Association of Corporate Counsel

By in-house counsel, for in-house counsel.®

LEADING PRACTICES PROFILES SERIES

Leading Practices In Privacy and Data Security: Compliance Programs Across the Globe

Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103, **fax** +1 202.293.4701
www.acc.com

Leading Practices In Privacy and Data Security: Compliance Programs Across the Globe

Updated June 2015

Provided by the Association of Corporate Counsel
1025 Connecticut Avenue, NW, Suite 200
Washington, DC 20036 USA
tel +1 202.293.4103
fax +1 202.293.4107
www.acc.com

This Leading Practices Profile, which updates 2010's *Leading Practices in Privacy and Data Protection: What Companies Are Doing*, examines the data security and privacy practices of six companies with operations spanning the globe. Organizations featured in this Profile described practices and approaches for working through the matrix of varying and changing requirements across multiple jurisdictions, as well as integrating policies and practices with systems and security features. In addition, organizations described the importance of implementing proactive practices to help ensure that privacy and data security considerations are included as part of business process evaluations.

The information in this Leading Practices Profile ("LPP") should not be construed as legal advice or legal opinion on specific facts, and should not be considered representative of the views of ACC, unless so stated. Further, this LPP is not intended as a definitive statement on the subject; rather, it is intended to serve as a tool for readers, providing practical, benchmarking information to the in-house practitioner.

This material was compiled by the Association of Corporate Counsel. For more information about ACC please visit our website at www.acc.com.

OVERVIEW

June 2015

This Leading Practices Profile updates our 2010 Privacy and Data Protection LPP and provides practical information on what six companies are doing with regard to global privacy and data security programs. Representatives provided information on the types of privacy and data security initiatives their organizations are implementing, including information on both internal and external privacy practices and compliance efforts on an international spectrum. Representatives also gave their thoughts on success factors and challenges, and on elements of their organizations' programs they consider to be leading practices.

In featuring the challenges and best practice solutions of organizations with extraterritorial operations, this LPP examines the privacy/data security and data security schemes that govern operations in the regions where ACC member organizations operate with greater frequency. Their insights and leading practices may be instructive for smaller organizations seeking to build smart compliance programs with more limited resources as well as larger organizations seeking to improve and refine existing programs. Although no single particular industry was targeted as participants, the LPP will nevertheless address particular privacy and data security concerns that arise in the context of those industries represented by the legal departments that agreed to take part.

This Profile once again features insights from Trevor Hughes, the Executive Director of the International Association of Privacy Professionals (IAPP), who discussed current privacy-related "hot topics" and trends and provided a contextual framework for the industry, highlighting how it has developed over the years, particularly as it relates to the in-house practitioner. In his analysis, he explores both the substantive issues and operational/management issues within the industry, and also shares his views on leading practices in global data privacy and protection.

Section I of this Profile provides an Introduction on data privacy and protection, including insights from Trevor Hughes, Executive Director of IAPP, on nascent industry topics and trends. Section II examines themes among the participants and Leading Practices for in-house counsel in implementing and maintaining successful data security and privacy practices for an organization. Section III describes each of the six organizations' privacy programs' structure and practices in detail, and Section IV provides sample documents, data security checklists, member affiliate directory disclosure forms, and sample privacy policies. Finally, Section V identifies key resources that were either discussed/mentioned in the Profile or are additional references useful to in-house counsel wishing to further explore this topic.

This LPP features the privacy and data safeguarding policies of the following six profiled entities:

- BP P.L.C.
- Dell Inc.
- EMC Corporation
- Hewlett-Packard
- Lawyers' Professional Indemnity Company (LAWPRO®)
- Legal Department of an Australian Technology Company

Representatives from each of these entities were asked to respond to some or all of the following general inquiries:

- Describe your privacy and data security programs, including information on both internal and external privacy practices and compliance and risk mitigation efforts on an international spectrum. Which standards are your programs based on? (This included questions about privacy systems and systems for securing and transferring data; privacy policies and sustainable programs governing products (i.e., internet of things considerations, certifications, preserving client/consumer trust). These questions helped paint a picture of the organization's ability to address both privacy and data security holistically.)

- Describe your incident response program for privacy breach or data leaks. Describe internal processes for employees to follow for data security/privacy protection (including cybersecurity breach responses, limiting exposure, and mitigating damages).

- Describe your privacy/data security personnel structure: teams/working groups (privacy, information security, IT); leaders, collaboration, integration and transparency, buy-in at all levels. Describe the enterprise management component of these structures, including the relationship between the CPO, CIO, and CLO. How do you see these areas as interrelating and how are they managed by the organization to mitigate the risk of a silos mentality?

- Describe your privacy and data security vendor facing programs, including outsourcing of data hosting/platforms and policies for external counsel. Is vendor management an important focus for in-house counsel? This inquiry includes potential questions about "taming" data through analytics to help manage relationships with external counsel and vendors, and improve data security with external fir

- Discuss privacy/data security concerns and solutions in cloud environments (including cloud issues in contracting, ISO standards, and EU data protection requirements). Discuss data security/privacy policies in the context of BYOD policies, including compliance with state and individual jurisdictional requirements, records management, technology controls, and litigation/regulatory holds.

- Describe success factors, challenges, and elements of your organization's programs you consider to be leading practices. What trends or developing issues do you anticipate will warrant a review of existing compliance frameworks within your industry (e.g., FTC privacy roundtable, EU new developments, impact of new requirements since 2010, emerging technologies, managing the scale of data creation)?

CONTENTS

I. Introduction

With increased globalization and the explosion of electronic communication channels, including social media platforms, we are in the midst of a prolific expansion into the world of data privacy and protection and a sharing of personal information unlike anything we have seen before. Privacy is being redefined and revolutionized. However, with new avenues and technologies come new problems and new risks, and companies have had to respond rapidly over the past few years to these changes in communication and the sharing of personal information. More than ever, corporate legal departments and privacy chiefs must ensure they are protecting their customers' privacy and are handling data correctly and effectively. Privacy and data security for companies has evolved from a conceptual framework or generalized practice to an institution-wide program with integrated official policies, procedures, and technologies. Companies have not only introduced integrated systems and technologies to handle data privacy and protection; in most cases, they have relied upon in-house counsel to construct and formally lead their privacy initiatives and practices throughout the organization.

Advances in globalization and technology present great opportunities and challenges in today's worldwide marketplace. Organizations featured in this Profile described practices and approaches for working through the matrix of varying and changing requirements across multiple jurisdictions, and developing and integrating policies and practices with systems and security features. In addition, organizations outlined the importance of implementing proactive practices to help ensure that privacy and data security considerations are included as part of business process evaluations.

A. Trends in Privacy and Data Security: IAPP Insights

As in 2010, ACC once again had the opportunity to speak with Trevor Hughes, President and CEO of the International Association of Privacy Professionals. In his role with IAPP, Hughes leads the world's largest association of privacy professionals. Hughes is an experienced attorney in privacy, technology, and marketing law. He has provided testimony before the U.S. Congress and the British and EU Parliaments on issues of privacy, surveillance, spam, and privacy-sensitive technologies.

We asked Hughes for his thoughts on some of the current "hot topics" and focus areas in the privacy and data security arena, and for his recommendations on leading practices and tips for practitioners.

1. Specific Practices & Key Elements of a Privacy and Data Security Program

According to Hughes, one size does not fit all when it comes to privacy programs. The size of the organization is not a measure of the size of the privacy function. With that said, most organizations in today's economy are touching data in significant ways, and that creates privacy risk. There is a need for expertise and risk mitigation.

Although some firms have a Chief Privacy Officer and a small team around that person, privacy issues need to be addressed throughout the organization, Hughes explains. The marketing team, the operations team—they may *all* need to have some expertise in dealing with privacy issues. One possibility is a **hub and spoke model** – a privacy leader, small team, and liaison network (privacy champions). This model is not based on a direct reporting relationship, but a dotted line and an obligation on that subject matter. These people also have other jobs; that is, they may come from various product lines and play other roles in the company. Whatever the structure, it is important to keep them all focused – the effectiveness of the function is correlated with the strength of the dotted-line relationship. The more that programs and processes like annual training requirements, accountability, and reporting are added into that relationship, the better. In a very sophisticated multinational company such as GE, Hughes says, he might want a chief privacy officer in each wholly owned subsidiary. "We are clearly seeing organizations recognizing the risks associated with privacy and the best mechanisms to deal with that risk – even rank and file employees need to have responsibility. If their "spidey" sense is tingling, they need to know what to do with that."

Within any organization, there are many components to a mature privacy program, Hughes explains. Research conducted in 2014 looked at how organizations are managing privacy today. Organizations need to start with how they are using/storing data (its life cycle in the organization), **building the systems and policies** for that data, **ensuring compliance**, and **ensuring the ongoing viability of the system**. "How do we ensure that we are mitigating risk to the greatest extent possible?" Hughes queries. "We employ **privacy impact assessments** and other tools for every new product and every new service."

Training and certification for employees is also important. Most organizations do a twenty-minute awareness campaign for new employees: "data is important." This has a limited value for risk reduction. Some employees will need more and better training than others, so role-based training appropriate to the individual is the way to go, Hughes advises. Certifications are important for some employees and not others. "For every contract you sign involving data, you must ensure that it is handled appropriately, from transfer to storage to management." Training is the best way to implement privacy initiatives, according to Hughes, and that applies to privacy generally, not just the policy or statement. Asking employees to read a statement is of limited value. Getting in front of people so they engage with and understand how the organization uses and manages data is more useful. The most forward-leaning organizations spend a lot of time and resources on making this happen.

As the world changes, data practices change. An overriding **mission statement** and broad parameters are important, Hughes explains, but most organizations update on a fairly regular basis as data practices change. "It's not constitutional and unmoving, but is in a constant state of change and improvement." The law will not answer every question. There are extra-legal issues; **understanding the ethical framework and values of the organization** is important. Executive support and thinking on handling data in the organization is important. "If the law is silent but the idea is stupid, that makes for a tough question for privacy professionals," Hughes says.

There are many thousands of pages written on what a policy statement should cover, so it is not possible to give a concise description. The policy statement needs to be specific to the organization.

At a minimum, it should cover what types of data the organization collects and what can be done with it.

Internally, the authority provided to the chief privacy officer depends on the organization. Clearly the most effective have **strong executive support and support from throughout the organization**.

Management of privacy within an organization is very complex. Professionals are developing a **strong tool kit** to understand and reduce the risk. This is not the type of thing where there is a single solution; there's no silver bullet. Good privacy management is made up of lots of good decisions and lots of careful management over time, according to Hughes.

2. External Privacy and Data Security Issues

Data is an asset. Privacy practices can be a risk vector. In any **mergers and acquisitions** activity, a company should make sure it understands how data and privacy are playing in that relationship. Can the asset be transferrable? What were the policies and expectations around the data when it was collected? If a company is acquiring data as part of an M&A activity, it must look at that data strategically and at privacy as a vector to completely understand it as part of the acquisition. It is also a management issue. "You want to do your due diligence to see how privacy works in that organization. If you can't show good practices, that should be on the table as part of the deal," Hughes says.

There is an incredible diversity of practices among different companies, according to Hughes. Some companies just want to do compliance. Some view it as a way to build customer trust. How a company handles privacy matters can be a **competitive differentiator**, and a part of the service. Google, Microsoft, Apple, and other major tech companies are trying to demonstrate that they are providing the highest level of privacy services. In the wake of the Snowden disclosures, tech companies looked at how they protected information from government surveillance, and some are using their policies on that front as a differentiator.

Vendor management for data is a challenging issue for privacy professionals and a risk vector for most organizations. "If you are providing or receiving data from a vendor, the privacy practices of the vendor are 'yours' for customers and regulators," Hughes states. "Ensuring that you have contractual protections and mechanisms for ongoing accountability are increasingly important in vendor contracts. If you are signing vendor contracts, the sophistication and complexity of the data exchange will drive the controls you should have for the agreement." Consider a cleaning service as compared with outsourcing health care review under a self-insured plan for a large organization – the number of laws and risks and sophistication is much higher in the latter case. "You want guarantees, accountability, and training/certification requirements," according to Hughes. "Vendor management is a big issue – whatever a vendor does with your data is what you do with data. It is very common for CPOs to be involved so that there are broad and encompassing provisions."

Cloud services add more layers of complexity. Providers are reluctant to amend their contracts, but increasingly, customers are demanding more protections in those agreements. The data may move all sorts of places around the world. What jurisdictions may be implicated? Do they have

privacy professionals on staff? There has been some guidance from regulatory agencies around the world, as well as some advisory opinions from a number of agencies, but the cloud is a complex and sophisticated place.

Hughes says he has not seen enforcement actions yet for the cloud, even though it has been embraced so quickly and completely. "We have seen in the wake of Snowden interest in data not flowing outside the country. Cloud management is not that different from other data management." The more mature an organization is, the better it can handle those issues. Good organizations are doing good things, and others are creating risks that they are not accounting for, adds Hughes.

3. New Trends and Developing Issues in Privacy and Data Security

According to Trevor Hughes, the BIG TRENDS include:

- Continued regulator and legislator focus. President Obama's initiatives involve student and consumer privacy, and "that's just the tip of the iceberg." In the EU, they are in the final stages of regulation that will preempt all privacy regulation in Europe at the national and regional level. Basically, Hughes says, "**EXPECT MORE LAW**. Watch as they apply new laws to industry and cross-functional areas. There will be more standards."

- Another trend is an **external enforcement risk**. The Federal Trade Commission has 170 privacy cases now, and they do a consent agreement on each one. State attorneys general are also active. California is the first state with a defined unit with staff within the AG's office. Also watch industry-specific and other regulators, Hughes advises. The Federal Communications Commission is also starting to move toward privacy enforcement, for example. Privacy and data security are also within the mandate of the Consumer Financial Protection Bureau.

- At the **class action** level, plaintiff's attorneys have been limited by the harm standard applied in breach cases because it is hard to articulate damages. Courts have been hesitant to go forward when they cannot determine harm. However, notes Hughes "[a]s theories of harm emerge, be prepared for class action activity."

- **Competitive forces** are also at play: Organizations that are sloppy on privacy are going to pay the price because competitors are going to have a field day with them. Those organizations that do a good job with privacy are going to engage the customer's trust and do more business with them.

- **BYOD** is incredibly complex, which is arguably a good thing. Employees are paying to buy the devices for their convenience. How much can the organization demand of the employees? "Leaks … confidential information … this remains a nascent area of privacy. Standards are just emerging. There is a huge amount of information being shared and discussion, but not a complete cycle of decision-making yet for legislation and courts." According to Hughes, employers recognize that there are risks and benefits when employees BYOD, "but having a privacy pro is the critical piece. You cannot move forward with BYOD without assessing privacy risks associated with it."

- There is a growing and increasingly clearly defined field of **privacy** emerging – it **is its own profession**. Companies are responding by making staff responsible for issue spotting and planning. Organizations must master these issues to be successful. "This is becoming a required skillset, especially for in-house counsel," Hughes says.

- Finally, it is important to recognize that not all **consent** is created equal. There are different flavors of consent. Some require an opt-in, some an opt-out – the broader issue is understanding what the law says and ensuring the organization is in compliance with the law, but also ensuring compliance with standards. Unsolicited commercial email is frowned on, even though the CAN-SPAM Act actually describes an opt-*out* standard for such messages. Questions to ask are, "How do you want to use privacy as a differentiator? Consent with an opt-out in every message? What is the sensitivity of the message/product? What will the recipient respond?" Full compliance with the law may not answer these questions, Hughes warns.

II. THEMES AND LEADING PRACTICES

A. Themes

Despite the variety of industries, size, and types of organizations profiled, the following themes emerged among the participants in discussing their data security and privacy practices. For details on participant programs, please see Section III, **Participant Profiles**.

1. Organizational Structure/Design Characteristics

Consistent with our 2010 observations, overall the participants' organizational structure could be generally categorized as either a centralized model, in which there is a centralized privacy office or team/group through which all privacy matters are directed, or a decentralized model, in which there is usually a Chief Privacy Officer, but responsibilities and implementation of the program are distributed throughout the organization via designated individuals. Large multinational organizations tend to follow the centralized model, meaning they have a clearly established central Privacy Office or Team through which all privacy matters are funneled. This model is seen at Dell, for instance, which described its structure as centralized. However, these organizations also typically utilize privacy officers or subject matter experts throughout the organization to help the central privacy office/team effectuate the program and reach its many offices and employees.

The decentralized model is one in which there is usually a single individual who "leads" the organization's privacy effort, typically a Chief Privacy Officer or Data Protection Director (although for some organizations, there is no single designated leader). In these instances, however, responsibility for privacy practices is distributed heavily throughout the organization, as staff are delegated specific roles to assist with implementation of the organization's privacy practices. This model is more commonly utilized by smaller organizations that can avoid having an entire Privacy Department or Team by allocating the responsibility among its staff in very specific, planned ways.

This concept is demonstrated by LAWPRO®, whose structures emphasize cross-functional roles and intercompany cooperation. LAWPRO®'s program is led by a single Chief Privacy Officer (CPO), but leading the program is not his only function. In that organization, privacy practices are distributed among others, including Department Heads (typically company vice presidents) who do not report directly to the CPO, as well as a Privacy Working Group. Thus, the decentralized model capitalizes on cross-functional leadership, in which different offices work closely together but often report to different executives. At BP, although there is a central data privacy team, there are also local privacy coordinators throughout the world who liaise with the central team. The privacy role in the smaller, wholly owned entities (with total staffs of around twenty) takes only about ten to fifteen percent of the employee's time, so the role is often assumed by the Human Resources Manager or another staff member.

2. Integrating Other Groups Into the Privacy Program

Another continuing common theme, regardless of which organizational model is employed, is integrating other areas of the business unit into the privacy program. Several participants reported that the privacy office works very closely with the organization's Information Security or Information Management Group in implementing their privacy practices. At LAWPRO®, for instance, the Chief Privacy Officer reports directly to the CEO. The Chief Information Officer (CIO) also reports to the CEO, so in essence, the CIO works in conjunction with the CPO.

Some participants also reported using a Privacy Working Group to either assist them with effectuation of the privacy program or to simply enhance the efficacy of the privacy office's role. For instance, L AWPRO®'s Chief Privacy Officer utilizes the company's Privacy Working Group, which is comprised of a cross-section of both management and other level staff from numerous areas throughout the company, meeting on as as-needed basis to discuss privacy-related issues. HP's Privacy and Data Protection Review Board, which meets quarterly, includes representatives from all business units and functions.

3. Thinking Globally

Most of the profiled entities conduct business across borders—if not internationally, then at least interstate or across provincial borders. Given the prevalence of the global business market, a few common threads emerged. Multiple participants, including Stephen Freedman of LAWPRO®, mentioned the importance of following the laws of the jurisdiction with the most stringent requirements, to be on the safe side. At BP, the company's Binding Corporate Rules were designed to meet the data privacy standards of 28 European member states, and business units must comply with the Rules, regardless of where they are located. Ellis Parry of BP also noted that the BP data privacy policy and personal information handling standards are standardized worldwide, with local versions where necessary that may set out a specialized policy or process for a particular area, such as consumer marketing or a given business line. The variations deal with specific scenarios when local laws exceed BP's global standards.

Cloud services add additional layers of complexity in a global setting. Trevor Hughes of IAPP stresses the importance of considering, up-front, which jurisdictions' laws may be implicated. Amy Holcroft of HP concurs, reiterating that it is essential to consider all of the implications of cloud

storage, including which jurisdictions' laws may be implicated. The avoidance of legal complexities encourages some participants to stick with home-based cloud entities.

B. Leading Practices

In both 2010 and 2015, Profile participants were asked to identify the elements of their data security/privacy programs they considered to be leading or best practices. The following are their leading practices, which discuss some of the program elements; however, interview summaries for each participant, providing additional details on their leading practices as well as their other practices and program elements, can be found in Section III of both this LPP and the 2010 Privacy and Data Protection LPP.

1. **A clear mission statement is the foundation of any privacy and data security program.** Understanding the ethical framework and values of an organization is important, says Trevor Hughes of IAPP, because the law does not answer every question. A mission statement should be fluid and updated as data practices change. Dale Skivington, Executive Director of Global Compliance and Privacy at Dell Inc., also stressed the importance of insuring that that the right policies and standards are adopted by the company. Amy Holcroft, Global Privacy Counsel for Hewlett-Packard Ltd., concurs.

2. **Training on privacy and data security, at all levels of an organization, is essential.** According to Hughes, "[m]ost organizations do a twenty-minute awareness campaign for new employees" that simply conveys a sense of importance about data. "This has a limited value for risk reduction." Depending on their role, some employees will need more specialized training than others, so customizing training for the individual's role is smart. Training is the best way to implement privacy initiatives, according to Hughes, and that applies to privacy generally, not just the policy or statement. Asking employees to read a statement is inadequate. Employees need to engage with and understand how the organization uses and manages data to achieve efficacy. Dell and Hewlett-Packard, too, emphasized the importance of a good training and communications program. EMC provides privacy and data security training on its information governance policy and other related policies. "An unknown policy is a nonexistent policy," EMC's Eleftheriou says.

3. **It is essential to obtain support from throughout the organization.** The most effective privacy officers have not only strong executive support, but also support from employees organization-wide, says Hughes of IAPP. Obtaining executive level support and sponsorship of the privacy program/privacy initiatives is truly a best practice, as this internal support can easily influence the ultimate success of the program. HP similarly indicated that this is an important success factor, and LAWPRO® cites obtaining company "buy-in" as a key success factor for its program, adding that this support should come from *every* level of the company, not merely from the executive level. One way to achieve this support is by showing employees why privacy is important and demonstrating its impact in understandable, practical ways.

4. **Vendor management is critical to privacy and data security.** If a company is providing or receiving data to or from a vendor, the privacy practices employed by the vendor effectively become those of the company, Hughes says. Accordingly, it is mission-critical to ensure, up-front, that your company has contractual protections that maintain its privacy and data security principles. Ellis Parry, BP's Global Lead for Data Privacy, advised that in contract negotiations, a company must seek to align vendor privacy programs with the company's global program. Skivington of Dell also mentioned the importance of considering the privacy and data security risks of working with vendors, and she emphasized that the process should begin with an up-front risk-based assessment. Skivington says it is important to have clearly defined expectations and ensure that the vendor's staff is trained on these expectations. LAWPRO® addresses the issue of privacy in all of its contracts with outside vendors, the terms of which inform the vendors of the company's policies and expectations. HP also expects its suppliers to agree to a robust set of privacy and security obligations.

5. **Cloud control is complex and cannot be ignored.** It is essential to consider all of the implications of cloud storage, including which jurisdictions' laws may be implicated. Holcroft of HP emphasized that security must be the "number one concern" in cloud computing. The general counsel of an Australian technology company also emphasized the sensitivity of cloud hosting and the need for strict guidelines, including adopting and applying ISO standards.

6. **BYOD can be even more complex.** Bring-Your-Own-Device standards are just emerging. Employers recognize that there are both risks and benefits when employees BYOD, but before personal devices are allowed, a company must assess the privacy risks and lay down clear rules. BP, for instance, allows some employees to BYOD, but restrictions apply; emails must be sent or received via a proprietary app, for example. If a device is lost, BP sends a kill message to the phone. LAWPRO® also allows employees to BYOD, but it allows access only through the company's web-based portal.

7. **When operating across jurisdictional lines, follow the strictest jurisdiction's rules.** Stephen Freedman noted that LAWPRO® follows the common practice of looking at which jurisdiction has the highest, most onerous requirements, and then applying those requirements across the board. Demetrious Eleftheriou, Senior Counsel for Privacy and Data Security at EMC, says that a template breach notification letter should address individual state requirements and be at the ready at all times.

8. **Base your data security compliance program on established privacy directives.** As in 2010, a number of participants that operate multi-nationally reported that a leading practice is building the company's privacy and data protection program and policies around the principles set forth in the EU Data Protection Directive or other high-level privacy directives. The rationale is that establishing standards at a higher level allows for easier transferability and broader application, so that a company's policies can apply globally with only minor modifications needed for certain countries. HP's global policies and standards are based on the EU Data Protection Directive, according to HP's Holcroft. Freedman reports that LAWPRO® has a specific internal Employee Privacy

Policy that is distinct from its regular Privacy Code, and that this employee policy applies to all of its employees. T he separate policies stem from the EU Data Protection Directive and Canada's legislative response in 2001, through which Canada sought to ensure it was compliant on a national level and could continue to do business in the EU.

9. **Keep consumer trust by taking a permissions-based approach to data collection and usage.** A number of participants, including LAWPRO®, indicated that transparency with consumers and keeping the focus on consumer permission for data collection and usage is the best way to secure and maintain consumer trust. LAWPRO® makes sure that it has thorough and accessible privacy policies to deal with the customer's personal information and takes steps to explicitly obtain the customer's consent on exactly how it handles personal information.

10. **Develop a formal incident response program for data breaches and/or leaks.** Organizations should ensure that they have some type of incident response program/procedures in place should a breach in data security or a data leak occur. A leading practice is having a *formalized* response program in place. In fact, Eleftheriou of EMC identified a security breach notification policy as one of the four core parts of EMC's privacy and data security program. Holcroft, Global Privacy Counsel for HP, also advised that security incidents be managed by clearly defined processes. LAWPRO® also has an incident response plan is in place in the event of a privacy breach.

11. **From the outset, focus on developing a privacy policy that is comprehensive, yet also readable and understandable by everyone.** Multiple participants identified a need to create policies that are communicated in a clear, transparent way for both customers and employees as a leading practice. To the extent possible, a company should try to develop a policy that is comprehensive, but that is also understandable by everyone. LAWPRO®, for one, takes this approach. HP's Global Master Privacy Policy, Online Privacy Statement, and Employee Privacy Policy are supplemented by a set of comprehensive privacy standards that help ensure compliance and consistency throughout the company.

12. **Establish a detailed internal system of processes and procedures for employees to handle privacy/data security matters.** Detailed written guidelines and processes for employees to follow is a clear best practice, even outside the data breach context. LAWPRO® cited this approach as a leading practice, indicating that providing detailed guidelines and resources to employees helps reduce the number of privacy issues arising on a daily basis, and more important, ensures that employees know how to handle privacy issues when they do arise. According to Freedman, LAWPRO®'s CPO, providing resources, such as a data incident response plan, precedent privacy letters, and consent statements integrated into various transactional documents, allows employees to both recognize the data privacy issues and know exactly how to deal with situations, including when to see a supervisor. Dell, EMC, and HP also stress the importance of strong internal policies and procedures.

III. PARTICIPANT PROFILES

A. BP P.L.C.

1. Background

BP P.L.C., registered in England and Wales, is one of the world's leading international oil and gas companies. It provides customers worldwide with fuel for transportation, energy for heat and light, lubricants to keep engines moving, and the petrochemicals products used to make everyday items as diverse as paints, clothes, and packaging. BP has 84,500 employees in nearly 80 countries, about 17,200 retail sites, and it generates economic value of $359.8 billion. ACC had an opportunity to speak with Ellis Parry, BP's Global Lead—Data Privacy. Parry's role focuses on global privacy issues management – data security being a distinct but closely aligned discipline at BP as it is in many conglomerates.

Parry is a contributing author to Sweet & Maxwell's "Data Protection Law and Practice" (4th ed.), IAPP's "Building a Privacy Program," and Nymity's "A Privacy Office Guide to Demonstrating Accountability."

2. Organizational Structure of the Privacy Group

BP is a large organization that is mature and sophisticated in its management of personal data. Personal information is managed according to BP's "Binding Corporate Rules," which is a global compliance framework forged from the European concept of data privacy. BP's rules meet 28 separate European member states' standards for data privacy, which all 100% owned BP entities, irrespective of where they are located in the world, must operationalize.

For instance, when someone applies for a job with BP anywhere in the world, Parry explains, the global data privacy policy sets out how information should be collected from the applicant so that it meets European Union standards as embodied by BP's BCR framework. So, an applicant in Germany (as an example of a country with some of the strictest data privacy laws in the world) should have the same experience as someone who applies in Oman or another country with less stringent requirements. The Binding Corporate Rules ensure that BP's data privacy handling standards are uniform across the global organisation. BP was one of the first multinational companies to adopt this European model as a global standard.

The data privacy policy and personal information handling standards are standardized worldwide, with local versions where necessary that may set out a specialized policy or process for a particular area, such as consumer marketing or a given business line. The variations deal with specific scenarios when local laws exceed BP's global standards.

In terms of staffing, there is a central data privacy team, the members of which are located globally. The central team members are responsible for specific areas of the world, such as Asia Pacific, Western Hemisphere, Northern and Southern Europe. In countries where BP has a wholly owned legal entity that employs at least twenty or more staff, BP appoints a local privacy coordinator who is responsible for the privacy program roll-out locally. That person reports locally, but the central team liaises with them closely offering active support and advice. The LPC role takes about ten to fifteen percent of the person's time, so the job is often taken on by the Human Resources Manager or a local IT or Legal staff member.

Joint ventures' policies depend on which entity has majority ownership. BP seeks to apply its policy when it has majority ownership; otherwise, it encourages the joint venture partner to accept its privacy policy and practices.

3. Key Elements of the BP Privacy and Data Protection Program

When an incident arises, the organization's preparedness is key to managing it successfully, Parry says. A company should have its written procedures readily available. People need to understand the process—both staff and stakeholders. Within BP, there are mandated reporters who must relay privacy breaches that come to their attention, although every staff member is responsible for alerting the correct stakeholders to issues which raise concerns. The incident response process includes the following steps:

- Breach
- Containment
- Preliminary Assessment
- Evaluation of Risk
- Notification (external regulators and/or affected individuals as needed)
- Future Prevention

Everything proceeds on a very tight time schedule. Teams need to understand their roles in advance, which is helped by performing dry runs.

For vendor facing programs, the vendors are triaged into segments according to the size of the BP spend and the sensitivity of the data the vendor handles. In contractual negotiations BP seeks to align vendor privacy programs with the company's own global program. The Central Data Privacy Team sets the strategy, produces the tools, and then supports the various business units' implementation of the centrally mandated strategy.

With regard to BYOD, if employees need a mobile device to perform their job role then BP will give them one, but BYOD is possible for most workers. For some teams, however, BYOD is not allowed owing to the sensitivity of the information they handle. In terms of technology, BP information on BYOD devices resides inside a virtual encrypted data "container" within the BYOD device. It is impossible to access a BP-provided email account on a BYOD device without first installing an app, which is available internally from the BP app store. It is a high-security third-party solution in its second generation. If the user loses the device, BP sends a

kill message to the lost mobile device, but BP is confident that the local encryption on the missing device ensures an adequate level of data protection even if the kill switch is not successfully activated.

4. Global Data Compliance

According to Parry, European regulators are frustrated with their inability to control large Internet companies without European headquarters. The apex of this battle is the European Court of Justice's "right to be forgotten" case allowing people, under certain circumstances, to rewrite their discoverable on-line history by demanding search engines de-list results which are returned when their personal information has been used as the search term. These types of decisions will have a dramatic impact on how search engine providers operate, raising new challenges and issues, Parry says, including an ideological battle between champions of freedom of expression and privacy advocates.

5. Leading Practices

When considering success factors for privacy programs, first take care in deciding what you measure, Parry advises. There is no legal or regulatory necessity yet to measure a program's success. BP gauges the success of its privacy program locally, then aggregates that data so that BP can demonstrate successful roll-outs by country or region or for BP as a whole across the globe. This system of measurement allows the Central Data Privacy Team to find potential gaps that indicate areas for focus in the short to medium term.

B. Dell Inc.

1. Background

Michael Dell started out in 1984 by building and selling personal computers from his dorm room at the University of Texas. The original name of the company was Dell Computer Corp., doing business as PCs Limited. The company was started with $1,000. Four years later, shares of Dell stock were sold for $8.50, and the IPO raised $30 million. Dell now employs approximately 100,000 people worldwide, which is six times the number of people employed at the University of Texas, where the company was born. Now a private company, Dell is focused on accelerating its end-to-end, enterprise solutions growth strategy and serving its customers.

Dale E. Skivington is the Executive Director of Global Compliance and Privacy at Dell Inc. She is responsible for leading a team that manages various compliance risks for Dell, including anti-bribery and data privacy. She serves as Dell's Chief Privacy Officer. Skivington has frequently lectured on privacy matters. ACC recently spoke with Skivington about privacy and data security issues.

2. Organizational Structure of the Privacy Group

According to Skivington, the Privacy Program at Dell is based in the legal department. Dell has implemented privacy programs for many years, with designated privacy professionals. The current Program is currently led by the Chief Privacy Officer, who reports to the Chief Compliance Officer, and the General Counsel. The other company compliance programs (anti-corruption, data security, gifts & entertainment) also share this organizational alignment. This collaboration of multiple programs enables each of them to leverage shared resources (e.g., strategy, communications, training, auditing, and project management).

Skivington notes that in addition to privacy professionals, the program is assisted by former auditors and CPAs to build and monitor controls in the various compliance programs and enable the programs to make advances, and to mature to meet challenges of emerging risks. The privacy team at Dell also consists of geographically dispersed lawyers and privacy managers aligned with various business units. The Program has been enhanced as the company moved into services and solutions—becoming an end-to-end solutions provider. The functions grew substantially, Skivington reports. The enhanced Program remains focused on data privacy and protection.

3. Dell's Privacy and Data Security Program: Key Elements and Leading Practices

According to Skivington, the key elements of any privacy program include:

- Insuring the right policies and standards are adopted.
- Providing a governance structure to ensure compliance.
- Performing comprehensive risk assessments.
- Implementing controls to mitigate risk.
- Having a good third party management program.
- Auditing and monitoring.
- Having a good incident response process.
- Having a good training and communications program.

These features are common to all compliance programs at Dell, Skivington says, and they assess the maturity of each program through the Global Compliance Office and Global Audit.

To handle risk assessments, privacy managers are assigned to a unit or function. They annually assess information management processes, as well as regulatory or statutory developments creating risks, gaps, or expectations. Privacy managers meet with leadership and stakeholders. They employ a "bottoms-up" assessment of risks, bringing many representatives together across the company to get a picture of the biggest risks. Based on this assessment, they build operational plans.

The biggest challenges cited by Skivington are the ever-increasing cybersecurity risks; the complexity of the regulatory landscape; managing different regulations and statutes globally; working to mature privacy impact assessments to include new risks; and managing third parties.

When third parties have access to data, processes need to be put in place. These processes should start when the third party is being considered as a possible vendor, beginning with a risk-based assessment. It is important to have clearly defined expectations up-front and ensure the vendor's staff is trained on these expectations. The third-party management process continues with monitoring and auditing as appropriate, she says.

C. EMC Corporation

1. Background

EMC Corporation is a global leader in enabling businesses and service providers to transform their operations and deliver IT as a service. Fundamental to this transformation is cloud computing. Through innovative products and services, EMC accelerates the journey to cloud computing, helping IT departments to store, manage, protect and analyze their most valuable asset — information — in a more agile, trusted, and cost-efficient way.

Demetrios Eleftheriou is Senior Counsel for Privacy and Data Security at EMC. Eleftheriou provides comprehensive legal and strategic advice on data security law and policy. He has published and presented extensively on global data security issues around the world, and is licensed to practice law in both the United States and Europe. ACC recently had a chance to speak with Eleftheriou about privacy and data security.

2. Organizational Structure & Key Elements of EMC's Privacy & Data Security Program

There are four important parts to EMC's model (all of which are proprietary):

1. First, EMC has an information governance policy that serves as the bedrock of data security at the company.

2. Second, EMC provides privacy and data security training on its information governance policy and other related policies.

3. Third, EMC has a data security breach notification plan to help expedite the response process.

4. Fourth, EMC has a template data protection agreement and playbook to help facilitate data security negotiations.

3. Data Breaches

"A good breach notification plan is critical to every organization," says Eleftheriou. "However, be sure not to have too many cooks in the kitchen implementing the plan," he advises. "Getting the facts of the incident to the legal department on an expedited basis is very important, since time is of the essence under the breach laws. For example, our plan has a Q&A document that can be sent to relevant stakeholders to collect the facts of an incident," he says. Eleftheriou adds that the Q&A is designed to ask the most important questions first to expedite the decisioning process, such as: What type of data was involved in the incident? Was the data encrypted? Did the data involve customer data? Was the data acquired? "Another important part of a breach notification plan is to have a template breach notification letter that addresses individual state requirements and includes helpful information on how the recipient can protect him or herself," Eleftheriou says. "You don't want to be researching the individual state requirements at the last minute," he adds.

Eleftheriou noted that nearly all 50 states have breach notification laws, and that there are breach notification requirements at the federal level as well. "Also, it's important to remember that breach notification may not only be required by law, but also by customer contracts, so check your contractual obligations," he adds.

4. How Technology Can Help Protect Personal Information and Comply with Global Data Security Laws

"Technology, of course, is not only necessary to secure data, but also can be used in innovative ways to reduce the risk of violating data protection laws," Eleftheriou says. "For example, can we use technology to take the 'identifiable' out of the definition of 'personal data' under the EU Data Protection Directive or out of 'personal data' held by a service provider or stolen by a thief?" he asks. "Let's take encryption, for example. If a cloud back-up provider is storing encrypted 'personal data' but does not have the ability to decrypt the data (only the cloud customer has the decryption key), the 'personal data' held by the provider is not identifiable – in other words, encrypted data or gibberish is not considered identifiable information," Eleftheriou points out. However, he argues, if the cloud provider has access to the decryption key and therefore has the ability to decrypt the data, the personal data is considered identifiable. "This is the same rationale used in the context of a data security breach, for example, when determining whether the decryption key was also compromised when encrypted data is stolen. If a thief has access to the decryption key, then encryption can't be used as a defense under security breach laws because the thief has the ability to use the decryption key to convert gibberish into identifiable data," he explains. "Let's also look at this from a cross-border data transfer perspective," Eleftheriou adds. "If a cloud user in Ireland encrypts his or her personal data and transfers it in an encrypted format to a U.S. back-up cloud provider and the provider is simply collecting and storing encrypted data and does not have the ability to decrypt the data, is the data transfer subject to European cross-border transfer restrictions on personal data?" he asks. This is a great debate to have with EU privacy experts, Eleftheriou further notes.

5. Will Additional Security Legislation Push Organizations to Do More to Secure Data?

"Generally, the problem of unreasonable security practices for organizations is not a lack of additional security legislation but a lack of proper resources and education," says Eleftheriou. "In

my opinion, we do not need any more redundant legislation on privacy and data security," he says. Eleftheriou argues that the U.S. needs a reasonable and comprehensive federal privacy and data security law, or at the very least, a federal security breach notification law that will preempt the significant number of state security breach notification laws and streamline the federal breach notification requirements. "Resources spent on trying to comply with a hodgepodge of federal and state breach notification requirements should be used to actually protect data," Eleftheriou adds.

6. Leading Practices

Eleftheriou identified the following leading practice pointers:

- Anonymization is your friend. Saying this is simple, but **don't collect personal information if you don't need it**. Work with anonymous or de-identified data if you can.

- Data minimization is your friend. **Collect only what you need and disclose only what is needed**. Try to avoid or minimize the collection or disclosure of sensitive personal information or the notice-triggering stuff under the breach laws.

- Encryption is your friend. Stolen encrypted data is a safe harbor under the breach notification laws (so long as the decryption process is not also compromised). Have a good password policy, since **encryption is only as strong as your password**.

- Train your employees on your privacy and related policies. **An unknown policy is a nonexistent policy**.

- **Perfect data security is not required, so don't guarantee it**. The general rule for data security is to have "reasonable" and appropriate administrative, technical, and physical measures in place.

- **You can outsource responsibility, but not accountability**. You are accountable for your personal information even if processed by your vendors. Do your due diligence on your vendors and have them sign a data protection agreement that includes audit rights and breach notification.

- You've had a data breach! **Just because you had a data breach does not mean you have unreasonable data security practices in place.**

- You've not had a data breach! **Just because you have not had a data breach does not mean you have reasonable security practices in place.** Take a look at your detection practices.

- **The perimeter is dead,** as some security techies are saying. Don't focus too heavily on prevention or the perimeter at the expense of detection and response. Make sure to also have reasonable detection and response measures in place.

- **Time is the enemy of a data breach**, but a data breach plan can help you expedite the response process. Get one in place.

D. Hewlett-Packard

1. Background

As noted in our 2010 LPP, Hewlett-Packard (HP) is an international technology company that clearly has a vested interest in data security and privacy. Headquartered in Palo Alto, California, it operates in more than 170 countries and on six continents around the world, managing over 300,000 employees and is involved in almost every industry. Equally powerful and impressive is HP's Privacy and Personal Data Protection program, distinguishing HP as a true global leader in privacy practices for over a decade. Just to highlight a few of its achievements in the privacy arena:

- Over the past 9 years, HP has consistently ranked in the Top 5 on Ponemon's "Most Trusted Company for Privacy Study".

- HP was a founding member of the Better Business Bureau Online Privacy Program, which evolved into the BBB Accredited Business Program and certifies privacy compliance.

- HP continues to play a leadership role in the International Association of Privacy Professionals (IAPP), including membership on the Board of Directors and the CIPP Certification team, and foundation of the IAPP Innovation Award.

- Since 2007, HP has taken a leadership role in developing the Asia Pacific Economic Forum privacy framework, including APEC Cross Border Privacy Rules, for which HP was certified in 2014.

- HP developed a privacy-by-design tool known as the HP Privacy Advisor in 2010, which helps HP continue to facilitate privacy education, guidance, and compliance.

- In 2011, HP became one of the first high-tech companies to obtain approval for Binding Corporate Rules for Controllers, and it hopes to obtain approval for Binding Corporate Rules for Processors in 2015.

- HP played a key role in the formation of the Information Accountability Foundation in 2013 and is a key contributor to the development of the Unified Ethical Framework for Big Data Analytics. HP is actively involved in the development of a "Big Data Code of Ethics" led by the Foundation and backed by regulators, companies, and the privacy community.

- HP Labs is an initiator and a key member of A4 Cloud, a four-year European funded research project into accountability in cloud computing.

- In 2014 HP business units staffed compliance offices to implement a pan-HP programs to ensure compliance with the US Health Insurance Portability and Accountability Omnibus Rule (HIPPA).

ACC had the opportunity to speak with HP's Global Privacy Counsel, Amy Holcroft.

2. Organizational Structure

The HP Privacy Office is critical to the success of HP's privacy program. The Privacy Office is part of the Ethics and Compliance Office within the Legal Department. The organizational structure of the Office has not changed since the 2010 LPP. Scott Taylor, Vice President and HP's Chief Privacy Officer (CPO) manages a team of 15 privacy subject matter experts who are all Certified Information Privacy Professionals (CIPP). The CPO reports to the Head of Ethics and Compliance who in turn reports to HP's General Counsel, John Schultz.

The Privacy Office is responsible for the development and management of policies and standards, compliance and training programs, providing consultancy to the business and external engagement with key regulators and government's stakeholders. The team is structured to provide advice and support by region (Americas, APJ and EMEA), business units (Enterprise Group, Enterprise Services, Cloud, HP Software and Printing and Personal Systems) and global functions (HR, marketing, government affairs and audit). This has ensured strong engagement and maintained the Privacy Office as a trusted advisor to the business. Holcroft provides strategic and specialist legal advice to the CPO, Privacy Office team and the business, with the support of local counsels to advise on local laws.

The **Privacy and Data Protection Review Board** (PDPB) remains a key part of HP's privacy and security risk management and governance. Senior representatives from all business units and functions are members of the board, which meets quarterly. The PDPB identifies risks annually, regularly assesses progress and helps to design and lead mitigation strategies.

The Privacy Office is actively engaged at global and regional level with regulators, governments, major think tanks, key industry and civil society organizations to promote innovative regulatory and business mechanisms protecting citizens' privacy while preserving innovation in business models and technologies.

3. Key Elements of HP's Privacy and Data Security Program

Accountability remains the foundation of HP's privacy program**, which is implemented through the HP Privacy Accountability Framework**, Holcroft reports. HP takes a holistic approach to compliance, based on the law and ethical principles. The framework aims to go beyond mere compliance and achieve effective data protection throughout the data lifecycle, while preserving innovation, by taking into account the potential risks, harms and data subject expectations as early as possible.

The HP Privacy Accountability Framework has three layers:

Oversight Layer: On the top is an oversight and governance layer in which the business identifies privacy risks and opportunities and ensures they are managed through a robust governance model.

Contextual Approach Layer: In this layer the Privacy Office plays a key role by ensuring that HP commits to clear privacy policies, which are then implemented and validated. HP refers to this as the "program backbone" and the Privacy Office has a major stake in developing, updating and enforcing policy.

Demonstration Layer: This layer is the internal and external proof point that the company takes privacy seriously. It has the objective of effectively demonstrating to key stakeholders, including data subjects and regulators that the company is behaving in accordance with its promises. This practical demonstration can take different forms, depending on the audience, but one of the best examples is the use of BCR as a demonstration of Accountability implementation to the regulators.

The framework is supported by HP's global policies and standards, which are based on the EU Data Protection Directive.[i]

The **HP Global Master Privacy Policy and HP Online Privacy Statement** govern the collection and processing of HP's customers' data. Both policies are publicly available on HP's websites and published in over thirty languages. These policies are supplemented by country or region specific policies, which are also accessible from the website. For example, the Privacy Data Rights Notice is accessible from all European web pages to inform European customers of their rights to access, delete and correct data under EU law and their additional rights under HP's Binding Corporate Rules.

HP has also implemented an extensive customer complaint handling system which aims to provide consistent incident management procedures from identification through closure. This incident management process provides the Privacy Office experts with an opportunity to deliver hands-on consulting to the business on issues, themes and trends.

Internally, the processing of employee data is governed by the **Employee Privacy Policy** which covers what data is collected from employees, how it is used and employee's rights regarding their personal data.

The privacy policies are supplemented by a set of comprehensive **privacy standards** to help ensure consistent and compliant practices throughout the company in relation to consumer, employee and enterprise customer personal data. These standards cover a broad range of subjects from data collection practices and direct marketing to the deployment of automatic data collection tools on HP websites. The standards are made available to employees through a dedicated Privacy Office intranet page. This site also provides easy access to policies, training modules and contact details of the Privacy Office team.

HP has certified to **binding co-regulatory programs** in all regions where it operates. In 2011 obtained approval for EU Binding Corporate Rules for Controller and more recently obtained certification for the APEC Cross Border Privacy Rules in 2014.

HP's engagement and oversight of **outside vendors** and suppliers seeks to ensure robust privacy protections are in place where personal data is processed outside the organisation. A privacy and data security questionnaire is provided as a part of HP's supplier due diligence and HP expects its

suppliers to agree to a robust set of privacy and security obligations to ensure the protection of data throughout the contracting ecosystem.

HP responds to **security incidents** through the deployment of defined incident management processes led by HP's Cyber Security team. Processes vary according to whether the incident has impacted HP or its enterprise customers' data but whenever personal data is involved Holcroft and other privacy specialists are involved in managing the incident from start to finish – understanding what has happened, defining the remedial actions to be taken, assisting with the notifications to customer and regulators and, at the end of the process, a review of lessons learned.

On the services side of HP's business, "Ensuring the privacy and security of our enterprise customers' data is fundamental to HP and critical to the success of our services business," says Holcroft. Privacy and security is the number one concern in cloud computing and HP aims to understand that and comprehensively address customer requirements both in its contracts and operations. International data transfers are a challenge for both service providers and customers as a result of the dynamic global technology systems relied on today. HP is in the process for applying for Binding Corporate Rules for Processor to offer its customers a comprehensive compliance mechanism for the transfer and processing of their data within the HP corporate group.

4. Success Factors

Holcroft explained that the success of HP's Privacy Program is attributable to both internal and external success factors.

Internally, a combination of Executive support and investment in HP's Privacy program and support at all levels of the company have been major contributing factors to the program's success. Holcroft explained that privacy and security needs to be part of a company's culture for any compliance program to be successful. "You can have all the policies you like, but if your employees don't understand and respect them they are not worth the paper they are written on." "Privacy and data security have a high visibility and presence" and HP seeks to create an "Accountability Culture at HP, including through HP's training program. Privacy training is a key part of HP's mandatory annual Standards of Business Conduct refresher course, which was completed by 99.9% of employees in 2014.

Externally, thought leadership and dialogue with regulators is the other key element of HP's success. HP's CPO and his regional team leads regularly engage with regulators around the world. HP firmly believes in constructive dialogue with regulators to help them understand the business context and challenges and inform the development of law and policy.

5. Future Challenges

Holcroft identified Big Data as one of the primary privacy challenges many companies face in the future as the power of this technology evolves. Whilst recognising the business opportunities of being able to collect and analyze huge amounts of data, both for its own business and the customers who buy its data analytics products, HP also understand the legal and ethical need to

ensure these new technologies are used in a way which protects individual rights. HP is at the forefront of the work in this area with its involvement in the development of a Unified Ethical Framework for Big Data Analytics. This groundbreaking initiative is led by the Information Accountability Foundation (IAF) and backed by regulators, companies and the privacy community. HP's CPO co-chairs the projects research team, which is developing a Code of Ethics to guide companies and other organisations that work with Big Data.[ii]

E. LAWPRO® (Lawyers' Professional Indemnity Company)

1. Background

In 1995, Toronto-based LAWPRO®—or LPIC, as it was then called—was little more than a Law Society of Upper Canada mandate, a collection of ideas and "to do" lists, and a handful of people working together to build a new insurance company from scratch and in record time. Now LAWPRO® is a successful, solid insurance company cited for its principled claims management, proactive practicePRO® risk management program, and innovative approaches to technology for the legal profession. LAWPRO® has grown from a single line, regional insurer to a multi-line insurance organization that operates nationally, serving lawyers' insurance needs through malpractice and title insurance. LAWPRO®'s products include a professional liability insurance program, serving over 25,000 lawyers within the province of Ontario, as well as an excess insurance program that insures more than 1,422 firms and more than 3,724 lawyers. LAWPRO® also provides nation-wide comprehensive title insurance and legal service in all of Canada's ten provinces and three territories.

Although LAWPRO® operates exclusively in Canada, it reports annual revenues of around $140 million and manages more than 2,000 new claims from lawyers every year. Privacy and data security are clearly imperative to its success. In fact, LAWPRO® received the "2006 Top Privacy Policy in Canada Award" by Nymity Inc.

In 2013, Stephen Freedman was appointed as LAWPRO®'s General Counsel & Chief Privacy Officer. Prior to that time, he served for five years as the company's Director of Compliance Risk & Chief Privacy Officer. Freedman directed LAWPRO®'s compliance with both federal and provincial privacy legislation by developing strategies and implementing policies, which he continues to manage. His duties as Chief Privacy Officer include an ongoing responsibility to analyze all of the company's personal information handling practices, ensuring that their privacy policy is current, and overseeing privacy compliance for all the departments within LAWPRO®.

ACC had the opportunity to speak with Freedman about privacy and data security issues, both this year and in 2010. The highlights of both conversations are reported below.

2. Organizational Structure of the Privacy Group

According to Freedman, LAWPRO® has been very focused on privacy since the early 2000s. (Canada passed federal privacy legislation in 2001 and 2004.) Now, LAWPRO® has "a robust"

privacy program. There has been buy-in for the program from the Board and management since day one, he says, and that has been very helpful. Freedman reports directly to the CEO. The Chief Information Officer (CIO) also reports to the CEO, so he works in conjunction with Freedman. The CIO is responsible for ensuring that all of the corporate data—not just personal information—is protected, whether this involves levels of encryption, access, or storing.

In differentiating their roles, Freedman states, "The CIO is more responsible for the data protection and security side of things, while my role is to ensure that from a privacy perspective, we, as a company, are doing what we need to do." Notably, the Chief Privacy Officer has few direct reports, aside from administrative staff; however, Freedman explains that this structure was by design, as the company opted for imposing obligations on Department Heads to effectuate privacy practices throughout LAWPRO®.

LAWPRO®'s CIO is very collaborative, and has been instrumental in coordinating the Privacy Working Group since the beginning. One person from each department is assigned to the working group as the "Privacy Liaison." The group is comprised of a cross-section of both management and other level staff from numerous areas throughout the company. They try to ensure that, within each department or function in the company, there is some representation of both management and non-management in the privacy group. There has been extra focus on training representatives to the group. At the executive level there is a weekly meeting, and privacy is a standard agenda item.

Perhaps attributable to the fact that LAWPRO® provides insurance to attorneys, LAWPRO® has a significant number of attorneys on staff: of its roughly 130 total employees, 50 are attorneys, including the CEO. However, due to LAWPRO®'s relatively small size, they cannot have a large independent privacy group. Even for Freedman, privacy is not his sole responsibility; it's one of his many functions. Thus, LAWPRO®'s organizational structure reflects cross-functional roles and an emphasis on intercompany cooperation. While Freedman serves as the head, the privacy function is dispersed throughout the company in a variety of ways. Individual department heads—typically vice presidents within the company—are responsible for ensuring compliance with the company's privacy policies and procedures for their department, along with their other responsibilities.

3. LAWPRO® Policies & Practices

a. Updated Comments

Freedman emphasized during his recent conversation with ACC that LAWPRO® has an **incident response plan** in place for privacy breaches. Managers in each department make employees aware of the response plan. Responsibility ultimately lies with the department heads to be fully aware of the many requirements, but the General Counsel actively assists.

When there is a breach, it is understood that the appropriate people must be made aware of it. The harm done by the breach is assessed. If there is a risk of harm, notification is made. If the breach is not serious, a message goes to the impacted location. In appropriate circumstances, the response plan requires notice of the breach to the person whose information was compromised.

LAWPRO® writes Errors & Omissions insurance for lawyers, so there is a lot of sensitive information at risk. **Breaches are taken seriously**. When information goes to an unintended recipient, the notified person whose data was breached generally appreciates the lengths to which LAWPRO® goes to rectify the problem. It is intended that the person who receives the information will delete or destroy it. Breaches are tracked to look for patterns, so that problems may be addressed and, if possible, prevented. Detailed training is provided to all employees.

One way of preventing breaches is to **adjust how email addresses are pre-populated**, Freedman notes. Pre-population is limited to addresses in the sender's address book, not everyone to whom or from whom an email has ever been sent or received. Also, for documents sent out externally, LAWPRO® prefers using PDF versions, because of the way metadata is stripped. Employees are not permitted to add software to, or make changes to software on, their devices without prior permission. Personal data is not normally allowed on any company-issued devices.

Employees who need a portable device are generally issued one by the company, but they are also allowed to use their own devices, within limits. Information on the issued devices is controlled. **For BYODs, LAWPRO® allows access only through the company's web-based portal, which primarily limits access to email and calendar functions**.

The issue of privacy is addressed in **contracts with outside vendors**. Vendors are informed of the company policy and the company's expectations.

LAWPRO® is concerned about data in the **cloud**. The sensitive nature of the data LAWPRO® collects and uses is such that they prefer to keep data in their own environment. In other words, they are particular about where data is stored, choosing to maintain core data exclusively on their own servers in most cases. According to Freedman, they prefer to stick with Canadian providers when opting for cloud storage; they will generally work with a foreign provider only if the servers are in Canada. Otherwise, there is the potential that data may be accessed by foreign law enforcement or governments, which is viewed as an unnecessary risk.

With new amendments to the federal legislation currently before Parliament will come new breach notification requirements, Freedman says, but the new requirements will not require many changes to existing practices at LAWPRO®. He says that other amendments will allow for the sharing of information between organizations for purposes of detecting and preventing fraud, which is particularly helpful in the insurance context.

b. Reflections from 2010

When ACC spoke with Freedman in 2010, he indicated that LAWPRO®'s customer Privacy Code was based upon the Canadian Standards Association's ("CSA's") Model Code for the Protection of Personal Information (Q830), which CSA established in 1996.[9] CSA's Model Code articulated Ten Principles of Privacy, very similar to the seven principles contained in the EU Safe Harbor framework.[10] Thus, LAWPRO® utilized CSA's Ten Principles to construct the company's privacy code. As such, their customer Privacy Code, which is available on their homepage, includes the following ten essential provisions:

1. **Accountability.**

2. **Purposes/Reason**: Identifies the purposes/reasons for which they collect information.

3. **Consent.**

4. **Limiting the collection of information**: They will not collect anything without a real or substantial need for it.

5. **Limiting the use, disclosure, and retention of information**: They will not even hold the information if there is no pressing need for it.

6. **Accuracy**: Their commitment to ensure that the information they have is accurate and the ability of the person to correct it, if necessary.

7. **Safeguarding**: How they protect the customers' personal information (which meshes with their Security Policy, which is a separate document).

8. **Openness**: The desire to be open and transparent about what their privacy policies are, and also communicate these in a way that is clear and straightforward.

9. **Access**: It's important for people to be able to access the information that they have.

10. **Recourse**: How they deal with concerns/complaints that customers might have.

LAWPRO®'s Security Policy focuses on its internal security controls and the ways that LAWPRO® protects its customers' information. Examples range from physical protections (like locked cabinets) to electronic-based protections, including passwords and access limitations. It also addresses network and server security, and web access (what they track, what they know about visitors to their site, cookies, the kind of encryption and other things they use to protect information through web-based interfaces). Other controls include automatic, timed log-outs for secured parts of the website to protect information, facts on caching of information, and destruction guidelines (how they deal with eliminating personal information that they no longer need or that has reached a limit on how long they can retain that information).

Both the Privacy Code and Security Policy are provided in English and French versions on LAWPRO®'s site, along with a number of other consent statements for different types of customers and clients, like LAWPRO®'s Personal Information Statement for Ontario Lawyers. As Freedman emphasized, "We really want to be as open about our privacy handling practices as we can. We certainly don't want to be in a situation with a customer where we have to point them to some antiquated privacy policy tucked away."

LAWPRO® also has a specific internal Employee Privacy Policy that is distinct from its regular Privacy Code, and this employee policy applies to all of its employees. Freedman explained that the separate policies stem from the EU Data Protection Directive and Canada's legislative response in 2001, through which Canada wanted to ensure it was compliant on a national level and could continue to do business in the EU. Thus, in 2001, Canada passed the Personal Information Protection and Electronic Documents Act (PIPEDA), a federal law governing private-sector privacy

practices across Canada, except where individual provinces have passed their own substantially similar privacy law.[11]

However, as Freedman explained, PIPEDA resulted in a "loophole" for many companies across Canada in connection with personal information about their employees. Specifically, PIPEDA does not apply to employee-related personal information, unless the information is held by a federally regulated business, such as a bank or telecommunications company.[12] This means that the law does not regulate how numerous businesses handle the personal information of their employees. Nevertheless, the provinces that have passed comprehensive, substantially similar privacy legislation (as of 2010, Alberta, British Columbia, and Quebec) have chosen to regulate employee personal information.[13]

In provinces where no comprehensive private-sector privacy law has been passed, the law does not require protection of employee personal information. This is the case in Ontario, which has not passed its own substantially similar provincial law. Freedman summarized, "Like most businesses in Ontario, we wouldn't actually be required to have a privacy code or privacy policy in relation to employee information, but we do because we think it's important."

The **employee privacy policy**, which is predominantly administered by the Director of Human Resources, covers a whole range of topics, including what LAWPRO®'s corporate commitment to privacy is with respect to its employees and the employee's role and/or duty in maintaining privacy. Key elements of this policy include:

- LAWPRO®'s expectations of its employees in complying with its Privacy Code, Security Policy, and other policies around computer use and related uses;
- Explanation for why they collect, use, and disclose personal information;
- A number of examples of purposes for which they collect, use, and disclose that sort of information;
- Examples of types of personal information that they collect about employees;
- Explanation of how long they maintain personal information and how employees can get access to their information; and
- How LAWPRO® addresses employees' concerns (if they have any) about LAWPRO®'s handling of their personal information.

LAWPRO® communicates this policy to its employees in a variety of ways, with particular emphasis on electronic communication. "We're pretty electronic," Freedman explains about the company, "so most everything these days for us is done electronically." Their primary vehicle is LAWPRO®'s Intranet, with a **Privacy Policies page** that is contained within a larger GRC (Governance, Risk, and Compliance) section of the Intranet. This Privacy Policies page is subdivided into the following areas:

1. **External Privacy Policies:** Provides LAWPRO®'s actual External Policies including the Privacy Code and Security Policy.

2. **Internal Privacy Policies:** This includes the Employee Privacy Policy, a Guidelines Document on Personal Information in Claims Handling (related to claims handling and litigation), a procedure document on how to deal with privacy complaints and access to personal information (the two most common issues in the business units), a policy on Electronic Document Handling (which covers issues such as when an employee needs to send out a document externally and can avoid sending personal/sensitive information).

3. Incident Response Plan: This is a comprehensive plan for privacy matters. If there is any kind of breach relating to personal information, this details precisely what to do and who to inform. It covers anything from someone hacking-in externally to their system to an employee who thinks he put something in a recycle bin instead of a shredder, detailing what steps they take in terms of informing various persons, etc.

4. Policy on Use of Portable Devices: Because of the heightened vulnerabilities around the use of portable devices, there are specific policies governing the use of such things as laptops, phones, blackberries, etc. (especially applicable to the sales and marketing group). Their basic policy is that they do not want employees keeping personal information on these devices unless it is absolutely critical that it be there; the preference is for the employee to connect remotely to their system.

5. Consent Statements: The rationale for these statements is that when it comes to management of personal information of their customers, it is very important to LAWPRO® that they make sure they have thorough and accessible privacy policies to deal with the customer's personal information, but also to take steps explicitly to obtain the customer's consent on exactly how it handles their customer's personal information. So, LAWPRO® created a number of consent statements that they have built directly into various documents and forms that they use for transactions. The consent statement is usually a few pages in length, explaining: the types of information they collect, use, and disclose; examples of how they use it; when it might be disclosed; and their (LAWPRO®'s) commitment to abide by the consent the customers provide. These are used for lawyers who are obtaining insurance as part of their practice, but similar types of consent statements are used for their title insurance businesses as well, such as for homeowners or lenders.

6. Precedent Privacy Letters: LAWPRO® has assembled a number of policy letters that staff can use for the more straightforward external relationships that involve a sharing of personal information, whether it is with suppliers or others with whom they do business. These precedent letters provide wording on what they expect their relationship to be with that party. In some cases, they include model contract terms for fairly straightforward external relationships. For example, for agreements with their suppliers or vendors, if there is sharing of personal information, then the starting point is that they will agree to abide by LAWPRO®'s privacy code or that LAWPRO® is satisfied that the other company has a privacy policy that is adequately equivalent to their own. However, for more complex situations, they will refer directly to Freedman.

All of LAWPRO®'s staff is trained in privacy. A certain form of this **training** applies to all employees, but then certain employees receive specialized training depending on their level or function. For example, certain managers or supervisors will undergo more specialized training because they have responsibilities involving outside requests for personal information or are

receiving complaints. Moreover, LAWPRO® also makes an effort on a regular basis to post articles on their intranet on privacy law issues that would be relevant or of interest to their staff.

Finally, like many other companies, LAWPRO® internally utilizes a type of **entitlement management system** to control the access and use of sensitive and important data. With restrictions built right into the system, Freedman states that "it is actually quite granular in terms of who gets access to what. It's not just a simple layered type of system where if you are in, for example, the executive group, you receive access to everything." Thus, their system is very customized, tailored to the specific duties and responsibilities of the specific employee. Essentially, only those who have a need to access personal data, in terms of their specific responsibilities, will be granted access to it. LAWPRO® utilizes this approach for many different types and forms of information. According to Freedman, because of this customization, there can be enormous differences from one employee to another in terms of what they have access to.

4. Global Data Compliance

LAWPRO® has to deal with privacy issues only in Canada, but in many jurisdictions within Canada. The company monitors developments in all jurisdictions: federal, provincial, and territorial. They perform gap analyses as necessary, and adopt policies accordingly. LAWPRO® follows the common practice of looking at which jurisdiction has the highest, most onerous requirements. Those are the requirements that are followed. Only a few Canadian jurisdictions have breach notification laws, but amendments to the federal law are currently before Parliament, including a national breach notification requirement.
Canada has some of the same conceptual privacy issues that exist in the U.S. (e.g., there is no single national private-sector privacy law). Although the Canadian federal government passed one of the first private-sector privacy laws, and several provinces have passed their own privacy laws, only three supplant the federal law. There is no expectation that Ontario will enact comparable legislation in the future, Freedman says. The anticipated federal amendments will be beneficial.

5. Leading Practices

In discussing success factors or best practices for LAWPRO®, Freedman identified a few key factors. First, he indicated that their privacy program works well due to the enormous amount of time they spent at the outset establishing the program and creating a **policy** that was **not only comprehensive, but readable and understandable** by everyone.

Further, he indicated that a leading practice is that all of the **processes/procedures** for how they handle things (e.g., access to information, issuing complaints, etc.) **are very detailed**, so employees have the guidance they need given that privacy issues do not necessarily arise every day. For example, when someone asks for access to their file, an employee can utilize the existing procedures (including precedent letters) to be able to see when it is appropriate, when there are exceptions, and what information they should provide to the requestor. Then, if there are questions or issues, they will go to the department head or, if necessary, to the Office of the General Counsel to assist.

Therefore, LAWPRO® has a **system in place to make sure they are managing privacy well** because they want to make sure their customers are happy, as well as to manage their risk and reputation.

When asked about key success factors and/or challenges in implementing a privacy program, Freedman felt that a key success factor is **obtaining company "buy-in"** on the whole idea of privacy compliance. Further, this support needs to come from every level of the company, not merely from top-level management. Thus, people have to understand why privacy is important and the downsides of not having an effective compliance program, whether this is from a regulatory standpoint or simply reputation management. According to Freedman, it is critical to find ways to make privacy "real" for staff by presenting it in a way they can understand.

As for challenges in implementation, LAWPRO®'s privacy program was implemented back in 2004, so now the challenge centers more around **keeping staff aware of and continually involved** in privacy. As Freedman explained, "While you don't need or expect all staff to be privacy experts, they have to at least know enough to be able to identify when there is an issue." The challenge over the years is finding that balance between making sure there is enough information so privacy is on everyone's minds and they can identify an issue, and over-saturating them so they simply ignore communications and privacy issues completely. This is a process that is continually being refined and enhanced, Freedman says.

F. Legal Department of an Australian Technology Company

1. Background

One of the participants in this year's Leading Practices Profile on Privacy and Data Protection chose to remain anonymous, both personally and as to the entity with which he was affiliated, but was willing to share his insights gained from serving as general counsel of an Australian technology company.

2. Privacy and Data Security in Australia

Data security rules must live up to the needs of government and financial institutions to protect unique user information. Because of the sensitivity of the information, cloud hosting and data centers must have strict guidelines. Becoming certified to the ISO 27001 standard ensures that there are controls in place. The ISO standards help organizations keep information assets secure. Using this family of standards helps organizations manage the security of assets such as financial information, intellectual property, employee details, or information entrusted to them by third parties. ISO/IEC 27001 is the best-known standard in the family providing requirements for information security management systems (ISMS). The standard places limits on who can access data, making information more truly confidential. In this way, the standard facilitates customer information management while making sure only authorized "eyes" have access. Organizations should strive to get such a program up and running.

In Australia, the Privacy Act governs what is private, when it can be revealed, and the confidentiality of various types of information. It sets forth an obligation to tell people what you

collect and what you do with that data, including cross-border data storage. At the federal level, Australia introduced a new Data Retention Law, which recently passed (as this article explains). Another important Australian law is the Telecommunications Act. Under that post-9/11 law, information can be retrieved by law enforcement based on suspicion.

Privacy disclosure issues are sometimes handled in the courts. In a series of notable cases in Australia and elsewhere, the company behind the movie *Dallas Buyer's Club* vigorously pursued people who violated the film's copyrights through illegal downloads. The plaintiff in those lawsuits argued that a violator's Internet Service Provider should reveal end-user identities, without the plaintiff having to go to court to obtain that information. The ISPs argued that the information is protected by the Australian Privacy Act. The Australian Federal Court ruled that a group of Australian ISPs had to hand over the identities of some 4,726 of their customers.

IV. ADDITIONAL RESOURCES

A. Participant Resources

1. BP P.L.C.

- Privacy Statement

2. Dell Inc.

- Privacy Statement

3. EMC Corporation

- Privacy Statement
- Privacy Speech at Tech for Justice
- Comments of EMC Corporation on FTC Staff Report on Protecting Consumer Privacy
- Information Security & Privacy in Our Operations
- Product Information Security & Privacy
- RSA Advanced Security Operations Center Solution (see use cases)
- Trusted IT Solutions for Healthcare Providers
- EMC Global Data Protection Index

4. Hewlett-Packard

- Privacy Statement
- Worldwide Privacy Statements
- Protecting privacy: Building in safeguards for personal data

5. Lawyers' Professional Indemnity Company (LAWPRO®)

- LAWPRO Privacy Code
- Code de la protection des renseignements personnels de LAWPRO
- LAWPRO's Security Policy
- Politique sur la sécurité de LAWPRO
- LAWPRO Personal Information Statement for Ontario LAWYERS
- Déclaration de LAWPRO sur l'utilisation des renseignements personnels à l'intention des avocats titulaires de permis de l'Ontario
- LAWPRO Personal Information Statement for Canadian lawyers (excluding Ontario and Quebec)
- Déclaration de LAWPRO sur l'utilisation des renseignements personnels à l'intention des avocats canadiens (l'exclusion d'Ontario et de Québec)
- LAWPRO Personal Information Statement for Quebec notaries/lawyers
- Déclaration de renseignements personnels de LAWPRO à l'intention des notaires/avocats du Québec
- Security Policy (English version)
- Security Policy (Version française)

6. Miscellaneous

- Sample Personal Data Protection Agreement (ACC)
- Practices for Secure Development of Cloud Applications (Cloud Security Alliance)
- ABA Article on Cloud Computing (Am. Bar Ass'n (ABA))
- Protecting Consumer Information in the Retail Sector (ABA)
- Security & Privacy Best Practices (Online Trust Alliance)

B. ACC Resources

Countless additional resources are available on the ACC website by searching the library. Recent articles of potential interest include, but are not limited to:

- Top Ten Emerging Privacy Litigation and Compliance Risks
- Top Ten Tips for Companies Buying Cyber Security Insurance Coverage
- U.S. Privacy and Data Security Challenges For Critical Infrastructure
- Data Breaches and Cyber Risk Update: This Can Mean You Too
- Is Privacy the Next Superfund? How to Navigate Privacy & Data Security Issues
- DLA Piper Handbook on Data Protection Laws of the World
- U.S. Online Data Privacy and Security Compliance: A Roadmap for In-house Counsel
- Sample Information Security Risk Assessment Questionnaire
- Top Ten Emerging Privacy Litigation and Compliance Risks
- Information Security Risks when "Going Cloud": How to Deal with Data Security: an EU Perspective
- Cloud Computing in eDiscovery and Information Governance
- Complying with Data Security Breach Laws

1. ACC Docket Articles

- Jeremy Otis and Hannes Saarinen, "Data Privacy in a PRISMed World: The Corporate Counsel's Perspective from Finland," ACC Docket 32, no. 5 (June 1, 2014), *available at* http://www.accdocket.com/articles/resource.cfm?show=1369272.
- Laura I. Sorafine and Colin J. Zick, "Protect Your Customers: Solutions to New Privacy and Security Regulations," *ACC Docket* 28, no. 5 (June 2010), *available at* http://www.acc.com/legalresources/resource.cfm?show=928911.
- Carol A. DiBattiste and James E. Lee, "Trust, But Verify: The Reality of Data Protection in an Information-Driven World," *ACC Docket* 26, no. 4 (May 2008), *available at* http://www.acc.com/legalresources/resource.cfm?show=14335.

- Michael C. Lamb and Ronald I. Raether, Jr., "Defining Data Security Measures That Protect Your Company and Customers," *ACC Docket* 25, no. 10 (Dec. 2007), *available at* http://www.acc.com/legalresources/resource.cfm?show=14419.
- Adam Palmer and Tim S. McClain, "New to In-House: Data Security in a Digital World," *ACC Docket* 25, no. 8 (Oct. 2007): 20, *available at* http://www.acc.com/legalresources/resource.cfm?show=14444.
- Amy L. Halverson and Rebecca A. Askew, "Online Privacy," *ACCA Docket* 20, no. 2 (Feb. 2002): 62-75, *available at* http://www.acc.com/legalresources/resource.cfm?show=148525.

2. ACC Annual Meeting Materials

- Jon Leibowitz ET AL., "Is Privacy the Next Superfund? How To Navigate Privacy and Data Security Issues," ACC 2007 Annual Meeting, Session 410, *available at* http://www.acc.com/legalresources/resource.cfm?show=19931.
- Lael Bellamy ET AL., "Privacy, Spam, and Spyware 2006," ACC 2006 Annual Meeting, Session 311, *available at* http://www.acc.com/legalresources/resource.cfm?show=20131.
- J. Michael De Janes ET AL., "Leading the Way in Privacy and Data Security Compliance," ACC 2006 Annual Meeting, Session 502, *available at* http://www.acc.com/legalresources/resource.cfm?show=20115.
- Jeffrey D. Adelman ET AL., "Pitfalls and Landmines in Privacy and the Collection, Use, and Security of Personal Information," ACC 2005 Annual Meeting, Session 110, *available at* http://www.acc.com/legalresources/resource.cfm?show=20343.
- James R. Beyer ET AL., "Workplace Privacy," ACC 2005 Annual Meeting, Session 306, *available at* http://www.acc.com/legalresources/resource.cfm?show=20316.
- Paula Barrett ET AL., "International Privacy Law," ACC 2004 Annual Meeting, Session 103, *available at* http://www.acc.com/legalresources/resource.cfm?show=20445.

3. ACC InfoPAKs

- "Big Data" in Healthcare: Legal and Regulatory Considerations in the Path to Monetization," ACC InfoPAK (April 2015), *available at* http://www.acc.com/legalresources/resource.cfm?show=1400026
- "Email and Internet Policies," ACC InfoPAK (Feb. 2007), *available at* http://www.acc.com/legalresources/resource.cfm?show=19683.

4. Other ACC Resources

- "Privacy and Data Protection in Europe," ACC QuickCounsel (May 2010), *available at* http://www.acc.com/legalresources/quickcounsel/papie.cfm.
- "Data Privacy and Protection: EU as Compared with U.S.," ACC QuickCounsel (Apr. 2010), *available at* http://www.acc.com/legalresources/quickcounsel/dpapeacwu.cfm.
- Coudert Brothers LLP, "Data Protection Surveys for EU Member States" (Aug. 2003), *available at* http://www.acc.com/legalresources/resource.cfm?show=16739.
- White & Case LLP, "Global Privacy Law: A Survey of 15 Major Jurisdictions" (Apr. 2002), *available at* http://www.acc.com/legalresources/resource.cfm?show=16325.
- Seyfarth Shaw, "Privacy in the Workplace" (Mar. 2002), *available at* http://www.acc.com/legalresources/resource.cfm?show=144385.

C. Outside Resources

1. Government Resources

- U.S.-EU Safe Harbor Framework, http://export.gov/safeharbor/.
- European Commission, Data Protection page, http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm/.
- European Data Protection Supervisor, http://www.edps.europa.eu/EDPSWEB/.
- "Binding Corporate Rules Frequently Asked Questions," Information Commissioner's Office (United Kingdom), *available at* http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_ guides/ico_bcr_faqs_v1.1.pdf.

2. Privacy Organizations

- International Association of Privacy Professionals, https://www.privacyassociation.org/.
- Electronic Privacy Information Center, http://epic.org/.
- Ponemon Institute, http://www.ponemon.org/.
- Privacy International, http://www.privacyinternational.org/.

3. Privacy Seal Programs

- BBBOnline, http://www.bbb.org/us/business/.
- TRUSTe, http://www.truste.com/.

- WebTrust, http://www.webtrust.net/.

4. Privacy Publications

- BNA Privacy Law Watch, http://www.bna.com/products/ip/pwdm.htm.
- IAPP Daily Dashboard, https://www.privacyassociation.org/publications/daily_dashboard/.
- Privacy Laws & Business International, http://www.privacylaws.co.uk/templates/Publications.aspx?id=299.
- Privacy Journal, http://www.privacyjournal.net/newsletter.htm.

V. ENDNOTES

[i] See more at http://www8.hp.com/us/en/hp-information/global-citizenship/society/privacy.html.

[ii] See more at http://informationaccountability.org/.