy management initiatives. But any short-term gains will be overshadowed by the negative and costly consequences a privacy breach will bring.

Like many of those that we interviewed, organizations should be seeking to lead by example, rather than waiting for regulators — or consumers themselves — to mandate accountability.



Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 152,000 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.

Ernst & Young refers to the global organization of member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit www.ey.com.

About Ernst & Young's Advisory Services
The relationship between risk and performance improvement is an increasingly complex and central business challenge, with business performance directly connected to the recognition and effective management of risk. Whether your focus is on business transformation or sustaining achievement, having the right advisors on your side can make all the difference. Our 20,000 advisory professionals form one of the broadest global advisory networks of any professional organization, delivering seasoned multidisciplinary teams that work with our clients to deliver a powerful and superior client experience. We use proven, integrated methodologies to help you achieve your strategic priorities and make improvements that are sustainable for the longer term. We understand that to achieve your potential as an organization you require services that respond to your specific issues, so we bring our broad sector experience and deep subject matter knowledge to bear in a proactive and objective way. Above all, we are committed to measuring the gains and identifying where the strategy is delivering the value your business needs. It's how Ernst & Young makes a difference.

EYG no. AU1064

In line with Ernst & Young's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither EYGM Limited nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor. The opinions of third parties set out in this publication are not necessarily the opinions of the global Ernst & Young organization or its member firms. Moreover, they should be viewed in the context of the time they were expressed.

www.ey.com

How Ernst & Young makes a difference

At Ernst & Young, our services focus on our individual clients' specific business needs and issues because we recognize that each is unique to that business.

IT is a key to allowing modern organizations to compete. It offers the opportunity to become closer to customers and more focused and faster in responses, and can redefine both the effectiveness and efficiency of operations. But as opportunity grows, so does risk. Effective ITRM helps you to improve the competitive advantage of your IT operations, by making these operations more cost efficient and managing down the risks related to running your systems. Our 6,000 IT risk professionals draw on extensive personal experience to give you fresh perspectives and open, objective advice — wherever you are in the world. We work with you to develop an integrated, holistic approach to your IT risk or to deal with a specific risk and information security issue. We understand that to achieve your potential you need tailored services as much as consistent methodologies. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

For more information on how we can make a difference in your organization, contact your local Ernst & Young professional or a member of our team listed below.

Contacts

Global		
Norman Lonergan (Advisory Services Leader, London)	+44 20 7980 0596	norman.lonergan@uk.ey.com
Paul van Kessel (IT Risk and Assurance Services Leader, Amsterdam)	+31 88 40 71271	paul.van.kessel@nl.ey.com
Advisory Services		
Robert Patton (Americas Leader, Atlanta)	+1 404 817 5579	robert.patton@ey.com
Andrew Embury (Europe, Middle East, India and Africa Leader, London)	+44 20 7951 1802	aembury@uk.ey.com
Doug Simpson (Asia-Pacific Leader, Sydney)	+61 2 9248 4923	doug.simpson@au.ey.com
Naoki Matsumura (Japan Leader, Tokyo)	+81 3 3503 1100	matsumura-nk@shinnihon.or.jp
IT Risk and Assurance Services		
Bernie Wedge (Americas Leader, Atlanta)	+1 404 817 5120	bernard.wedge@ey.com
Manuel Giralt Herrero (Europe, Middle East, India and Africa Leader, Madrid)	+34 91 572 7479	manuel.giraltherrero@es.ey.com
Troy Kelly (Asia-Pacific Leader, Hong Kong)	+852 2629 3238	troy.kelly@hk.ey.com
Giovanni Stagno (Japan Leader, Tokyo)	+81 3 3503 1159	stagno-gvnn@shinnihon.or.jp