Can privacy really be protected anymore?

Privacy trends 2016
Can privacy really be protected anymore?

As a concept, privacy, and the need to protect it, has been around for decades. Yet the programs and governance structures in place to turn the concept of privacy protection into reality remain, if not in their infancy, then certainly in their adolescence.

In EY’s Global Information Security Survey (GISS) 2015 privacy questionnaire, 38% of respondents admit that they address security in new business processes and technologies, but not privacy specifically.\(^1\)

However, more telling, and perhaps more concerning for organizations and individuals alike when it comes to managing privacy, is that for nearly half (46%) of survey respondents, their number one or two concern is not having a clear picture of where personal information is stored or processed outside of their main systems and servers.\(^2\) This is exacerbated by the fact that for 40% of respondents, their number one or two concern is that there are simply not enough people to support their privacy program.\(^3\)

In a world where laws and regulations cannot keep pace with digital change, the question many are asking is: can privacy really be protected anymore? As the onus of accountability shifts from regulators to organizations, organizations need to take heed of where they are in terms of their privacy maturity and what they need to do to make privacy protection a part of everything in an organization.

---

1. EY’s Global Information Security Survey 2015 asked approximately 630 privacy professionals for their views on a number of critical privacy issues.
2. Ibid.
3. Ibid.
We see an increasing overlap of four areas that were once viewed as distinctly separate: financial reporting; cybercrime; national security; and the use of personal information.

The merging of some of these areas is not new. Some, such as cybercrime and national security, have had intersecting points for some time now. However, during 2016, we expect these intersections to become more frequent and more pronounced.

As organizations increasingly monitor employees in an effort to track cyber threats, for example, they need to be doing so in a way that balances security with employee privacy. Similarly, the Securities and Exchange Commission in the US is considering requiring organizations to report on cybercrime or cybersecurity risks as part of its financial reporting because of the calamitous financial impact a major cyber breach can have.

In the context of this mashup, organizations need to be mindful of the impact these overlaps have and how they address the associated privacy risks. Specifically, organizations should be thinking about three trends that will improve the level of privacy accountability that all stakeholders, from customers and clients to vendors to governments themselves, expect.

1. Governance
Given the increasing complexity of the cyber world, organizations can no longer rely solely on ad hoc privacy processes to protect personal data. Rather, they need a robust privacy program that demonstrates accountability throughout the privacy life cycle and effectively interacts with other parts of the organization that process personal information.

2. Rigor
Promises are fine, but stakeholders are also demanding proof of accountability, adopting the motto “trust, but verify.” To meet the rigors of verification, auditors acknowledge that they are serving as independent verifiers not only of financial reporting, but also cybersecurity reporting through Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2) because of increasing cybersecurity risks.

3. Trust in service providers
Just as customers are looking to trust organizations to be accountable for their privacy, organizations are looking to trust third-party providers with their data. Following the financial crisis in 2008, the demand for cloud services spiked, primarily as an effective means of cost-cutting – even as organizations worried about the cybersecurity risks. Now, organizations are moving to the cloud because cloud services providers are seen to have more sophisticated cybersecurity programs to prevent advanced attacks than in-house resources can provide. Moving forward, trust in third-party providers will become the critical foundation upon which organizations build their businesses for a digital era.

Looking forward, expect these trends in privacy management to become ever more critical as the lines among financial reporting, cybercrime, national security and use of personal information blur into a single overriding issue for which organizations will be accountable.
The view today

Building on the key trends from 2015

As more aspects of an individual’s life move online, their propensity to share personally identifiable information, whether intentionally or inadvertently, has risen exponentially. The digital age abounds with opportunities to connect and grow and expand in every direction. Yet, as individuals, organizations and governments explore these opportunities, someone has to be responsible for monitoring – and managing – the privacy risks. Given the speed of change, regulators and individuals alike are increasingly looking to organizations to assume this responsibility. And they are demanding proof.

Digital disruption threatens privacy

Digital technology continues to disrupt everything and everyone in every industry around the globe. Social, mobile, big data, cloud, Internet of Things: all of these technology advances are fundamentally altering how companies do business. They are creating massive opportunities for companies to develop new products and services, strengthen relationships with customers and employees, and expand into new territories. Social media enables organizations to interact directly with customers and employees. Mobile is becoming the primary channel for commerce and an indispensable tool for work. Cloud is increasingly being adopted as the go-to data storage option for anywhere anytime access. Big data enables organizations to understand the individual preferences of their customers and tailor their products and services accordingly. And the Internet of Things makes everything smarter: refrigerators that can tell homeowners when their milk is going bad; thermostats that can automatically adjust based on peak loads and rates; and smoke detectors can let you know if there’s a problem when you’re not at home. Yet for all the opportunities digital technologies present, they also come with an abundance of new and unforeseen risks – and complexity when it comes to dealing with personal information. Who, for example, is monitoring – and protecting – all of the data associated with these “smart” technologies? Likewise, as individuals and organizations entrust their data to third-party cloud providers, how can they make sure providers are worthy of that trust? And what about all that big data that organizations are collecting to personalize customer experiences, improve products and generally learn more about their target audiences? Who’s making sure that all that personally identifiable data is both safe and scrubbed of anything that may jeopardize an individual’s privacy? The answers to some of these questions, according to EY’s GISS 2015, are less than satisfying. In this year’s GISS survey, 54% of privacy questionnaire respondents say that their organization have no formalized requirements for using big data while addressing its privacy obligations. Similarly, although 46% of respondents plan to increase their use of social media in the coming year, 37% have no formalized requirements to address privacy concerns related to social media. As for minimizing personal identification of data, 61% of respondents say that they either have no mandate to minimize or de-identify personal information, or they only do it in unique circumstances.

Innovation, convenience, customer satisfaction, profitable growth are all important, but they cannot come at the expense of personal privacy. Increasingly, organizations are compelled to determine not only what information they collect, but how they collect it, store it, use it, maintain it, and protect it. Current privacy regulatory regimes may not be enough to address privacy issues in digital ecosystems where data flows across regions and continents, and where different players are subject to different laws and users can access the services anywhere. As such, regulators and individuals are looking to organizations to assume the mantle.

Message from regulators to organizations: take responsibility

In 2010 at the 32nd International Conference of Data Protection and Privacy Commission in Jerusalem, Privacy by Design (PbD) gained international recognition with the signing of the Privacy by Design Resolution. Five years later, PbD, which advocates that all new business processes and technologies be created with privacy already embedded into them, has become the international privacy standard that has been translated into multiple languages. Further, both the United Nations, the European Parliament and the US government have indicated that PbD is absolutely critical in maintaining personal privacy. Yet, despite its international reputation as the leading privacy standard, only 18% of the 630 GISS privacy questionnaire respondents use PbD as part of how they create new processes and technologies. Another 24% plan on including PbD in the near future. However, a full 38% don’t specifically address privacy at all.

For organizations all over the world, this laissez-faire approach to managing privacy has to change, particularly as regulators mandate that organizations do so. In the EU, data protection reform produced MEmO/13/923 and MEmO/14/60, which specifically address privacy at all stages of development, and that privacy-friendly default settings should be the norm – for example, on social networks.4 European Commission4 EU’s Global Information Security Survey 2015 privacy questionnaire.

European Commission. “ ‘Privacy by Design’ and ‘Privacy by Default,’ will become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example, on social networks.”

Continued

1. Internet of Everything. The Internet of Everything looks at the Internet of Things as a whole. This includes factory sensors, global positioning systems, wearable devices (Google Glass, Fitbit, etc.), and “smart” technology that tells you when it’s time to order food or when it’s time for a medical checkup. Right now, there is a huge market out there to build cheap sensors to connect ordinary things to the internet, and to add content and capacity into traditional telecommunications type networks to enable that connection.

2. Internet of Everyone. This is where privacy as a notion of the authorized processing of personalized identifiable information according to fair legal and moral principles lies. In the process of the Internet of Everything gathering and transferring information, the Internet of Everyone has to have a say. If the Internet of Everything and the data associated with it offers a quantitative distinction, the Internet of Everyone identifies a qualitative difference. We need to be designing the Internet of Things so that everyone can feel as if they have the right level of control and management over their data.

3. Internet of Ethics. The Internet of Ethics challenges us to ask what our ethics are in a world of devices that do not recognize our cultural barriers. Around the world, cultural norming varies vastly from household to household. We need to have a really robust, cross-cultural and cross-generational discussion around the Internet of Ethics that considers all kinds of different perspectives, as well as the quantitative and qualitative differences when we think about exponential data flow.

4. Internet of Experience. People like the experiences of being able to communicate on our smartphones and tablets. However, the Internet of Experience isn’t only about what the technology can do for us, but also what experience we want to have, and who gets to control these experiences. As well, we need to consider whether all of these billions of micro-experiences need to be recorded, tracked and saved. We need to do a better job of documenting what’s important and deleting the rest.

For the most part, we tend to see the Internet of Things as technology that gathers data for the purposes of making our lives easier or more enlightened. But the missing ingredient within all of this qualitative data is the human element – the qualitative differences that explain what the data can’t. Ultimately, in the age of the Internet, the age of the Internet of Things, the most important thing we need to remember is to be human.

4 European Commission. “ ‘Privacy by Design’ and ‘Privacy by Default,’ will become essential principles in EU data protection rules – this means that data protection safeguards should be built into products and services from the earliest stage of development, and that privacy-friendly default settings should be the norm – for example, on social networks.”

Approximately 60 companies have certified, with Mexico joining in 2013, Japan in 2014 and Canada in 2015. These certifications push more responsibility from regulators to companies themselves, requiring companies to have relatively mature privacy programs in place, from having a privacy officer, to training, to maintaining the program.

To date, more than 5,000 entities globally have certified under the US-EU Safe Harbor Framework. However, on 6 October 2015, the European Court of Justice (ECJ) declared the US Safe Harbor agreement to be invalid because it does not protect data transferred from the EU to the US against access by US intelligence agencies. Although we have yet to understand the full impact, we do know that Safe Harbor will have to change. EU and US authorities are working on a Safe Harbor 2.0 framework to meet a January 2016 deadline imposed by the ECJ. However, it remains a work in progress. In the meantime, Safe Harbor cannot be relied on as a certified framework for transferring data from the EU to the US in compliance with EU data protection laws. Organizations using the Safe Harbor framework will need to review their data protection policies, contracts, and terms and conditions as a result of this ruling. They will also want to consider other mechanisms, such as BCR, to meet EU requirements.

Proof of privacy programs emphasizes accountability

BCR in EU and CBPR in Asia-Pacific come of age, while Safe Harbor in the US faces a setback

In today’s global and increasingly digital economy, processing and transferring personal information across borders is a fundamental part of an organization’s daily activities. That’s why standard-setters in the US, EU and Asia-Pacific regions, established frameworks and guidelines that set the tone for cross-border privacy protection. There are three recognized programs for transferring personal data: the US-EU Safe Harbor Framework, Binding Corporate Rules (BCR) and the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules (CBPR).

To date, more than 5,000 entities globally have certified under the US-EU Safe Harbor Framework. However, on 6 October 2015, the European Court of Justice (ECJ) declared the US Safe Harbor agreement to be invalid because it does not protect data transferred from the EU to the US against access by US intelligence agencies. Although we have yet to understand the full impact, we do know that Safe Harbor will have to change. EU and US authorities are working on a Safe Harbor 2.0 framework to meet a January 2016 deadline imposed by the ECJ. However, it remains a work in progress. In the meantime, Safe Harbor cannot be relied on as a certified framework for transferring data from the EU to the US in compliance with EU data protection laws. Organizations using the Safe Harbor framework will need to review their data protection policies, contracts, and terms and conditions as a result of this ruling. They will also want to consider other mechanisms, such as BCR, to meet EU requirements.

Approximately 60 companies have successfully applied for approval of their BCRs – 20 more companies than the number approved when we reported on BCR in 2013. Approved by APEC in 2011, CBPR has gained traction beyond the Asia-Pacific, with Mexico joining in 2013, Japan in 2014 and Canada in 2015. These certifications push more responsibility from regulators to companies themselves, requiring companies to have relatively mature privacy programs in place, from having a privacy officer, to training, to maintaining the program.

Until the October 2015 ruling, there was every indication that all three programs were reaching or had already reached a tipping point. Yet, despite their importance, 43% of respondents who plan on transferring personal information out of the EU, only 10% are in the process of or have already obtained BCR approval. Similarly, of the 43% of respondents intending to transfer personal information out of regulated APEC countries, only 6% are in the process of or have already obtained CBPR approval.

As accountability for privacy protection continues to shift to corporations, companies who are on the fence about implementing a certifiable privacy framework will need to make a move sooner rather than later. 6

The conundrum of privacy in the connected car

In the automotive industry, the notion of the connected car is not new. The emergency “e-call” feature in BMW cars has been available since 1999. What is new is the level of connectedness in vehicles as digital technology revolutionizes the driving experience. This is a challenge for the automotive industry because the development cycle of a vehicle is seven or eight years, whereas the development cycle for technology can be as short as seven to 14 days.

BMW has a Privacy by Design (PhD) policy that we maintain and enhance. We also spend time training the appropriate resources within the business to adhere to the principles outlined in the policy. Part of that policy states that at a very early stage, our privacy professionals need to be involved in the development of new features and apps. More importantly, we have defined methods for privacy that consider and synchronize the traditional long-term development cycle of classic car production with the extremely short-term IT development life cycle.

We have also achieved BCR certification to establish and maintain consistent and adequately protective data privacy policies across all of our legal entities around the world. We believe that PhD and BCR offer robust frameworks for establishing privacy programs. However, today’s and tomorrow’s connected cars offer automated driving features. The questions automotive companies are asking are: who should be controlling these features and who should control the data? The e-call feature is a good example, if the driver has the option to deactivate the feature, but the next driver doesn’t reengage it, experiences an accident and no one comes to the rescue, who is responsible? One person’s choice is impacting another’s driving experience. Similarly, there is the issue of who controls the data that a vehicle collects. Does the driver or owner of the vehicle control it? Or does the original equipment manufacturer (OEM)? The connected car creates conflicts between consumer choice and the OEM. Much like the health care industry, consumers and OMEs alike may look to regulators to resolve these conflicts.

Ultimately, privacy may become a feature that influences a consumer’s car-buying decision so it’s important that automotive manufacturers get it right early. Privacy professionals add that level of value.

EY’s GISS privacy questionnaire asked 630 respondents “when it comes to adopting BCR as a means of legitimizing those transfers out of the EU, which of the following statements best describes your organization?” (Select one)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We don’t transfer personal information out of the EU countries</td>
<td>57%</td>
</tr>
<tr>
<td>Undecided as to whether to take it or not</td>
<td>17%</td>
</tr>
<tr>
<td>We are in the process of, or have already obtained, BCR approval</td>
<td>10%</td>
</tr>
<tr>
<td>BCR is not a path we intend to take</td>
<td>9%</td>
</tr>
<tr>
<td>It is very likely that we will apply for BCR but don’t know when</td>
<td>7%</td>
</tr>
<tr>
<td>Numbers may not sum due to rounding</td>
<td></td>
</tr>
</tbody>
</table>

“Companies should build-in privacy protections at every stage as they develop their products and services... Privacy protections are most effective when they are part of a company’s fundamental business model and not overlooked or added later as an afterthought.”

Jessica Rich, Director, Bureau of Consumer Protection

More countries adopting breach notification regulations

Despite the financial, operational and reputational damage a privacy breach can cause, breach notification remains a tactical rather than a strategic imperative. Executives continue to be more interested in compliance than understanding the risks that precipitated the breach.

As we have stated in previous Privacy trends reports, this leaves individuals increasingly vulnerable to both aggressive organizations seeking to create competitive advantage, or nefarious actors looking to profit from unauthorized access to personally identifiable information.

In the US, in the absence of federal regulatory action to produce standardized breach notification requirements, the states are going it alone. In 2015, at least 32 states introduced or are considering security breach notification bills or resolutions. Many of these bills would amend existing data breach laws to require:

- Companies to report breaches to state attorneys general or other central state agency and expand the definition of “personal information” to include medical, insurance or biometric data (fingerprints)
- Businesses and governments to implement security plans or security measures
- Educational institutions to notify parents or government entities if a breach occurs.

This patchwork of data breach laws across 47 states makes it hard for organizations to implement consistent breach notification programs that address every state’s compliance requirements. Moreover, there is no single standard reporting mechanism.

In June 2015, Canada’s mandatory federal security breach notification law received royal assent. Organizations are now required to notify the Privacy Commissioner and affected individuals of any security breach involving personal information the organization experiences if there is a reasonable expectation that the breach will create a real risk of significant harm to an individual.

Most recently, in December 2015, the EU issued a Network and Information Security Directive (NIS Directive), the first EU-wide legislation for cybersecurity. In addition to improving cybersecurity capabilities in EU Member States and enhancing member state cooperation on cybersecurity, it requires “operators of essential services in the energy, transport, banking and healthcare sectors, and providers of key digital services like search engines and cloud computing, to take appropriate security measures and report incidents to national authorities.”

As we have stated in previous Privacy trends reports, this leaves individuals increasingly vulnerable to both aggressive organizations seeking to create competitive advantage, or nefarious actors looking to profit from unauthorized access to personally identifiable information.

EY’s GISS privacy questionnaire asked 630 respondents “when it comes to adopting CBPR as a means of legitimizing transfers out of regulated APEC countries, which of the following statements best describes your organization?” (Select one)

<table>
<thead>
<tr>
<th>Statement</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>We don’t transfer personal information out of regulated APEC countries</td>
<td>58%</td>
</tr>
<tr>
<td>Undecided as to whether to take it or not</td>
<td>21%</td>
</tr>
<tr>
<td>CBPR is not a path we intend to take</td>
<td>8%</td>
</tr>
<tr>
<td>It is very likely that we will apply for CBPR but don’t know when</td>
<td>7%</td>
</tr>
<tr>
<td>We are in the process of, or already obtained, CBPR approval</td>
<td>6%</td>
</tr>
<tr>
<td>Numbers may not sum due to rounding</td>
<td></td>
</tr>
</tbody>
</table>


A strong foundation for privacy accountability makes compliance easier

At Corning Incorporated (Corning), we take the protection of personal data seriously, particularly when it is being transferred across borders among the Corning group of companies.

Four and a half years ago, Corning implemented policies that would enable us to adhere to the principles associated with US-EU and US-Swiss Safe Harbor Frameworks. These certify that we comply with appropriate standards for privacy protection when transferring data between Corning’s US and EU entities. When we started working on complying with Safe Harbor, we made a conscious effort to address as many BCR requirements as possible. We have since gone on to receive BCR certification, making it possible to transfer personal data between Corning entities throughout the world. Formally adopting the BCR requirements was easier mainly because we already had many of the basic principles in place — a data privacy office, a corporate privacy policy, privacy impact assessments that identified current practices and any gaps, and an inventory system for third parties.

Furthermore, we had embedded privacy into our culture. The principles that certify us under BCR and Safe Harbor are the same principles we apply globally when it comes to protecting personal information.

BCR, Safe Harbor and other certifications serve as motivational compliance tools for organizations to be accountable for the personal information in their care. We found at Corning that compliance is much easier if organizations implement a strong privacy foundation and accountability mindset from the outset.


Can privacy really be protected anymore? — Privacy trends 2016
Can privacy really be protected anymore?

— Privacy trends 2016

How can companies improve their accountability and become trend leaders?

There are eight actions companies can take to help improve their accountability and become trend leaders.

1. Develop KPIs for privacy
2. Build privacy impact assessments into the system development life cycle
3. Prepare a robust incident response plan – and prepare to respond
4. Monitor for insider threats
5. Know the assurance options
6. Implement identity and access management for privacy
7. Consider right-on-time notice of privacy policy
8. Get consensus on an approach to de-identification

Actions to help improve accountability in 2016

The pace at which new and emerging technologies are penetrating and disrupting every aspect of our lives is far outstripping the pace at which lawmakers can keep up. As a result, regulators – and consumers – are looking to companies to assume accountability for privacy.

For privacy accountability to be successful, leadership and management need to be aligned in terms of both priorities and culture when it comes to managing privacy.

Organizational leaders need to understand that it’s no longer enough to know what they are tracking. They have to know why they are tracking it and which KPIs will enable them to develop a robust privacy program that zeros in on accountability, within and outside the organization.

Companies will want to consider adopting KPIs for privacy in the same way they do for any other performance-based program. These KPIs can be tied to the company’s existing GRC program. In a recent survey conducted by the International Association of Privacy Professionals (IAPP) and sponsored by EY, IAPP-EY Annual Privacy Governance Report 2015, 31% of respondents indicate that they plan to increase their use of GRC tools in the coming year, with more than half ranking data protection controls as their most used GRC tool. Automating KPIs helps enable companies to gather and analyze accurate privacy data that they can then use to develop, implement, monitor and maintain robust privacy programs that help increase compliance with regulations, and meets increasing consumer demands.

<table>
<thead>
<tr>
<th>KPI</th>
<th>Top priority for management</th>
<th>Top priority for executive leadership</th>
</tr>
</thead>
<tbody>
<tr>
<td>Progress in addressing compliance obligations</td>
<td>42%</td>
<td>41%</td>
</tr>
<tr>
<td>Number and impact of breaches and incidents</td>
<td>42%</td>
<td>32%</td>
</tr>
<tr>
<td>Progress in addressing privacy risks</td>
<td>42%</td>
<td>32%</td>
</tr>
<tr>
<td>Closing known gaps</td>
<td>32%</td>
<td>23%</td>
</tr>
<tr>
<td>Complete and maintain inventory of personal information</td>
<td>31%</td>
<td>12%</td>
</tr>
<tr>
<td>Complaints received</td>
<td>22%</td>
<td>22%</td>
</tr>
<tr>
<td>Degree of collaboration with the business</td>
<td>14%</td>
<td>23%</td>
</tr>
</tbody>
</table>

Moving forward

1 Build privacy impact assessments into the system development life cycle

Privacy impact assessments (PIAs) analyze how personally identifiable information is collected, used, shared, and maintained. It aids organizations in identifying and mitigating privacy risks within projects and across the entire enterprises. PIAs are not new. But where they were once optional, today they are leading practice. In the recent IAPP-EY survey, 59% of privacy professionals indicate that they use PIAs, with approximately 50% saying that they are part of their organizations system development life cycle process.11

One of the PIA leaders is the UK. It was the first country in Europe to develop and disseminate a privacy impact assessment methodology. In 2012, the EC’s Data Protection Regulation introduced made PIAs mandatory for both public and private sector organizations throughout Europe.

We see 2016 as the year that organizations build PIAs into their development life cycle so that they are conducted consistently for every project, every time.

2 Prepare a robust incident response plan – and prepare to respond

In EY’s GISS only 7% of 1,755 respondents to the cybersecurity questionnaire claim to have incident response programs for cyber attacks. These include third parties and law enforcement and are integrated with their broader threat and vulnerability management function – a percentage that remains unchanged from last year.

The next question becomes, of the 7% that have incident response programs in place for cyber attacks, how many have incorporated responses to privacy breaches as part of their program?

In April 2015 in the US, the cybersecurity unit of the Department of Justice released new guidance on leading practices for responding to data breaches. The guidance is divided into four sections that address what steps to take before a cyber attack, how to respond when a cyber attack occurs, what not to do following a cyber incident and what to do in the aftermath,12

First and foremost, the guidance recommends that before a breach occurs, organizations should conduct risk assessments to identify and prioritize critical assets, data and services. From a privacy perspective these risk assessments should particularly focus on identifying and flagging any personally identifiable information. The guidance goes on to suggest that organizations develop a robust incident response plan that outlines the concrete steps they need to take in the event of a cyber breach.13

Governments in Canada, the EU and the UK all have similar advice regarding incident response. Yet, for global organizations, a country-by-country response is a poor option. Instead, multinational organizations may want to consider developing a robust, consistent, unified and clearly articulated approach to addressing incidents related to privacy breaches before they occur.

Given that more than a third of EY’s GISS cybersecurity respondents say that it is unlikely that they would be able to detect a sophisticated attack, there’s a good chance that one or more readers of this report is currently experiencing a breach and doesn’t even know it yet.

3 Monitor for insider threats

In EY’s GISS 2015, when we asked the cybersecurity respondents what they consider to be the most likely source of a cyber attack, 56% indicated their employees, a 12 percentage point increase from last year, and second only to criminal syndicates.14

When asked whether they monitor their employees’ use of data, 42% indicate they have formalized requirements for monitoring employees while balancing their privacy obligations. That said, a majority of respondents admit that protecting proprietary information is more important than protecting employee privacy.

Although a healthy minority monitor their employees’ use of data, few organizations assess their employees’ adherence to data protection requirements through their performance evaluation process. Instead, organizations rely on more traditional, administrative mechanisms, such as computer-based education, emails, posters and agreements. Many of these mechanisms focus on communicating expectations rather than emphasizing deterrence.

Understandably, organizations want to use monitoring tools to keep an eye on their data. However, these tools can also end up monitoring an employee’s personal information. This is particularly evident in the case of bringing your own device (BYOD), which is now ubiquitous across organizations.

4 Proposed breach notification law eases customer anxieties

In early December 2015, the Australian government proposed a new law that will require organizations operating in Australia to disclose serious breaches of people’s information within 30 days if the breach has a potential to cause serious harm. The concept of mandatory data breach notification has been around for a long time. In fact, the previous government introduced similar legislation, but it was not put to parliament for a vote.

Broadly speaking, Telstra is supportive of a mandatory breach notification law because we believe customers expect that they should be notified if there is a significant breach that can cause them harm. We haven’t seen the final details of the legislation. However, we believe that organizations should be doing everything they can to notify, remediate and manage to the best of their ability any such lapses. Certainly, this is what Telstra does.

However, we need to make sure that laws such as these do not produce notification fatigue. A lack of harmonization in breach notification laws around the world means organizations need to understand the different laws in different jurisdictions. Does a breach require telling the regulator before the consumer? When contacting the consumer, which form must the notification take — verbal, written? And then there’s the additional requirement of notification based on the size of the breach. We’re conscious of over notifying customers and creating levels of anxiety for breaches that will have no material impact. That said, we are fully in favor of legislative instruments for instances where serious harm can occur.

In recognition of the anxiety customers feel around breach notification, the Australian Privacy Commissioner has released guidance on what he expects should happen if there is a data breach, but at the moment, without a law, it’s entirely voluntary.

Telstra already has a framework in place that ensures we not only meet our legal obligations, but also our customers’ expectations on privacy and data protection. As a large organization, we have large numbers of resources invested in compliance and management of regulatory requirements. We will be well-positioned to meet any compliance obligations the new breach notification law imposes.

The same cannot be said for smaller organizations with fewer resources, less experience, and no back office IT systems to support the requirements of the new law. For them, this new law will likely pose significant challenges — ones worth resolving to keep customers informed and to remediate and mitigate the impact today’s data breaches can cause.

13 Ibid.
With a market capitalization of $124b, revenues of approximately $50b, and more than 400 diverse brands globally, Unilever is a large organization with unique challenges in terms of data privacy. When we embarked on a cross-enterprise, cross-geography privacy program in 2013, we were interested not only in developing and implementing a robust global privacy program, but also in monitoring and measuring its success.

When we officially launched our privacy program, we broke it down into four or five main components:

1. **Partitioning.** This would help to alleviate at least some of the privacy issues associated with dual-use devices (laptops, tablets, and smartphones). Partitioning would provide the device with two different desktops—one for work and one for personal—located on two separate components of the device’s hard drive.

2. **Guest network.** A guest network separate from the main network allows employees to use their personal device to gain access to the web directly, perhaps even through a work-only email account.

3. **sandboxes.** Using third-party services or an organization’s own coding to create “sandboxes” enables organizations to separate company data and company-issued applications from any interaction with personal data, applications, or online services. As the workforce becomes increasingly mobile and technologies continue to evolve, finding the right balance between personal privacy and corporate security is more important than ever.

4. **Privacy.** Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA. The principles of security, availability, and processing integrity are used to evaluate whether a system is reliable. The SOC 2 reports play a different role in giving consumers, commercial customers, shareholders, and the market at large the confidence that an organization is meeting a comprehensive standard when protecting their data.

5. **Implement identity and access management for privacy.** Identity and access management for privacy differs from traditional identity and access management programs because it’s about privacy, not security. Organizations can control access by modifying, or de-identifying the data. Identity and access management for privacy focuses on determining what level of detail a user needs, which is determined, in part, on role, identity and access management for privacy needs to be customized, not by role, but by customizing data elements with privacy in mind.

Organizations can be smarter about how they handle privacy by providing users with the least-specific data based on a user’s need. For example, a company provides reports to 1,000 users over the course of a year. Currently, every one of those 1,000 people gets access to the complete set of data. However, not everyone needs complete access. Identity and access management for privacy helps companies to evolve their privacy programs so that only 100 of the 1,000 get a complete set of data. The rest of the people get a subset of the data based on their need.

The benefits of this approach as organizations move to implement it in the coming year are twofold: fewer vulnerabilities related to insider threats; and greater rigor for organizational accountability.

---

5. **Know the assurance options.** Service providers are often asked to obtain an independent assessment of their privacy and data security practices. Previously, organizations used the Statement on Auditing Standard No. 70 reports. However, these reports are not intended to address privacy or security. In 2011, AICPA issued a new framework—Reports on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and Privacy (SOC 2). SOC 2 reports provide independent assurance on a wider range of service provisions than simply financial reporting. They enable service providers to be transparent and accountable to their clients. Additionally, organizations that outsource can use the SOC 2 reports to be accountable to their shareholders and other stakeholders.

SOC 2 reports enable service providers to be transparent and accountable to their clients. Further, organizations that outsource can use the SOC 2 reports to be accountable to their shareholders and other stakeholders.

6. **Implement identity and access management for privacy.** Identity and access management for privacy differs from traditional identity and access management programs because it’s about privacy, not security. Organizations can control access by modifying, or de-identifying the data. Identity and access management for privacy focuses on determining what level of detail a user needs, which is determined, in part, on role, identity and access management for privacy needs to be customized, not by role, but by customizing data elements with privacy in mind.

Organizations can be smarter about how they handle privacy by providing users with the least-specific data based on a user’s need. For example, a company provides reports to 1,000 users over the course of a year. Currently, every one of those 1,000 people gets access to the complete set of data. However, not everyone needs complete access. Identity and access management for privacy helps companies to evolve their privacy programs so that only 100 of the 1,000 get a complete set of data. The rest of the people get a subset of the data based on their need.

The benefits of this approach as organizations move to implement it in the coming year are twofold: fewer vulnerabilities related to insider threats; and greater rigor for organizational accountability.

---

### Monitoring program effectiveness through KPIs

With a market capitalization of $124b, revenues of approximately $50b, and more than 400 diverse brands globally, Unilever is a large organization with unique challenges in terms of data privacy. When we embarked on a cross-enterprise, cross-geography privacy program in 2013, we were interested not only in developing and implementing a robust global privacy program, but also in monitoring and measuring its success.

When we officially launched our privacy program, we broke it down into four or five main components:

1. **Partitioning.** This would help to alleviate at least some of the privacy issues associated with dual-use devices (laptops, tablets, and smartphones). Partitioning would provide the device with two different desktops—one for work and one for personal—located on two separate components of the device’s hard drive.

2. **Guest network.** A guest network separate from the main network allows employees to use their personal device to gain access to the web directly, perhaps even through a work-only email account.

3. **sandboxes.** Using third-party services or an organization’s own coding to create “sandboxes” enables organizations to separate company data and company-issued applications from any interaction with personal data, applications, or online services. As the workforce becomes increasingly mobile and technologies continue to evolve, finding the right balance between personal privacy and corporate security is more important than ever.

4. **Privacy.** Personal information is collected, used, retained, disclosed, and destroyed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA and CICA. The principles of security, availability, and processing integrity are used to evaluate whether a system is reliable. The SOC 2 reports play a different role in giving consumers, commercial customers, shareholders, and the market at large the confidence that an organization is meeting a comprehensive standard when protecting their data.

---

### Can privacy really be protected anymore? — Privacy trends 2016

- **37%** of GISS cybersecurity respondents have no formalized requirements to address privacy concerns related to social media.

- **61%** of GISS privacy questionnaire respondents say that they either have no mandate to minimize or de-identify personal information, or they only do it in unique circumstances.

---

However, that has not stopped regulators from trying. In the US, the Health Insurance Portability and Accountability Act (HIPAA) defines protected health information as identifiable data that “identifies the individual or for which there is a reasonable basis to believe [that the information] can be used to identify an individual.” 37

The FTC doesn’t provide a definition per se. Instead, it offers advice to help organizations assess whether data is identifiable. However, there is currently no leading practice.

In Europe, the General Data Protection Regulation promotes techniques such as anonymization (removing personally identifiable information where it is not needed), pseudonymization (replacing personally identifiable material with artificial identifiers), and encryption (encoding messages so only those authorized can read it) to protect personal data.

Two organizations have taken additional steps to help de-mystify de-identification:

- **Future of Privacy Forum (FPF)** has developed a framework for de-identification.
  1. Future of Privacy Forum (FPF) has developed a framework for de-identification.
  2. National Institute of Standards and Technology (NIST) has published the De-Identification of Personally Identifiable Information to provide an overview of the different approaches and gaps associated with common de-identification techniques.

Despite these noble efforts, before organizations can move forward in developing and implementing a de-identification plan, the global community needs to agree on a common approach to de-identification.

In a recent draft report, FPF makes the argument that rather than focusing on what constitutes personal data and therefore which data should be de-identified, we should consider reorienting legal rules for data based on “multiple categories of identifiability, while keeping the option open to assess other factors such as the data’s sensitivity, accessibility and permanence to modify additional legal requirements.” 18

This approach allows that rather than a black and white approach to data, organizations and policymakers should “view data in various shades of gray.” 19

In 2016, we expect to see progress by the global community in finding consensus in terms of what constitutes de-identification, and a framework to help organizations develop a plan to achieve it.

The human side of data

In 2012, Colombia’s congress issued new statutory law related to a new data protection law. Part of these regulations requires that the data controller within an organization must be in charge of the company’s data protection compliance program. As the Chief Information Security Officer for my organization, that operational responsibility was delegated to me and my team. I now serve as the Chief Information Security and Privacy Officer.

Combining these two roles provides a unique perspective for me to look at the issue of data protection from both a security and a privacy standpoint. My team and I need to know what information needs to be protected, where it needs to be protected and how it needs to be protected. It’s not good enough to protect the information itself. It also requires a better understanding of where the privacy issues are within the various functions of the organization, and to identify and implement policies and procedures to mitigate the associated risks.

When we talk about protecting information, we are, of course, talking about customer data and employee data and how to protect both. How to protect the privacy of our employees. But also, how to ensure that our employees respect and protect our customers’ privacy too.

One of the biggest advantages I see to having dual responsibility for information security and privacy is our visibility and ability to trace the flow of information across the enterprise from start to finish so that we can ensure that the data is protected at every touch point. When I only held the role of Chief Information Security Officer, my primary focus was securing the data. As both Chief Information Security Officer and Chief Privacy Officer, my focus is now on the people as well as data security. This is a significant shift that enables us to look at more than the compliance implications – it enables us to look at the human implications.

---

19 Ibid.
The need for maturity in privacy accountability

If the evolution of privacy protection is still in the adolescent phase, then it needs to grow up – fast. The digital future is upon us and it won’t wait for governments to craft laws that address the myriad privacy risks it creates.

Organizations are increasingly being held to account for the reams upon reams of personally identifiable data they collect. Yet, alarmingly large numbers of organizations still have no idea where this data lives within their systems, let alone how to protect it.

Organizations need to be taking clear and decisive action to develop and enhance privacy management beyond ad hoc policies and toward fully accountable, certified and trusted privacy programs. Knowing how information is collected, used, shared and maintained, developing KPIs, finding the balance between monitoring for insider threats and employee privacy, controlling access by modifying and de-identifying data, preparing for the worst and providing independent assurance on privacy programs are all signs of an evolving maturity that governments and individuals alike are demanding.

For years, we’ve been talking about the need for accountability in privacy management. We expect 2016 may be the year when privacy programs mature from adolescence to adulthood.
Can privacy really be protected anymore?

— Privacy trends 2016

Insights on governance, risk and compliance is an ongoing series of thought leadership reports focused on IT and other business risks and the many related challenges and opportunities. These timely and topical publications are designed to help you understand the issues and provide you with valuable insights about our perspective.

Please visit our insights on governance, risk and compliance series at: www.ey.com/GRCinsights.

Want to learn more?

Unlocking the value of your program investments: How predictive analytics can help in achieving successful outcomes

www.ey.com/PRM

Enhancing your security operations with Active Defense

www.ey.com/activedefense


www.ey.com/GISS2015

Using cyber analytics to help you get on top of cybercrime: Third-generation Security Operations Centers

www.ey.com/3SOC

There’s no reward without risk: EY’s global governance, risk and compliance survey 2015

www.ey.com/GRCsurvey2015

Reducing risk with Cyber Threat Intelligence

www.ey.com/CTI

Cybersecurity and the Internet of Things

www.ey.com/IOT

Cyber program management: identifying ways to get ahead of cybercrime

www.ey.com/CPM

Unlocking the value of your program investments: How predictive analytics can help in achieving successful outcomes

www.ey.com/PRM

Achieving resilience in the cyber ecosystem

www.ey.com/cyberecosystem

If you were under cyber attack, would you ever know?

As many organizations have learned, sometimes the hard way, cyber attacks are no longer a matter of if, but when. Hackers are increasingly relentless. When one tactic fails, they will try another until they breach an organization’s defenses. At the same time, technology is increasing an organization's vulnerability to attack through increased online presence, broader use of social media, mass adoption of mobile devices, increased usage of cloud services, and the collection and analysis of big data. Our ecosystems of digitally connected entities, people and data increase the likelihood of exposure to cybercrime in both the work and home environment. Even traditionally closed operational technology systems are now being given IP addresses, enabling cyber threats to make their way out of back-office systems and into critical infrastructures such as power generation and transportation systems.

Anticipating cyber attacks is the only way to be ahead of cyber criminals. With our focus on you, we ask better questions about your operations, priorities and vulnerabilities. We then collaborate with you to create innovative answers that help you activate, adapt and anticipate cybercrime. Together, we help you design better outcomes and realize long-lasting results, from strategy to execution.

We believe that when organizations manage cybersecurity better, the world works better.

So, if you were under cyber attack, would you ever know? Ask EY.
About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the 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 ey.com.

© 2016 EYGM Limited.
All Rights Reserved.
EYG no. AU3733
ED None

About EY's Advisory Services

In a world of unprecedented change, EY Advisory believes a better working world means helping clients solve big, complex industry issues and capitalize on opportunities to grow, optimize and protect their businesses.

Through a collaborative, industry-focused approach, EY Advisory combines a wealth of consulting capabilities – strategy, customer, finance, IT, supply chain, people advisory, program management and risk – with a complete understanding of a client’s most complex issues and opportunities, such as digital disruption, innovation, analytics, cybersecurity, risk and transformation. EY Advisory’s high-performance teams also draw on the breadth of EY’s Assurance, Tax and Transaction Advisory service professionals, as well as the organization's industry centers of excellence, to help clients realize sustainable results.

True to EY’s 150-year heritage in finance and risk, EY Advisory thinks about risk management when working on performance improvement, and performance improvement is top of mind when providing risk management services. EY Advisory also infuses analytics, cybersecurity and digital perspectives into every service offering.

EY Advisory’s global connectivity, diversity and collaborative culture inspires its consultants to ask better questions. EY consultants develop trusted relationships with clients across the C-suite, functions and business unit leadership levels, from Fortune 100 multinationals to leading disruptive innovators. Together, EY works with clients to create innovative answers that help their businesses work better.

The better the question. The better the answer. The better the world works.

Our Risk Advisory Leaders are:

<table>
<thead>
<tr>
<th>Global Risk Leader</th>
<th>+31 88 40 71271</th>
<th><a href="mailto:paul.van.kessel@nl.ey.com">paul.van.kessel@nl.ey.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Risk Leaders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Americas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Amy Brachio</td>
<td>+1 612 371 8537</td>
<td><a href="mailto:amy.brachio@ey.com">amy.brachio@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jonathan Blackmore</td>
<td>+971 4 312 9921</td>
<td><a href="mailto:jonathan.blackmore@ae.ey.com">jonathan.blackmore@ae.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Iain Burnet</td>
<td>+61 8 9429 2486</td>
<td><a href="mailto:iain.burnet@au.ey.com">iain.burnet@au.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Yoshihiro Azuma</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:azuma-yshhr@shinnihon.or.jp">azuma-yshhr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

Our Cybersecurity Leaders are:

<table>
<thead>
<tr>
<th>Global Cybersecurity Leader</th>
<th>+44 20 795 15769</th>
<th><a href="mailto:kallan@uk.ey.com">kallan@uk.ey.com</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>Area Cybersecurity Leaders</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Americas</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bob Sydow</td>
<td>+1 513 612 1591</td>
<td><a href="mailto:bob.sydow@ey.com">bob.sydow@ey.com</a></td>
</tr>
<tr>
<td>EMEIA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scott Gelber</td>
<td>+44 207 951 6930</td>
<td><a href="mailto:sgelber@uk.ey.com">sgelber@uk.ey.com</a></td>
</tr>
<tr>
<td>Asia-Pacific</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Paul O’Rourke</td>
<td>+65 8691 8635</td>
<td>paul.o’<a href="mailto:ourke@sg.ey.com">ourke@sg.ey.com</a></td>
</tr>
<tr>
<td>Japan</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Shinichiro Nagao</td>
<td>+81 3 3503 1100</td>
<td><a href="mailto:nagao-shnchr@shinnihon.or.jp">nagao-shnchr@shinnihon.or.jp</a></td>
</tr>
</tbody>
</table>

Global Privacy Leader

Sagi Leizerov | +1 703 747 0899 | sagi.leizerov@ey.com