

Conference Report

CONFERENCE ON CROSS BORDER DATA FLOWS, DATA PROTECTION, AND PRIVACY

Washington, D.C., October 15-16, 2007

Conference Organizers:



U.S. Department
of Commerce



European Commission
Article 29 Working Party
on Data Protection

TABLE OF CONTENTS

Executive Summary	1
Introduction.....	4
Welcoming Remarks.....	4
Opening Remarks.....	5
Keynote Address.....	7
Panel I: Workshop on the U.S.-E.U. Safe Harbor Framework	9
Panel II: Global Sourcing and Data Flows – Compliance and Security in the Global Economy	13
Panel III: The European Union’s Data Protection Framework – 12 Years Later: Intra-E.U. Data Flows, Adequacy, and the Role of the Article 29 Working Party on Data Protection	17
Panel IV: Implementing and Enforcing Corporate Privacy Rules	22
Panel V: Binding Corporate Rules (BCRs) and Contractual Clauses – The European Union’s Context.....	23
Closing Remarks.....	26
Conclusion and Recommendations.....	26
Appendix A: Agenda	28
Appendix B: Speaker and Panelist Biographies	31

EXECUTIVE SUMMARY

International data flows are an integral and expanding part of the modern economy. The proliferation of digital data, the explosion of new communications technologies, and the globalization of corporations and markets are key drivers in this expansion. But while global data flows are an essential part of commerce, they also hold great significance for the safety and security of businesses and consumers alike.

Global data flows require corporations and regulators to seek the balance between facilitating the expansion of international trade and protecting personal privacy rights. In the last 30 years, several privacy protection instruments have been adopted internationally, one of which is the European Union (E.U.) Data Protection Directive (Directive 95/46/EC of 24 October 1995, “the Directive”). The Directive establishes a comprehensive legal framework and fundamental principles for processing data, providing E.U. member states with the authority to block transfers to countries whose privacy enforcement regime does not meet the Directive’s adequacy requirements. It also gives the national data protection authorities necessary powers via national implementation laws to enforce compliance. The Directive is widely considered a success in Europe, but as new technologies continually flatten the globe, the E.U. aims to guide the evolution of global privacy principles with an E.U.-centric model.

To advance cooperation between the E.U and the United States, both parties have agreed to regular consultations and information exchanges. The Conference on Cross Border Data Flows, Data Protection, and Privacy is part of this bilateral commitment regarding the agreement on transfers of personal data from the European Union to the United States known as the U.S.-E.U. Safe Harbor Framework. Under the U.S.-E.U. Safe Harbor Framework, the United States received an “adequacy” determination from the European Commission limited to those U.S. organizations that self-certified to Safe Harbor.

The conference focused on the challenges posed by cross-border data flows and how the U.S. and E.U. work with the private sector to promote such data flows, protect consumer privacy, and build consumer confidence in the global economy. Leading experts in the privacy compliance field presented case studies of organizations that are participants in Safe Harbor, and of those that have employed binding corporate rules as the principal instrument for complying with the Directive. The conference also examined current data protection efforts in Asia and discussed ways to enhance collaboration in the context of the Safe Harbor framework. Through in-depth panel discussions about the following topics, the conference highlighted the need for ongoing collaboration and continued discussion in order to improve the security of data flows worldwide.

WORKSHOP ON THE U.S. – E.U. SAFE HARBOR FRAMEWORK

This discussion provided the historical context to the evolution of the legal framework for privacy in the European Union. It also evaluated data security and Safe Harbor certification from the perspectives of both companies and regulators. The panel addressed issues of trust in the digital economy through a discussion of advocacy and certification organizations such as TRUSTe, and by providing the corporate example of Intel, whose mission involves creating an

environment where people can trust technology. In this context, Safe Harbor is a vital mechanism that will be the foundation for continued dialogue in the future.

GLOBAL SOURCING AND DATA FLOWS – COMPLIANCE AND SECURITY IN THE GLOBAL ECONOMY

This panel explored how multi-lateral flows of data relate to modern global business processes. In today's economy, privacy enforcement systems based on accountability encourage both protection and productivity. Corporate representatives from IBM, Schering Plough, Accenture, and Procter & Gamble spoke about global data flows in the context of how businesses operate in the global technological landscape. In developing privacy programs, global corporations can create an environment of trust and confidence, therefore deepening the customer relationship. From the perspective of a service provider, outsourcing is an important consideration in evaluating the benefits of territorial regulatory regimes versus one unified data regime. Above all, the company plays a role as an agent of accountability, and Safe Harbor is a key accountability mechanism.

THE EUROPEAN UNION'S DATA PROTECTION FRAMEWORK – 12 YEARS LATER: INTRA-E.U. DATA FLOWS, ADEQUACY, AND THE ROLE OF THE ARTICLE 29 WORKING PARTY ON DATA PROTECTION

The E.U.'s Data Protection Directive aims to harmonize the data protection standards in all member states, but also to respect the different legal structures of the nations. The main task of the Article 29 Working Party is to organize data protection in the member states and safeguard this fundamental right of European citizens. This panel focused on the rules and instruments of the European legal system in the area of data protection, addressing the enforcement powers and challenges of national data protection authorities, and providing a specific example of auditing and enforcement at the Spanish DPA. It also addressed data transfers from the perspective of a Safe Harbor member and AMCHAM E.U. Member. Finally, it examined data protection from the perspective of a third-party country and emphasized the need for continued collaboration on an even broader scale.

IMPLEMENTING AND ENFORCING CORPORATE PRIVACY RULES

This panel combined several topics in a discussion of a hypothetical situation focused on how data protection initiatives work on a global basis for companies in countries outside the E.U. Although accountability models are designed to work, many questions of jurisdiction can cripple the enforcement process. In light of such complications, the consumer likely does not know how to seek redress, and as such, an alternative model could be beneficial. Companies and regulators must increase cooperation to make Binding Corporate Rules (BCRs) more effective.

BINDING CORPORATE RULES (BCRs) AND CONTRACTUAL CLAUSES – THE EUROPEAN UNION'S CONTEXT

This panel discussed the differences between participation in Safe Harbor and compliance with BCRs. It also addressed contractual clauses, which face difficulties due to the wide variety of

applications throughout the E.U., and the resulting challenge for multi-party situations. The panel discussed the corporate examples of General Electric, which uses BCRs and internal enforcement to provide strong, global data protection. BCRs can benefit companies and DPAs alike by providing a unified, in-house, global standard, and by creating a simplified approval process and a clearer enforcement role. Finally, the panel examined methods outside the E.U., in Asia, where APEC is developing Cross Border Privacy Rules (CBPRs). The commonalities between BCRs and CBPRs hint at global corporate best practice for data protection, but to implement these instruments we must continue to share resources and knowledge.

INTRODUCTION

The U.S.-E.U. Safe Harbor Framework is a bilateral commitment governing transfers of personal data from the European Union to the United States. In support of this agreement, government and private sector representatives from the U.S., E.U., and other nations met in Washington, D. C. on October 16-17, 2007 for the Conference on Cross Border Data Flows, Data Protection, and Privacy, hosted by the U.S. Department of Commerce. The Conference enabled continued cooperation between the European Commission and the United States in their joint efforts to facilitate understanding, improve oversight, and discuss related data protection issues and opportunities. Through speakers, panel discussions, and corporate case studies, the Conference helped data privacy leaders review compliance with privacy frameworks, address challenges posed by cross-border data flows, and renew commitment for continued dialogue on data privacy.

WELCOMING REMARKS

To begin the Conference, officials from the Federal Trade Commission, the U.S. Department of Commerce, the European Commission, and the Indiana University Center for Applied Cybersecurity Research gave brief addresses to the audience. Each speaker discussed key principles and initiatives at his or her organization in the context of Safe Harbor and future global data privacy programs.

Lydia Parnes, Director, Bureau of Consumer Protection, Federal Trade Commission (FTC)

In her welcoming remarks, Ms. Parnes discussed how the conference would be focused on the challenges posed by cross-border data flows and how the U.S. and E.U. work with the private sector to promote such data flows, protect consumer privacy, and build consumer confidence in the global economy. She explained that the conference would highlight current efforts in both places and enhance joint efforts in the context of the Safe Harbor framework.

According to Ms. Parnes, privacy and data security are top priorities for the FTC, and the organization devotes substantial resources and energy to enforcement in these areas. As part of this work, the FTC is committed to its enforcement role in the Safe Harbor Framework, and it especially appreciates the chance to participate in this dialogue about cross-border data flows. Ms. Parnes explained that the message she always tries to convey is the great need for enforcement. In the last several years, the FTC has brought 14 law enforcement actions involving data security, which set out four general lessons for companies.

1. If you make a claim about data security, be sure that it is accurate.
2. Be aware of well-known and common security threats, and protect against them.

3. Know with whom you are sharing your customers' sensitive information.
4. Do not retain sensitive customer information that you do not need.

She then highlighted two recent FTC initiatives in two new areas: education and research.

Education

The FTC has an extensive program to educate consumers and businesses about privacy. Last year it launched a consumer education campaign urging consumers to deter, detect, and defend themselves against identity theft. Earlier this year, the FTC launched a popular new business guide, which articulates key steps businesses should take to implement a good data security plan.

Research

The FTC will host two workshops in the next few months on the following subjects:

1. November 1-2: Behavioral Advertising – how it works and online data collection practices.
2. December 10-11: The Use of Social Security Numbers by the Private Sector – domestically and internationally focused on how to promote the beneficial use of personal data without compromising privacy.

OPENING REMARKS

Michelle O'Neill, Deputy Under Secretary for International Trade, U.S. Dept. of Commerce

Ms. O'Neill expressed her appreciation to meeting attendees for their participation at the conference and in the Safe Harbor initiative, which has more than 1,300 members. She discussed her participation in a government-to-government discussion that morning. The discussion underscored the fact that many questions persist and that all Safe Harbor participants can benefit from more dialogue. Ms. O'Neill stated that DOC is looking at ways to continue the dialogue in a government-to-government context and that those gathered are important stakeholders, both in the agreement, and as participants in additional mechanisms to implement the E.U. directive.

Jonathan Faull, Director General for Justice, Freedom, and Security

In his opening remarks, Mr. Faull described how several instruments have been adopted internationally in the last 30 years. Some are legally binding, some are not, but their principles provide an excellent framework for data privacy. In the E.U., the Data Protection Directive establishes a comprehensive legal framework and sets out the fundamental principles for processing data. It also gives the appropriate authorities the necessary powers to enforce

compliance. But since the E.U. is part of the larger world, it must establish rules for an increasingly global and interlinked environment.

The E.U. Data Protection Directive confronts tensions between the needs of expanding international trade and the need for privacy. Transfers of personal data from the E.U. to a foreign country are possible where that country offers an adequate level of protection. This is a fundamental rule. If a country does not offer adequate protections, transfers may still be possible through the use of contracts, which are often used in the case of developing countries. The European regime for international transfers can be seen as a source of concern by E.U. trading partners, who might fear that data flows could be cut off at any time. This, however, is a misunderstanding. The E.U. makes every effort to bridge this gap.

The goal of the European Commission's data privacy initiatives is to provide organizations with different mechanisms to fit their needs and conduct their activities in an interlinked international environment, while ensuring the protection of data subjects and their fundamental rights. Safe Harbor is an instrument developed with the U.S. to create an area for adequate protection for data flows between the E.U. and the U.S. Reports from 2002 and 2005 show that the system is working well and they recommend strengthening it. A new report will be presented in 2007. On the Data Protection Directive itself, the E.U. authorities found in a meeting last March that it continues to provide good responses and that the general principles remain valid. Therefore, there is no need to modify the Directive at this stage, but it will remain continually under review in light of the many challenges facing the E.U. in this area.

The main challenges are ones of practical implementation. Mr. Faull discussed two of them:

1. The explosion of new information technologies

There has been some talk of a worldwide instrument on privacy, and it is worth exploring although it could be difficult to implement. The European Commission continues to work on contractual solutions for international transfers. New information and communication technologies can make life easier, but they carry risks as well, such as identity theft, discriminatory profiling, and deceit. Therefore, the European Commission is developing a series of Privacy Enhancing Technologies, which minimize collection of personal data and facilitate compliance with data protection rules. These technologies would make breaches of rules more difficult and would increase consumer confidence.

2. The tension between the right to privacy and the prevention of terrorism and organized crime.

These are conflicting interests. Law enforcement authorities need sensitive information about individuals. Compliance with the right to privacy should not be seen as an obstacle, but rather as a partner. The E.U. is considering new laws and engaging with the U.S. in continuous dialogue. A high-level group has been created to study data protection policies and systems to find commonalities and differences. What we find is that the differences are ones of implementation and application, not ones of basic principles and objectives. This work could pave the way for further participation between the E.U. and the U.S. Other measures will remain necessary in

parallel. We are also constantly exploring ways to meet the challenges of stakeholders in this area, and the current process of reform in the E.U. will make these efforts easier if a new treaty enters into force in the E.U.

KEYNOTE ADDRESS

Fred H. Cate, Distinguished Professor and Director, Indiana University Center for Applied Cybersecurity Research

In his keynote address, Dr. Cate explained that participants have much to celebrate, namely the 12th anniversary of the passage of the E.U. Data Protection Directive and the 7th anniversary of the Safe Harbor. He said that the group has facilitated the movement of a vast amount of data and helped diffuse several controversies.

However, according to Dr. Cate, it is unclear that any data privacy and protection issues have actually been solved. Instead, what we have are workable accommodations, some of which are tenuous or narrow. For example, the Safe Harbor does not extend to the financial services industry, telecommunications common carriers, or insurance companies. Further, many issues are still on the table including the surveillance of European communication, and the emerging conflict between U.S. civil discovery, law, and needed data protection.

Dr. Cate's goal was to talk about two closely interrelated challenges that should be of greatest concern to the group:

1. The proliferation of digital data

In 2006, 161 exabytes (1 billion gigabytes or 1,000 feet of books for every person on Earth) of information were created and the quantity of this data is increasing dramatically. What's more, the vast majority of this data is digital. What does it mean for this data to be digital? Digital data has come to define our lives by capturing detailed information about our behavior, thoughts, and backgrounds. Moreover, not only are these data digital and growing, but there are multiple copies of these data. The absolute critical function in making these data useful are that these data are held on interconnected systems. The most obvious example is the Internet, to which most people do not connect directly, but rather through networks of networks, so we are seeing an increasingly networked society. Add to this, technologies such as wireless devices, cell phones, and sensor networks, all of which are collecting and sharing data in an automatically interconnected environment. Indeed, reliable interconnectivity is so important that it has become part of our business and personal backbone, as evidenced by the vast amount of remote storage. But remote storage tends to alienate people from their data because it is no longer in the owner's hands, but in someone else's.

This obviously poses significant challenges to data protection law. We tend to give notice and choice to individuals who in fact have little control over their data. Further, because digital data

is easy and inexpensive to store, we tend to store it forever. Digital data is also very functional, and its utility is enhanced by the proliferation of tools we create to use it. This means we have increased the usefulness of this data, but also increased the security issues and threats as well. Digitalization has improved the speed with which we can move data, but also the speed with which we can move data surreptitiously. Perhaps most significant is that the cost to store and transit data today has effectively reached zero.

2. The expansion of global data flows

All of these aforementioned attributes have made possible the globalization of data flows. It is not just the U.S. and Europe – the Internet is the backbone of our activities in more than 200 countries. The expansion of multinational companies and the tremendous growth of outsourcing are made possible by these technological developments. Perhaps most important is the increased interest shown by new countries in the data protection field, particularly China and India. The types of data protection measures these countries implement is tremendously important because of the amount of our data that will be stored there, not to mention the number of people who live there.

In general, external borders and the physical locations of processing operations are less relevant. We are absolutely dependent on these data flows, and the free flow of information between member states, and between member states and third-party countries, will become more and more important in the future.

What should we do in light of these developments? We have built powerful data protection tools and edifices, but they already appear increasingly outdated and vulnerable. The old data protection regime seems ill-suited and inapplicable to the Web. Many authorities are not interested in privacy to the exclusion of other interests. Moreover, notice and choice tools are proving increasingly intellectually dishonest – we may talk of consent, but it is absent. The U.S. and E.U. both struggle with this. In the U.S., we have glorified notice and choice to the exclusion of all other principles, even though we know that consumers do not understand or act on them. There has been little consumer response to the billions of privacy notices mailed under the Graham Leach Bliley Act, and yet notices remain our primary legal response.

The U.S. government has engaged in vast data surveillance efforts in and out of the country, often by co-opting the private sector. Even before 9/11, the head of the National Security Agency testified that the NSA received more than 650 million communications intercepts per day. In total, it is difficult to fathom the amount of data in the government's hands, and even more difficult to believe that it is protecting it well. It is difficult to tell, but the same might be true in Europe as well.

Despite all of our collected efforts, it is not at all clear that privacy is better protected than it was a decade ago, due mainly to the growth of digital data and global information flows. The situation does not appear to be getting better, and Dr. Cate believes that we are losing the data protection arms race.

How do we resolve these problems? Officials in the U.S. and Europe are already working on initiatives to make privacy protections more substantive, efficient, and responsive – many of these will be discussed during this conference – and Dr. Cate enthusiastically endorses these efforts. He also urges the group to keep in mind the global nature of data flows and the need for a truly global data protection infrastructure. Information flows were the subject of the earliest treaties we know. A good approach may be suggested by the APEC privacy framework, under which nations adopt divergent data protection laws based on common principles and features national data protection authorities dealing with each other.

Whatever the approach, we must avoid a one-size-fits-all approach because at heart privacy is a local issue that reflects different cultures, standards, and institutions. The focus should be on a collaborative enforcement model – like the Safe Harbor – but on a global rather than bi-national level. What matters is that individuals have good reason to believe that their data is under control, that they are protected against illicit use, and that they are officially available to serve their needs on demand, that they have accessible redress if these expectations are violated, and that these expectations apply irrespective of where the data or the individuals are located.

PANEL I: WORKSHOP ON THE U.S.-E.U. SAFE HARBOR FRAMEWORK

This panel discussed the evolution of the legal framework for privacy in the European Union. It also evaluated the issues of data security and trust in the digital economy through a discussion of Safe Harbor certification, independent certification organizations, and corporate examples.

Damon Greer, Safe Harbor Program

Mr. Greer provided some historic context to the evolution of the legal framework for privacy in the European Union. Data collection has been around forever, but modern technology is the reason for protection efforts.

There are different approaches to data privacy. The European Union’s overarching Data Protection Directive creates a barrier for those countries, including the U.S., that do not meet the E.U.’s “adequacy” requirements. The U.S. Department of Commerce and the European Commission negotiated the Safe Harbor to provide U.S. companies with a simple, streamlined means of complying with the adequacy requirement. This is crucial because of the volume of trans-Atlantic trade, which in 2006 reached \$630 billion. Safe Harbor has seven key principles: Notice, Choice, Security, Onward Transfer, Data Integrity, Access, and Enforcement.

In general, enforcement will take place in the U.S., where the culture of customer service is highly effective in addressing customer complaints and concerns, perhaps more so than comprehensive legislation. Independent recourse mechanisms are required to notify DOC of a company’s failure to comply with the Safe Harbor principles, and FTC has authority to take action. The results are that no referrals and no complaints have been filed with the E.U. DPAs. Further, TRUSTe, BBB, DMA, and others report that internal complaints have been resolved.

Joining Safe Harbor is not the only means of meeting the E.U. Directive's requirements. These are the Article 26 derogations:

- "Unambiguous" consent
- Necessary to perform contract
- Codes of conduct
- Model contract clauses
- Direct compliance/registration with E.U. Authorities

Since 2000, we have built credibility and confidence in Safe Harbor as demonstrated by the fact that in November 2000 there were six Safe Harbor companies, and today we are approaching 1,300 organizations, and averaging 35 new members per month.

Moving forward, we need expanded dialogue with the European Commission. Further, the E.U. must work to harmonize the Data Directive and educate data subjects. Also, industry must increase emphasis on harmonizing the approval process for binding corporate rules. Today, more than 70 nations have some form of data protection/privacy framework, and more plan to enact data protection or privacy legislation.

Joan Antokol, Partner, Baker & Daniels, LLP

Ms. Antokol spoke on Safe Harbor certification from the company perspective. An increasing number of U.S. companies are certifying to the Safe Harbor for various reasons including knowledge of sweeping enforcement, as in the SWIFT case; prompting from E.U. affiliates; need for global human resource databases; and increased awareness about the business advantages of certifying. In the U.S., the perception is that the FTC may not be doing enough in terms of enforcement, but that is not the case.

Some of the hesitations companies have with regard to Safe Harbor include:

- Lack of perceived need.
- Limited staff, and attorneys are already overburdened. They seem to think that if they open the door a little bit, then they will be responsible if there is a violation. This is the biggest reason.
- Uncertainty about how to begin.
- Lack of knowledge about the benefits to certifying.

Some considerations for companies in deciding whether to certify or not are the following:

- Current status of database registrations.
- Overall data transfer compliance.
- Plans for a global human resource database/remote HR managers.
- Ongoing business plan/globalization.
- Privacy/security landscape.

How costly and complicated is certification for Safe Harbor? Is it worth it? It depends on your progress in terms of data certification, and how many data transfers you have. The company must evaluate this. Ms. Antokol has prepared booklets and materials to help clients understand Safe Harbor better.

There are five key certification steps:

- Preparation, pre-launch stage
- Gap assessment (charting data flows, finding where to implement corrective action)
- Evaluation and analysis (implementation of processes and procedures)
- Launch
- Post certification (ongoing compliance)

The business advantages of certifying are many. A company can bring databases into compliance much more rapidly if the company is certified. It can increase efficiency by putting global standards in place. Further, it can bolster its reputation, save costs, and create competitive advantage by being able to launch global projects faster than competitors. For these reasons it is beneficial for most companies to consider Safe Harbor certification, which can be a simple process.

Martha Landesberg, Director of Policy & Counsel, TRUSTe

This presentation was a compliance and enforcement update on TRUSTe's E.U. Safe Harbor Seal Program. TRUSTe is an independent non-profit focused on advancing privacy and trust for the networked world. Its E.U. Safe Harbor Seal Program was launched in 2000 and now has 130 licensees with 317 websites, and 14 new Sealholders in 2007.

The TRUSTe E.U. Safe Harbor Program Certification Process has several steps:

- Strict Standards Incorporate all Safe Harbor Privacy Principles
- Detailed Self-Assessment + Rigorous TRUSTe Review
 - o Web site audit
 - o Access reputation and other data
 - o Revision of policy and practice
- Transparent Privacy Statement
 - o Sealholder states adherence to principles
 - o Clear notice of complaint mechanism
- Seals Awarded and Displayed
- Ongoing Monitoring & Dispute Resolution
- Annual Recertification Required

TRUSTe offers translation services for company privacy statements. They also field about 200 complaints per year, typically about spam, being unable to close an account, phishing, spyware, and inability to correct data. TRUSTe believes that its job is to work with its companies to keep them compliant. In terms of compliance and enforcement, key tools are certification, watchdog dispute resolution, and proactive monitoring. Its enforcement options include declining to recertify, suspending the company, or terminating its certification. The overall goal is to help

companies that want to do the right thing put themselves in that position, and to bring to light the bad actors.

Hugh Stevenson, Deputy Director for International Consumer Protection, Federal Trade Commission

Mr. Stevenson presented the regulators' perspective on the issues of data security. The basic, organic role of the FTC is enforcement. Companies can choose voluntarily to self-certify with Safe Harbor, and failure to comply can subject them to penalties. FTC jurisdiction is quite broad and, within the areas it covers, it has the tools to investigate, get relevant documents and statements, and develop a full investigation. The FTC also has tools to take action and stop bad practices.

Two points to keep in mind when considering how this enforcement regime works:

- 1) Keep the FTC enforcement role in context as one of several supporting players. Enforcement is not a lightning bolt, but just one measure among many measures to ensure compliance. Data can be transferred so quickly, in so many ways, that we must develop measures going forward with this large scope in mind.
- 2) We must bear in mind the overall context of privacy enforcement internationally. We have studied a layered approach, and we need a cooperative effort in the future to improve enforcement. We want to continue to strengthen our relationship with international enforcement authorities. In the U.S., we have a good set of tools – the one thing we have focused on recently, and will continue to focus on, is enhancing these tools for international cooperation.

David Hoffman, Chief Privacy Officer, Intel Corporation

Mr. Hoffman spoke on international data transfer and trust in the digital economy. He chose this topic particularly because of Intel's mission, which involves trying to create an environment where it is reasonable to get people to trust technology. Growth requires trust in technology and how data is processed.

He presented the "Triangle of Trust," which is a model for an environment where regulators, privacy seal organizations, and corporate compliance all come together. He believes that the Safe Harbor program has come a long way – it was not long ago that participants were stuck in a debate about the regulatory model (E.U.) versus the self-regulatory model (U.S.). In terms of the Safe Harbor agreement, such a triangle model seems to be working.

One of the backstops of the agreement is enforcement (or the threat of enforcement). Going forward, it is necessary for us to focus on the individuals who have not certified. This triangle approach is good, but can we make it broader? We all must do more outreach, and a key upcoming event is Data Privacy Day in North America in January 2008.

Giovanni Buttarelli, Secretary General, IT Garante (Italian Data Protection Authority)

Safe Harbor is the first data privacy instrument on which Europe has focused its attention, and after seven years, Safe Harbor has not lost its vitality.

Some issues raised in the past include transparency requirements, the functioning of dispute resolution mechanisms, the transparency of the relevant outcomes, the integration of the Safe Harbor Workbook, and the difficulties that may arise from the existence of multiple privacy policies declared by the same operator.

Are we struggling? Europeans tend to look with great concern on current arrangements, bordering on pessimism (unlike the U.S.). There is a need for getting the full picture in terms of data, figures, and information. Mr. Buttarelli has no criticism to raise against Safe Harbor, but he is not in a position to say that the agreements have provided us with comprehensive safeguards. He also raised the question of whether or not stakeholders are simply ignoring Safe Harbor and continuing their operations as usual.

Europeans do not have a full picture about what is happening in areas where Safe Harbor is applied. Some of the issues raised in the past include:

- Visibility of Harborites' privacy statements
- Legal status of the U.S. entities involved in data transfers (controllers or processors)
- Clarifying some key concepts such as "anonymous data" or "aggregate data"
- Awareness by human resources of their rights and recourse options
- Desirability of jointly waging educational campaigns

In the future, we must continue dialogue. The European Commission is about to submit a new report on Safe Harbor. He reiterated the need to set up a discussion forum on Safe Harbor that is open to the public. While we may not revise our separate regulations in the immediate short term, we should meet (not in a typical convention) to develop shared rules.

October 16, 2007, 2nd Day

PANEL II: Global Sourcing and Data Flows – Compliance and Security in the Global Economy

This panel explored how multi-lateral flows of data relate to modern global business processes. Through a discussion of their own privacy enforcement systems, corporate representatives from IBM, Schering Plough, Accenture, and Procter & Gamble spoke about how protecting data flows can help businesses operate in the global technological landscape.

Marty Abrams, Executive Director, Center for Information Policy Leadership (CIPL)

Mr. Abrams explained that the objectives of this panel were to explore multi-lateral flows of data; to discuss how these relate to modern business processes that are global, distributed, and based on teaming; and to discuss how privacy enforcement systems based on accountability encourage both protection and productivity.

Today, we see information being used more robustly. Computers are helping to expand the amount of data that we can process. Emerging economies are generating growth via knowledge-based employment. Communications improvements mean that work will be done where it is most efficient to do it – therefore, data will be moving there. And data transfers mean immediate customer service, international payment processing, business process re-engineering, global project teaming, and social networking in a global community.

There is an emerging model of governance. Privacy has many aspects, but it is a local phenomenon, and we must respect unique cultures and the accompanying cultural sensitivities. At the same time, data flows are global, and obligations are universal, so we must respect business deals regardless of where the data is processed. This leads to the concept of accountability-based systems of governance, which we are already seeing emerge, and with them the growth of accountability agents and methods.

Harriet Pearson, Chief Privacy Officer, IBM Corporation

Ms. Pearson spoke about global data flows in the context of how businesses are operating in the larger global technological landscape. She demonstrated five historical waves of economic and social transformation. The global economy has now entered the deployment phase of the fifth technology investment cycle of the past 250 years, which is the Age of Information and Telecommunications. Global economic activity since the advent of the industrial revolution has been dominated by five 40-60 year cycles or waves that are characterized by alternating periods of invention when investment spending slows, and periods of deployment when investment spending and productivity growth is more rapid. This will be a period of adjustment when novel business models will exploit the new IT infrastructure that is now being put in place. These business models enable more porous, open, collaborative approaches that seek to leverage the economics and flexibility of global sourcing.

Another way to see this transformation is by looking at Internet connectivity, which has grown tremendously since 1995. Still another way is by looking at the changing global landscape in which businesses are moving from local partnerships to global relationships. Given these trends, the individual holds more power than ever, choosing where to work, how to work, and what information to access. Enabling, harnessing, and eventually profiting from this power will be key for businesses around the globe.

To further illustrate the advantages available to firms of all sizes, witness the vast number of specialized services firms, both new and emerging, that offer very focused business execution and support services ranging from payroll to customer relations management. These services are delivered in a modular fashion that allows companies to get only what they need, when they need

it. Tapping into these services allows companies of all sizes to become globally integrated quickly and easily.

We are also seeing componentization, in which the unit of production is getting increasingly smaller. This is used to reduce complexity by splitting up a larger entity into its logical pieces, which can be recombined for higher value. For a business, this means that you can study the payroll system, for example, and take action to optimize only that system. Ongoing specialization, e.g., through outsourcing, as well as decreasing transaction costs drive broad collaboration among companies and individuals. Tools such as instant messaging, teamrooms, and virtual worlds (Second Life) support a highly productive collaborative environment for various processes. All things considered, the individual has more power than ever before to act without large investments. This new landscape has profound effects for business actions. We must consider how to configure our operations as a business to reflect this reality.

Dean Forbes, Senior Director - Global Privacy, Schering-Plough Corporation

Mr. Forbes began by describing Schering Plough, then speaking about global sourcing and teaming, and finally about Safe Harbor as a mechanism for accountability. A key part of Schering Plough's corporate mission is to earn trust every day. Global teaming in the pharmaceutical industry involves the collection of a considerable amount of sensitive data. In order to develop advantageous drugs, data flows from around the world must happen immediately. As a pharmaceutical company, there is a need to report adverse events efficiently across borders.

On the subject of governance, Mr. Forbes shifted to the subject of accountability and the company's role as an agent of accountability. When looking at the seven elements of the Safe Harbor program, the company can leverage these principles in their global business. For Schering Plough, Safe Harbor helps them set a global standard. Due diligence takes time, money, and the willingness to build disparate relationships. In a global company, systems house data from all over the world. Further, global companies are focused on identifying and addressing risks, and Mr. Forbes sees this happening more and more among pharmaceutical companies with regard to security standards. Mr. Forbes also emphasized that when a global company implements new security standards, they apply to all constituents.

Bojana Bellamy, Global Data and Privacy Leader, Accenture

Ms. Bellamy spoke about data privacy from the perspective of a service provider. Economic strength is growing in developing countries and emerging markets; outsourcing is both driving and benefiting from this shift. Much of the workforce of major multinational companies will be offshore in the years ahead. Therefore, it is necessary to talk about data privacy in the context of outsourcing.

There are two types of outsourcing: IT outsourcing and business process outsourcing. Business process outsourcing means taking a function of one company and giving it to another company.

This can occur for business functions such as HR, procurement, and e-learning, among others. IT outsourcing means application or infrastructure outsourcing. But why do people outsource? Cheaper cost and better capabilities are the key drivers.

How do we solve the data privacy issue? There is no point in looking for a legal solution to this issue because it would be too complicated and expensive. As we have increased players and actors in the data chain, we have increased commercial and legal risk. Data comes from many sources, so what rules can we apply to this disparate data? With increasing outsourcing, if we keep this current territorial regulatory regime, it may be a disadvantage. Ms. Bellamy would like to see one data regime, irrespective of where the data comes from or is processed. She would also like to see increased dialogue on the subject with clients. There is a need for a company-wide client data privacy compliance program based on the seven servicing guidelines standard. The compliance program is in place to support Accenture, but it does not mean that the client is outsourcing data privacy compliance to Accenture; this is not possible.

Jessica Rich, Assistant Director, Division of Privacy and Identity Protection, Federal Trade Commission

As a government representative, Ms. Rich spoke about the laws related to data privacy – what tools we have for privacy enforcement and management, and what challenges we face and how we can address them. She began with a reminder of the U.S. legal framework in the privacy area. The FTC is the primary federal regulator, and key to its role is Section 5 of the FTC Act, which can be applied broadly. Since the late 1990s, the FTC has used it to challenge companies on deceptive omissions, harmful spam, spyware, pretexting, failure to provide reasonable security, changing a privacy policy and failing to honor promises made when the data was collected, and other topics. In addition to Section 5, there are a variety of sector-specific laws governing privacy: the Graham Leach Bliley Act, the Fair Credit Reporting Act, and the Children’s Online Protection Act, among others. In addition, our laws now include the U.S. Safeweb Act, which complements existing laws by giving us new powers in cross-border situations and addressing information sharing, investigative assistance, and confidentiality.

In the context of service providers, the FTC expects U.S. protections to flow with the data. Safeweb is another very powerful cross-border tool that expands the FTC’s ability to follow data and pursue enforcement wherever the data lands. Revisiting Section 5, this tool can be used in developing new and creative methods to address cross-border issues. Although the APEC cross-border framework is still under development, we expect that Section 5 and the FTC’s enforcement role will be crucial to promoting accountability and compliance with this framework. Going forward in this changing world, we must think creatively about how to manage and regulate privacy. We must be open to new models, both regulatory and self-regulatory, that expand our reach and accomplish what no country can do alone through traditional single-country enforcement. These models, however, must be tied back to law to ensure enforceability, and the FTC Act allows us to develop such models while ensuring meaningful protections for consumers.

Sandy Hughes, Chief Privacy Officer, Procter & Gamble, Inc.

Ms. Hughes spoke about Procter & Gamble's (P&G) data privacy program. P&G has worldwide operations that require a global outlook and global implementation; above all, the consumer is boss. Its privacy program is based on creating an environment of trust and confidence, and developing a relationship with customers – the more trust, the more information customers share, and therefore the better P&G can meet their needs. Therefore P&G has one overarching privacy policy governing all personal information provided to P&G (shareholder, recruiting, customers, etc.) anywhere in the world, through any channel.

How do we make sure this privacy program is implemented? It starts with the corporate organization. The majority of the implementation work is performed through the Global Privacy Counsel, which features a leader for each type of data P&G collects. These people (about 45 in number) implement the company's specific policies and controls.

To build privacy into operations, P&G includes it in its conduct manual, provides general privacy training, includes it in its general operations controls and general audits, collects consumer comments, and reports measures to keep it visible. By having global standards, P&G can increase productivity by broadly applying decisions.

The key for P&G is that Safe Harbor matches its global privacy program. It may be easier for P&G because it focuses on one industry sector and has no financial services units, but the benefits of its program erode as countries become more different in their regulatory requirements. P&G may be a trusted company, but it still strives to have the best privacy program and the best controls, an effort that requires constant diligence.

PANEL III: The European Union's Data Protection Framework – 12 Years Later: Intra-E.U. Data Flows, Adequacy, and the Role of the Article 29 Working Party on Data Protection

This panel examined the E.U.'s Data Protection Directive and its efforts to harmonize the data protection standards in all member states, in light of different national legal structures. It focused on the rules and instruments of enforcement, the challenges of national data protection authorities, and specific examples of auditing and enforcement.

Peter Schaar, Chairman, Article 29 Working Party

Mr. Schaar explained that the improvement of the European market was one of the main motivations for the Commission to adopt the Data Protection Directive in 1995. The Directive aims to harmonize the data protection standards in all member states, but also to respect the different legal structures of the nations. He said that the main task of the Working Party is to organize data protection in the member states and safeguard the fundamental rights of now more than 500 million European citizens. Europe views data protection as a civil right, included in the

European constitution. This panel focused on the rules and instruments that the European legal system provides in the area of data protection.

Giovanni Butarelli, Secretary General, IT Garante

Mr. Butarelli described how, in the E.U., data protection is a real, fundamental, legal right. The data protection regime is wider than traditional privacy protections. The data subject has a right to see that his data are processed fairly.

Under Article 8, everyone has the right to the protection of personal data. Further, such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate legal basis laid down by law. Everyone has the right of access to data that has been collected concerning himself, and the right to have it rectified. Compliance with these rules is subject to control by an independent authority.

E.U. Data Protection Directive 95/46/EC

- The objective is to ensure a high level of protection of personal data
- It also enables free movement of data within the E.U./EEA
- Personal data: identified or identifiable
- Article 7 of the directive makes it applicable to the public and private sectors and presents some guidelines for the relationship between a controller and processor.

Personal data means any information relating to an identified or identifiable natural person. Processing of personal data means any operation or set of operations that is performed upon personal data, whether or not by automatic means. Processing means more than collection. Key principles in data collection and protection are legitimacy, quality, finality, and proportionality. The processing of sensitive data is in principle prohibited.

The rights of the individual include access to one's own data, rectification, objection, and complaint to the Data Protection Authority. The controller's obligations include the responsibility for the exercise of a data subject's rights, confidentiality and security of processing, notification to the data protection authority, and liability.

The E.U. is not only dealing with its European system – it also monitors external developments. It supports the development of universal international protection standards, and the recommendation that it is not practical to amend 95/46 at the moment. As noted at the International Conference in Montreal in September, the E.U. encourages data protection commissioners to further develop their existing efforts to support international cooperation and to work with international organizations to strengthen data protection worldwide.

Gary Davis, Ireland Deputy Data Protection Commissioner

Mr. Davis spoke about the enforcement powers of national data protection authorities. There are two E.U./EEA directives they enforce on a regular basis: Directive 95/46/EC (Protection of

Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data) and Directive 2002/58/EC (Privacy and Electronic Communications).

Enforcement obligations that come from Directive 95/46/EC include judicial remedy for individuals, entitlement for person to receive compensation, effective sanctions for breach of provisions, independent authority(s) in MS responsible for monitoring national provisions, and codes of conduct to be encouraged to contribute to implementation.

The powers provided by Article 28 include investigative powers (access to data and to collect information); prior checking of processing; making decisions on complaints; ordering of blocking, erasure, or destruction of data; power to initiate legal action; and cooperation between supervisory authorities. These powers must be interpreted in accordance with legal systems and administrative traditions of member states. The intent is that DPAs have the powers to ensure that things are done right and that individuals can complain if they feel aggrieved.

Mr. Davis presented the role of the Irish DPA as a case study. It has four key roles: Ombudsman Role, Enforcer Role, Educational Role, and Registration Authority.

Key issues to address include:

- The difficulties for multi-jurisdictional entities of implementation when trying to respect the individual tradition of each member state.
- Is the focus on preventing breaches overly bureaucratic?
- Perhaps stronger powers are needed to decide upon and deal with events after they happen.
- The need for more consistency of interpretation across authorities.

In light of these issues, the Commission is doing much to harmonize efforts. It has recently published a Communication on the implementation of the Directive. The way forward for now appears to be a carrot and stick approach: the carrot being the interpretive communications from the Commission on common provisions, and the stick being infringement procedures by the Commission to improve harmonization. Further, the Article 29 Working Party is encouraging a harmonized approach to issues, and it has agreed on the principle of E.U.-wide, synchronized national enforcement actions, setting criteria to identify issues for investigations. As data protection becomes more popular, Data Protection Authorities need to be adequately resourced. This is an issue across the E.U. – that DPAs have finite resources for issues that are becoming increasingly complex. Consumers must be aware that, in addition to Article 29, there are many other formal and informal forums dealing with electronic communications and privacy.

Artemi Rallo, Director, Spanish Data Protection Authority

Dr. Rallo spoke about auditing and enforcement at the Spanish DPA, and its experience with outsourcing to countries with a non-adequate level of protection. In May 2007, the Spanish DPA conducted an unprecedented enforcement action outside the E.U.: on-site inspections of data transferred to Colombia. The purpose was to audit the transfer of international data and verify effective compliance with the Spanish Data Protection Law at customer telephone attention

centers established by companies in the telecommunications sector in and out of the national territory.

The Spanish DPA carried out this inspection because the amount of cross-border flow of personal data between different public and private agents established in different countries has increased in recent years. Many Spanish companies adopt global sourcing to Latin American countries, and different Spanish Trade Unions had communicated their worries to the Spanish DPA. Therefore, the Spanish DPA decided to audit onsite certain data importers not only to evaluate the legal sufficiency of guarantees and their effective fulfillment, but also to analyze the transfer procedure. The telecommunications sector was specifically targeted because Spanish telecom companies have global sourcing in Latin America, and the whole telecom sector had a total of 22 international transfer authorizations, representing 15 percent of all authorizations.

The methodology used is based on identification of the purposes of the transfers and the development of a plan of action in three phases:

- First phase: Physical visits in Spain to the telecom operators (controllers) in order to analyze the services provided from companies located in Colombia, audit the processing of personal data, check that the information accessed is adequate, and study the security measures implemented.
- Second Phase: Inspections in Spain by the processor with a head office in Spain and a branch in Colombia, analysis of the services provided, checking compliance of the processing, and studying the security measures implemented.
- Third phase: Visits in Colombia to processors with collaboration by the telecom operator (controller).

The inspection found general compliance with technical and organizational security requirements. Under no circumstances should there be transfer of the telecommunications files to the companies that act as a processor. Due to these conclusions, the Spanish DPA put forth recommendations related to the level of security, including the duty of confidentiality, the duty to inform the Workers' Committee of the controller telecom company, and the duty to publish in the Spanish Official Journal.

Christopher Foster, Assistant General Counsel, Data Privacy, Honeywell International

Mr. Foster spoke about E.U. personal data transfers from the perspective of a Safe Harbor member and AMCHAM E.U. Member. He began by introducing a hypothetical situation in which Jonathan Faull is an employee of Department of Commerce, Inc., and representatives from each E.U. country have produced videos to share with the group. He raised questions to demonstrate the complications that can arise in even this simple situation: whether sensitive personal data is included, if consent is required, if DPA notifications are required, and how standard contractual clauses apply.

Honeywell's Data Privacy Function current compliance approach could be termed "Safe Harbor Plus." There is no systematic model for them to use data around the world, so they use a region

to region, country to country method. It is marked by a focus on human resources data, Safe Harbor principles for data transferred to the U.S., and model contracts for data sent from EMEA to non-U.S. countries. Their emerging compliance approach is a global one that incorporates Binding Corporate Rules to treat all personal data, an interim step of one-company policy guided by privacy principles, and an expanded global focus on security for the most sensitive data.

The AMCHAM E.U. position on intra-E.U. data flows features several key aspects:

- General Assessment
- Binding Corporate Rules
- Standard Contractual Clauses
- Consent
- Safe Harbor

Isabel Davara, Partner, Davara Abogados

There should be no such thing as two different approaches to data protection and privacy. Currently, the European one is based on principles and procedures, and the American one only applies to the U.S. But what are the consequences for third-party countries? The U.S. approach does not guarantee that the country fulfills E.U. requirements. Further, not opting for a European legal approach implies not being able to have a full commercial relationship with the E.U. Latin American countries are used to “law-based” regulations and state rules. Self-regulation does not always work properly in such an environment. As a result, the trend in Latin America is to follow European standards, and, specifically, Spanish ones for cultural, historical, and linguistic reasons.

Ms. Davara does not believe that Safe Harbor is an exportable model. She does not criticize it as a model for the U.S., where it works very well. But she stressed that privacy is local and we are not all from the same “organized” or “civilized” countries like Canada or the U.S. We do need rules, however, which oblige us to conform to the law. Security issues in third-party countries are extremely important, and while factors such as terrorism have raised many concerns, they have not led those countries to erase individual rights and civil liberties. There must be a balance.

What are the choices for a third-party country? As a general solution, the country should obtain the European Commission’s declaration of an adequate level of protection to obtain freedom in data exchange. Other solutions include using other means, such as contractual clauses, but these carry problems because they must be agreed upon between parties, they are not a general country solution, and they establish many responsibilities and duties. A new trend is Binding Corporate Rules. We need international standardization. Further, third-party countries want to comply with a uniform legal model, but we need comprehensive collaboration like this on an even broader scale. The E.U. should be flexible about fines and punishment, and the U.S. should be clear about regulation.

PANEL IV: Implementing and Enforcing Corporate Privacy Rules

This panel combined the topics addressed during the conference thus far by having a discussion based on a hypothetical situation. The panel focused on countries outside the E.U. – Canada, Mexico, and the U.S. – to talk about how data protection initiatives work on a global basis for global companies.

Miriam Wugmeister, a partner at Morrison & Foerster, LLP, began the panel with a hypothetical situation. Presume that a U.S. consumer purchases a computer on the Internet from an Irish manufacturer, and the computer is shipped to the consumer in the U.S. As part of the purchase agreement, the consumer purchases a customer support agreement. The customer support centers for North America are run out of Mexico and Canada by subsidiaries of the Irish company. The Mexican and Canadian affiliates use the personal information they receive to market products and services to the U.S. consumer (overall, the U.S. consumer sent information to Ireland, and Ireland sent it to Canada and Mexico).

Suppose the Irish manufacturer had fully disclosed to the U.S. consumer that his personal information would be provided to the Mexican and Canadian affiliates, as required under Irish law, but that the information would only be used to provide the services requested by the U.S. consumer. Also suppose that the Irish manufacturer had entered into a cross-border agreement with the Mexican affiliate, and in that agreement it is stipulated that the data can be used only to provide the services to the U.S. consumer.

The group then discussed what the different parties could do to resolve the situation under various scenarios, illustrating several key points. Even though accountability models are supposed to work, there can still be many questions about jurisdiction. On one hand is the accountability model (incorporating finality), and on the other hand is the notice and choice model. From the viewpoint of the consumer, they are unlikely to take any action.

The point is that it is very complicated, and the consumer likely does not know how to seek redress. As such, we want to discuss an alternative model. Companies want to do the right thing, and want to protect the consumer for commercial reasons, but they are struggling. Companies and regulators need to increase cooperation to make BCRs work better.

PANEL V: Binding Corporate Rules (BCRs) and Contractual Clauses – The European Union’s Context

This panel discussed the differences between participation in Safe Harbor and compliance with BCRs, focusing on the corporate example of General Electric, which uses BCRs and internal enforcement to provide strong, global data protection. It also addressed Cross Border Privacy Rules (CBPRs) in APEC, which are promising tools that reinforce the need for continued cooperation on data privacy issues worldwide.

Lokke Moerel, Partner, De Brauw Blackstone Westbroek

Moderator Lokke Moerel began the panel by discussing the difference between Safe Harbor, which can be an easier route, and compliance with BCRs, which are based on European rules. The Working Party has done a good job in trying to facilitate BCRs. In the U.S., there are rules, but enforcement is the main tool to achieve compliance, whereas in Europe, if the rules must be enforced then the DPAs feel they have failed.

Tanguy Van Overstraeten, Partner, Linklaters, LLP

Mr. Van Overstraeten began by insisting that not everything is wrong – we are moving in the right direction. There are many strategies for trans-border data flows, and his presentation focused on contractual clauses. In terms of standard contractual clauses, the basis is Article 26 (4) of Directive 95/46/EC. Also, member states are required to authorize transfers based on E.U. Commission standard contractual clauses. There are three sets of clauses so far: transfers between Data Controllers, transfers between a Data Controller and a Data Processor, and transfers between Data Controllers - ICC version. Standard Data Controller clauses date back to 2001 and set forth requirements for the Data Exporter and the Data Importer, and cover joint and several liability. Standard Data Processor clauses have similar obligations for the Data Exporter, reduced obligations for the Data Importer, and do not include joint and several liability. Besides these, ICC Standard clauses are based on more pragmatic principles and use more business-friendly language. These, however, are still designed for point to point use and only cover controller to controller transfers.

The main difficulties in application are the variety of applications throughout the E.U., and the challenge for multi-party situations. There is much room for improvement, and we must develop consistency and harmonization of procedural requirements, extension of use for multi-party transfers, allowance for onward transfer to data processors, the possibility to include additional clauses, and other sets of clauses required in specific areas (e.g. HR transfers).

Nuala O'Connor Kelly, Chief Privacy Leader, General Electric Company

Ms. O'Connor Kelly spoke about the achievements, challenges, and solutions related to General Electric's (GE) Binding Corporate Rules. GE is a huge global enterprise, and its policies (The Spirit and Letter) are the foundation of its integrity. BCRs were incorporated into GE policy in 2003, and today GE's BCRs continue to provide strong, global data protection. The key principles include a high, E.U.-like standard globally and protections such as transparency and fairness, purpose limitation, data quality, security, rights of access, and protections for onward transfer. GE has enforcement through internal controls and audits, reporting channels for suspected violations, cooperation with Data Protection Authorities, and communication and training. BCRs are an effective compliance approach for several reasons:

- Consistent with GE's compliance structure and practices
- Binding on GE entities and employees
- Harmonized global guidelines ensure a consistent, strong protection
- Policies are alive and visible to employees
- Language is user-friendly and has been translated into many local languages for data handlers and employees around the world
- Company assumes responsibility for providing adequate safeguards for data
- Strong support for a privacy compliant culture from GE senior management

GE sought recognition of its standards as a BCR in each country, but prior to the coordinated process it faced challenges because gaining individual approval by 28 E.U./EEA countries was time-consuming, and minor modifications suggested by individual DPAs triggered significant work. GE worked with UKIC as its "lead authority" for coordinated approval of BCR (mid-2004 through present). To manage practical implementation of its privacy program regionally and globally, GE maintains a strong privacy and policy governance structure to ensure daily compliance. Its policies are visible and user friendly, and it employs in-depth training and guidance for data handlers. BCRs benefit companies with a unified global standard, in-house policy driven by and tailored to a company's unique culture, and more ability to communicate rules and values to employees. BCRs benefit DPAs through a simplified approval process for BCRs, fewer unique data processing approvals, better awareness of data protection rights on the part of the individual, and an increased and clarified role for DPAs in enforcing and approving BCRs of global companies.

James Koenig, PricewaterhouseCoopers LLC

Mr. Koenig offered reflections on model contracts and binding corporate rules based on his experience working with global organizations. First he addressed the evolution and drivers for large companies in designing global approaches. Companies will often take a wait-and-see approach to see what actions industry and regulators take. Model contracts were initially considered on a transactional or single-purpose basis, while Binding Corporate Rules were considered, but pursued in the context of enforcements. Both are now increasingly considered by global companies as viable options. Recent changes have made both options more attractive to companies. Increasingly, companies appreciate the importance of developing a compliance

approach. Business is increasingly conducted on a global basis with global operations, workforce and vendors, and companies are increasing activities in this area. Further, data protection authorities have recently increased investigations and recommendations for criminal prosecution.

Some operational considerations include the context and timing for a decision, speed and certainty, and flexibility and the ability to adapt to changes. How should companies define security standards? Three main trends are evident. Trend #1 is to use data element inventories to identify scope, provide specific standards for internal security assessments and audits, and detail obligations of vendors. Trend #2 is to take advantage of more than one compliance method, where appropriate. Trend #3 is to use data architecture to simplify obligations. It is important for a company to remember that when it puts these policies in place, they are not aspirational, but binding. As companies mature their global privacy and data protection programs, points of leverage and consistency across regulations, along with novel approaches, can be developed. As leaders in industries move, the rest of the industry will move. As more companies have positive experiences with Binding Corporate Rules, experiences will be shared and others will follow.

Yukiko Ko

Ms. Ko shared her unique perspective from being in Asia (APEC) and from working on BCRs. TransUnion employs privacy protocols and security measures to create high consumer confidence in personal financial information, and to prevent and combat financial crimes by establishing the industry's first dedicated fraud victim assistance department. TransUnion advocates global privacy rules because of the proliferation of various data protection laws, the constant flows of data without frontiers, and the privacy, security, and market demands. The key features of global corporate privacy rules are transparency (intra-company and inter-company), efficiency, and uniformity. The E.U. and APEC have different backgrounds, but common interests: they are both looking for an instrument that will protect market players in an increasingly connected world. In terms of the privacy culture, the E.U. focuses on the protection of human rights, whereas APEC focuses on the protection of consumer rights.

What have we developed? The E.U. has BCRs, a widely recognized compliance tool, and APEC has Cross Border Privacy Rules (CBPRs), which are currently being developed. Implementation is key for both of these instruments, which aim to facilitate privacy compliance by creating corporate accountability.

In conclusion, the commonalities between BCRs and CBPRs hint at global corporate best practice for data protection. However, not all players have the resources and knowledge to implement these instruments, so there is a strong need to provide capacity building and technical assistance for emerging economies and SMEs. The rules development and approval process should be streamlined and clear, and to make this a reality, frequent information exchange among businesses, governments, and civil society organizations in the two regions is essential.

CLOSING REMARKS

Peter Schaar, Chairman, Article 29 Working Party

In his closing remarks, Mr. Schaar noted that there are some challenges for data protection across borders, but forums such as this one help us learn about these challenges. Mr. Schaar believes that BCRs are the best way because if a company adopts BCRs, then it must deal with its own data protection culture and define its own rules. Also, Safe Harbor encourages companies in that direction. We know we must speed up, simplify our procedures, and make them more transparent. Increased transparency is one of the most important measures.

Michelle O’Neill, Deputy Under Secretary for International Trade, U.S. Dept. of Commerce

Ms. O’Neill closed by stating that not only is it important to continue the dialogue between the U.S. and the E.U., but also to expand the discussion to a wider group of countries. We are moving toward a very complex system, but thanks to discussions like this one, the key mechanisms are becoming clearer, as are our expectations for our companies. We have made much progress, but there is still much to be done. We look forward to the next formal conference, but we must also continue an informal dialogue as well.

CONCLUSIONS AND RECOMMENDATIONS

There are many challenges in safeguarding data and enforcing privacy rules on a global scale, but continued dialogue through forums such as this one is necessary to achieve these goals. All parties to this global privacy debate must do more outreach on behalf of data privacy measures. From the FTC’s perspective, enforcement is critical to success, so the Department of Commerce is evaluating ways to continue this privacy dialogue in a government to government context. Together our governments must think creatively about how to manage and regulate privacy, remaining open to new models, both regulatory and self-regulatory, that expand privacy protections and accomplish what no country can do alone. These models must be tied back to law to ensure enforceability.

Regulators must avoid a one-size-fits-all approach because privacy is inherently a local issue that reflects cultural and institutional differences. Instead, the focus should be on creating a collaborative enforcement model – like Safe Harbor – but on a global rather than bi-national level. Public discussion forums and FTC-sponsored self-assessment tools can make the certification process simpler and easier for interested companies. Further, privacy organizations can work in the context of such a model to help companies gain certification and improve their data security, while also exposing those companies operating outside the system.

When discussing these privacy and enforcement models, we must be cognizant of the competing viewpoints of companies and individuals, the central figures in this debate. Companies can build privacy protections into their everyday operations by certifying through a system such as Safe Harbor, and by exploring the use of mechanisms such as BCRS. Companies and regulators must increase cooperation to leverage resources and make these protections more effective in the future. When considering the individual consumer's perspective, regulators and companies alike must recognize the limitations of accountability models and the complexity of the redress process.

In general, we must accelerate and simplify our data security procedures, making them more transparent for companies and individuals. Not only is it important to continue this dialogue between the U.S. and the E.U., but also to share resources and expand the discussion to a wider group of countries in Asia and around the globe. The current data privacy protection regime is a complex system, but discussions like this forum help to shed light on key mechanisms and expectations for all parties.

APPENDIX A

Agenda

15 Oct 2007	
Day 1 Afternoon	
12:00pm	REGISTRATION
1:45pm	Welcoming Remarks Lydia Parnes , Director, Bureau of Consumer Protection, Federal Trade Commission
1:55pm	OPENING REMARKS Michelle O'Neill , Deputy Under Secretary for International Trade, U.S. Dept. of Commerce Jonathan Faull , Director General for Justice, Freedom, and Security (TBC)
2:15pm	KEYNOTE ADDRESS Fred H. Cate , Distinguished Professor and Director, Indiana University Center for Applied Cybersecurity Research
2:40pm	Coffee Break
3:00pm	WORKSHOP ON THE U.S.-E.U. SAFE HARBOR (Moderator: Alisa Bergman , Partner, Venable LLP) Damon Greer , Safe Harbor Program <i>The U.S.-E.U. Safe Harbor Framework</i> Giovanni Butarelli , IT Garante <i>The European Union's Data Protection Framework 12 Years Later</i> <i>The U.S.- E.U. Safe Harbor: Between Present and Future</i> Joan Antokol , Partner, Baker & Daniels, LLP <i>Safe Harbor Certification: The Company Perspective</i> David Hoffman , CPO, Intel Corporation <i>International Data Transfer: Trust in the Digital Economy</i> Martha Landesberg , Director of Policy & Counsel, Truste <i>TRUSTe's EU Safe Harbor Seal Program: Compliance and Enforcement Update</i> Hugh Stevenson , Deputy Director for International Consumer Protection, Federal Trade Commission
16 Oct 2007	
Day 2 Morning	
8:00am	REGISTRATION
8:30am	GLOBAL SOURCING AND DATA FLOWS - COMPLIANCE AND SECURITY IN THE GLOBAL

	<p>ECONOMY</p> <p>(Moderator: Marty Abrams, Executive Director, Center for Information Policy Leadership <i>Global Sourcing, Global Teaming</i>)</p> <p>Bojana Bellamy, Global Data and Privacy Leader, Accenture</p> <p>Dean Forbes, Senior Director - Global Privacy, Schering-Plough Corporation</p> <p>Sandy Hughes, Chief Privacy Officer, Proctor & Gamble, Inc.</p> <p>Harriet Pearson, Chief Privacy Officer, IBM <i>The New Landscape: Global Integration & Data Flows</i></p> <p>Jessica Rich, Assistant Director, Division of Privacy and Identity Protection, Federal Trade Commission</p>
10:30am	Coffee Break
10:45am	<p>THE EUROPEAN UNION'S DATA PROTECTION FRAMEWORK - 12 YEARS LATER: <i>Intra-E.U. Data Flows, Adequacy, and the Role of the Article 29 Working Party on Data Protection</i></p> <p>(Moderator: Peter Schaar, Chairman, Article 29 Working Party)</p> <p>Francesco Pizzetti, President, Garante, Italian Data Protection Authority</p> <p>Gary T. Davis, Ireland Deputy Data Protection Commissioner <i>Enforcement Powers of National Data Protection Authorities and Experience Gained of the Data Protection Directive</i></p> <p>Dr. Artemi Rallo, Director, Spanish Data Protection Authority <i>Auditing and Enforcement at the Spanish DPA. Experience with Outsourcing to Countries With a Non Adequate Level of Protection</i></p> <p>Christopher Foster, Assistant General Counsel, Data Privacy, Honeywell International, Inc. <i>E.U. Personal Data Transfers: The Perspective of a Friendly U.S. Harborite And AMCHAM E.U. Member</i></p> <p>Isabel Davara, Partner, Davara Abogados <i>Protection of Public Safety v. Other Public Interests, such as the Privacy Rights of Individuals</i></p>
Luncheon	
12:45pm	Luncheon from 12:45PM to 2:00PM
Day 2 Afternoon	
2:00pm	<p>IMPLEMENTING AND ENFORCING CORPORATE PRIVACY RULES</p> <p>(Moderator: Miriam Wugmeister, Partner, Morrison & Foerster, LLP)</p> <p>Bob Rothman, Chief Privacy Officer, General Motors Corporation</p> <p>Marc Rotenberg, President, Electronic Privacy Information Center</p> <p>Jennifer Stoddart, Privacy Commissioner of Canada</p> <p>Jesus Orta Martinez, Director of Electronic Commerce, Ministry of the Economy, Government of Mexico</p> <p>Mrs. Lina Ornelas, General Director of Classified Information and Data Protection, Federal Institute of Access to Public Information (IFAI), Mexico (TBC)</p>
3:40pm	Coffee Break
3:50pm	<p>BINDING CORPORATE RULES AND CONTRACTUAL CLAUSES - THE EUROPEAN UNION'S CONTEXT</p> <p>(Moderator: Ms. Lokke Moerel, Partner, De Brauw Blackstone Westbroek)</p> <p>Nuala O'Connor Kelly, Chief Privacy Leader, General Electric Company <i>GE's Binding Corporate Rules: Achievements, Challenges and Solutions</i></p>

	<p>Tanguy Van Overstraeten, Partner, Linklaters, LLP <i>Transborder Data Flows & Privacy: Contractual Clauses in the Practice</i></p> <p>Yukiko Ko, Director, International Fraud and ID Management, TransUnion <i>Binding Corporate Rules – Global Implications</i></p> <p>James Koenig, PricewaterhouseCoopers, LLC <i>Model Contracts & Binding Corporate Rules: Reflections from Working with Global Organizations</i></p>
5:30pm	<p>CLOSING REMARKS</p> <p>Peter Schaar, Chairman, Article 29 Working Party</p> <p>Michelle O'Neill, Deputy Under Secretary for International Trade, U.S. Dept. of Commerce</p>

Speaker and Panelist Biographies

Marty Abrams

Executive Director

Center for Information Policy Leadership

Martin Abrams is Executive Director of the Center for Information Policy Leadership at Hunton & Williams LLP, a path-finding global privacy and information security think tank located in Washington, D.C. Mr. Abrams brings nearly 30 years' experience as a policy innovator to the Center where he pursues practical solutions to privacy and security problems. Mr. Abrams originated the multi-layered privacy notices that have been adopted by international data protection commissioners, the European community, leading companies and various government agencies and are expected to be adopted by APEC and OECD. He is a leading theorist on global transfers of data based on accountability, and has led the movement in the U.S. to adopt harms-based approaches to privacy. Mr. Abrams created the "Values Approach" to building privacy programs while Vice President of Information Policy and Privacy at TRW and Experian North America, and assisted other companies in adopting that approach. He has led privacy seminars in North America, Europe and Asia, and has conducted privacy training for many government agencies and companies. Mr. Abrams has given privacy talks on five continents and has participated in four APEC privacy workshops. Mr. Abrams assisted the U.S. Federal Trade Commission in designing their workshop on data flows, and the Center has conducted seven dialogue sessions for various U.S. government agencies. Outside of privacy, he developed the methodologies the Federal Reserve System used to bring banks and community organizations together to encourage community-based economic development and avoid disputes.

Joan Antokol

Partner

Baker & Daniels, LLP

Joan Antokol is recognized internationally for her work in privacy and data protection. She leads the firm's privacy and data protection group and also assists clients on document management practices.

Before joining Baker & Daniels, Joan was a Vice President and the Global Head of Privacy at Novartis, where she established and managed the Global Privacy and Data Protection Department for companies in the Novartis Group. She has worked closely with European and U.S. privacy regulators and sits on several international privacy committees.

Joan is a frequent presenter at privacy conferences in the U.S. and Europe, and she has particular expertise in a number of aspects of privacy and security, including medical and clinical research, addressing and preventing security breaches, and transferring personal information between countries. Joan has a background in litigation, health authority inspections and drug safety.

Prior to Novartis, Joan worked at Hoffmann-LaRoche, Inc., managing pharmaceutical product liability litigation. She also was responsible for certain regulatory, compliance and drug safety matters on a global level. Before her in-house role with the pharmaceutical industry, Joan was an external counsel at Drinker, Biddle & Shanley in New Jersey. She represented pharmaceutical companies and physicians in medical malpractice defense. Joan also served as an acting municipal prosecutor.

Bojana Bellamy

Global Data and Privacy Leader
Accenture

Bojana Bellamy works for Accenture as Global Data Privacy Compliance Lead, based in the company's London office and responsible for the company's internal data protection compliance efforts worldwide. Prior to joining Accenture, Bojana had worked for eight years as Principal Consultant with Privacy Laws & Business, on data protection consulting and auditing projects for private and public sector clients in the UK and abroad.

Bojana has spoken at numerous data protection and privacy conferences and workshops in the UK and abroad.

Bojana has a Master's degree from the European University Institute, Florence, Italy on the EC Draft Directive on Data Protection. She has a law degree from Belgrade University, Yugoslavia and a Diploma of Advanced European Legal Studies from the College of Europe, Bruges, Belgium.

Bojana is fluent and writes in English, French, Italian and Serbo-Croat.

Alisa Bergman

Partner
Venable, LLP

Alisa Bergman has many years of experience representing clients before the U.S. Congress, federal regulatory agencies, and state legislatures on privacy, data security, and e-commerce legislative and regulatory issues. She assists with drafting laws and developing regulations on issues including financial, health care, and children's privacy; e-mail and wireless marketing; and security breach notification and data safeguards requirements. She advises clients on compliance with all aspects of data protection, including international data management, e-marketing, and customer relationship management strategy. She has conducted multi-national data protection reviews of both consumer and employee data practices to assist companies with worldwide

privacy compliance and risk management. She also advises regarding international transborder data flow strategies, including participation in the Department of Commerce's Safe Harbor Program for compliance with the E.U. Data Protection Directive, model contracts, and binding corporate rules. In addition, she has extensive experience in advising on data protection issues in non-E.U. countries. Alisa has developed harmonized policies and practices across multiple divisions of diverse multi-national companies to comply with existing, as well as emerging, data protection and related laws.

Giovanni Buttarelli

Secretary-General

Italian Data Protection Authority

Mr. Buttarelli has been a member of the judiciary since 1986, and Secretary General to the Italian Data Protection Authority ("Garante per la protezione dei dati personali") since 1997.

In the 2002 to 2003 period, he was the President of the Joint Supervisory Authority (Acc Schengen) set up in pursuance of the Schengen Agreement, after being its Vice-President in 2000-2001. He was a member of the Acc since 1994 when he was designated by the Italian Parliamentary Committee on Security and Information Services.

He has represented Italy in many commissions and working groups both at the European Union level, including Art. 29 Working Group and Art. 31 Committee Directive N. 95/46/EC, and at the Council of Europe (T-PD; CJ-PD and DH-S-AC). During the E.U. Italian Presidency period (1996), he chaired the European Union Council Working Group which drew up Directive no. 97/66/EC on the protection of privacy in the telecommunications sector. He drafted as a consultant the "Report containing guiding principles for the protection of individuals with regard to the collection and processing of data by means of video surveillance" (2003), after which the European Committee on Legal Co-operation (CDCJ) has adopted a list of Guiding Principles at its 78th meeting May 20-23, 2003). He was a member of the Committee - set up in a decree by Italy's Public Administration Minister - that drew up the 2003 Personal Data Protection Code. Prior to this, he had drafted the Italian privacy bill passed in 1996.

He was a member of several Ministerial (in particular, at Ministry of Justice), and inter-Ministerial committees in Italy concerning community fraud, de-criminalisation, reformation of tax and computer crime laws, and access to confidential records, including the Commission for the Study of Laws Concerning Digitalisation of Public Administrative Agencies.

He currently teaches privacy at the Lumsa University, Rome. From 1984 to 1990, he collaborated with the Chair of Criminal Procedure at Rome University; he held several lectures and contributed to master degree and other courses exploring legal issues related to new technologies in various universities.

He worked for a number of years at the Legislation Department of the Italian Ministry of Justice where he contributed to drafting and following up many regulatory provisions, in particular concerning criminal law and criminal procedure.

Mr. Buttarelli took part as a speaker in many meetings and workshops both in Italy and abroad, as well as participated in hearings held by the Italian and European Parliaments. He is a regular contributor to specialized journals and has authored a number of papers as well as the first monograph on European and Italian data protection laws published in 1997.

Fred H. Cate

Distinguished Professor and Director of the Center for Applied Cybersecurity Research
Indiana University

Fred H. Cate is a Distinguished Professor and Director of the Center for Applied Cybersecurity Research at Indiana University and a senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams. He works at the forefront of privacy, security, and other information law and policy issues.

He is a member of the National Academy of Sciences Committee on Technical and Privacy Dimensions of Information for Terrorism Prevention and Other National Goals; a member of Microsoft's Trustworthy Computing Academic Advisory Board; and reporter for the American Law Institute's project on Principles of the Law on Government Access to and Use of Personal Digital Information.

Professor Cate served as counsel to the Department of Defense Technology and Privacy Advisory Committee, reporter for the third report of the Markle Task Force on National Security in the Information Age, and a member of the Federal Trade Commission's Advisory Committee on Online Access and Security. He directed the Electronic Information Privacy and Commerce Study for the Brookings Institution, and the Project on Electronic Commerce in the United States and Europe for the American Institute for Contemporary German Studies, and he chaired the International Telecommunication Union's High-Level Experts on Electronic Signatures and Certification Authorities.

He was a member of the United Nations Working Group on Emergency Telecommunications and principal drafter of the Tampere Convention on the Provision of Telecommunications Resources for Disaster Mitigation and Relief Operations, which was adopted in June 1998.

Professor Cate has testified before numerous Congressional committees, and he speaks frequently before professional, industry, and government groups. He has spoken throughout the United States and in Belgium, Canada, China, Finland, Germany, Italy, Japan, Switzerland, Taiwan, Trinidad & Tobago, and the United Kingdom. In 1997, he served as a Visiting Professor of Law at the Walther-Schücking-Institute für Internationales Recht, Christian-Albrechts-Universität zu Kiel, in Kiel, Germany.

He is the author of more than 100 articles and books, including the award-winning *Privacy in the Information Age*, *The Internet and the First Amendment*, and *Privacy in Perspective*. He serves on the board of editors of *Privacy & Information Law Report*.

Professor Cate is a senator and fellow of the Phi Beta Kappa Society, an elected member of the American Law Institute, and co-chair of the Alliance of Distinguished and Titled Professors. He attended Oxford University and received his J.D. and his A.B. with Honors and Distinction from Stanford University. He is listed in Who's Who in the World, Who's Who in America, Who's Who in American Law, and Who's Who in American Education.

Isabel Davara

Partner

Davara Abogados

Along with being a member of the Ilustre School of Lawyers in Madrid (Spain), Ms. Davara is Partner of Davara Abogados, a firm specializing in Information and Communications Technology (ICT) Law. Ms. Davara is Chair of the Latin American Electronic Commerce Committee of the Section of Science and Technology of the American Bar Association as well as Associate Professor of Law at the Mexico Autonomous Institute of Technology (ITAM).

Ms. Davara is a professor and lecturer in numerous seminars related to information and communication technology law, organized by various universities, government agencies, bar associations and commerce chambers in Europe and Latin America. Ms. Davara received her B.A. in Economics, her J.D., and her J.S.D. all from Comillas Pontificia University in Madrid (ICAI-ICADE).

Jonathan Faull

Director General for Justice, Liberty, and Security (TBC)

Mr. Faull is Director General for Justice, Freedom and Security at the E.U. Commission. He began his career at the Commission in 1978 as an Administrator for Customs Union Service within the Legal and General Affairs Division.

In 1981, he joined the Directorate General for Competition, where, until 1984, he worked as an examiner in individual 'antitrust' cases in the Directorate for Restrictive Practices and Abuses of Dominant Position, before becoming Principal Administrator in the Directorate for Coordination of Individual Cases. Between 1987 and 1989, he worked as Assistant to the Director General of DG COMP.

After a three-year interlude of working as a Member of the Cabinet of Sir Leon Brittan, Vice-President of the Commission, where he was responsible for competition policy and financial institutions, Mr. Faull returned to DG COMP in 1992, first as Head of Unit IV/D/3 (Transport and Tourism), then, in 1993, as Head of Unit IV/E/1 (Coordination and General Policy, General State Aid Schemes).

In 1995, he was promoted to Director for IV/A (Competition Policy, Coordination, International Affairs and Relations with the other Institutions). In 1999, he became Deputy Director General of DG COMP.

Mr. Faull holds a BA in Law and French from the Universities of Sussex and Geneva, and an MA in Law and European Studies from the College of Europe in Bruges.

Since 1989, he has been a Professor of Law at the Free University of Brussels. He is also a Visiting Fellow at the Centre for European Legal Studies at the University of Cambridge.

He was also a Visiting Lecturer at the Institut d'Etudes Politiques in Paris from 1992 to 1995.

Dean Forbes

Senior Director - Global Privacy, Global Compliance & Business Practices
Schering-Plough Corporation

Dean Forbes is Schering-Plough Corporation's Sr. Director, Global Privacy. In that role, Mr. Forbes is responsible for developing and implementing all strategic global privacy initiatives for the company. Mr. Forbes has worked with Schering-Plough since 2004.

Prior to taking on this responsibility, Mr. Forbes worked as an Attorney with the Federal Trade Commission's Bureau of Consumer Protection for over 13 years. His work for the Commission ran the gamut, from cases against deceptive advertising and technology fraud to Internet privacy and information security. He practiced law in the Agency's Division of Advertising Practices, and worked on landmark information privacy and security matters and on workshops addressing timely issues such as "spyware." His work on privacy and information security has been featured in the New York Times and the Privacy Officer's Advisor. In 2000, in an article titled "Defending Consumer Rights," the National Bar Association Magazine referred to Mr. Forbes as one of the Commission's "authorities on privacy and technology fraud."

Mr. Forbes is a member of the Board of Directors of the International Association of Privacy Professionals (IAPP), the Board of Directors of the International Pharmaceutical Privacy Consortium (IPPC), the Responsible Information Management Council Advisory Board, and the Center for Information Policy Leadership.

Mr. Forbes is a graduate of Brown University (1987), and a graduate of the University of Virginia School of Law (1991).

Christopher F. Foster

Assistant General Counsel – Data Privacy
Honeywell International, Inc.

Mr. Foster is responsible for driving compliance, legal and technical best practices and functional excellence in the area of data privacy. Mr. Foster's responsibilities include protection of Honeywell's employee, customer and supplier data, as well as website privacy compliance. Prior to joining Honeywell International Inc., Mr. Foster was Chief Privacy Leader for GE Insurance Solutions and Associate Attorney at Shook, Hardy & Bacon L.L.P. and at Hogan &

Hartson L.L.P. Mr. Foster received his B.A. in English from Duke University and his J.D. from Harvard Law School. He also received his Masters of Fine Arts in creative writing from the University of Iowa.

David A. Hoffman

Group Counsel and Director of Security and Privacy Policy
Intel Corporation

Mr. Hoffman joined Intel in 1998 as Intel's eBusiness attorney, in which capacity he managed the team providing legal support for Intel's Chief Information Officer. In 1999, he founded Intel's Privacy Team, and in 2000, was appointed Group Counsel of eBusiness and Director of Privacy. In 2005, Mr. Hoffman moved to Munich, Germany, as Group Counsel in the Intel European Legal Department, while leading Intel's Worldwide Privacy and Security Policy Team. Mr. Hoffman served on the U.S. Federal Trade Commission's Online Access and Security Advisory Committee.

Mr. Hoffman was also a founding member of the BBBOnline Steering Committee. Mr. Hoffman served on the TRUSTe Board of Directors from 2000-2006, where he was Chair of the Compliance Committee of the Board. Also, in 2005, Mr. Hoffman was appointed to the Department of Homeland Security's Data Privacy and Integrity Advisory Committee, on which he is Chair of the Data Sharing and Use Subcommittee. Mr. Hoffman is also on the Board of Directors for the International Association of Privacy Professionals, and holds the Certified Information Privacy Professional Certification.

Mr. Hoffman has a J.D. from The Duke University School of Law, where he was an Editor on the Duke Law Review. Mr. Hoffman also received an A.B. from Hamilton College.

Sandra R. Hughes

Global Privacy Executive (CPO)
Procter & Gamble Company

Sandra R. (Sandy) Hughes serves as the Global Privacy Executive (CPO) at the Procter & Gamble Company, headquartered in Cincinnati, Ohio, and since August 2007, is also responsible for the Global Ethics & Compliance organization. Procter & Gamble's privacy program has been designed and implemented to promote trust among consumers, employees and other constituencies by protecting an individual's rights to privacy as they would expect. The Ethics & Compliance organization is the bridge between external risks and the internal processes to mitigate them. By having both responsibilities, and with her prior internal experience in leading other compliance areas, Sandy is able to identify synergies to elevate the impact and reach of both programs.

Sandy is a Certified Information Privacy Professional (CIPP) and Vice President/President-elect of the International Association of Privacy Professionals. She is also leader of the Privacy, Security and Technology working group of the U.S. Council of International Business (USCIB),

and serves on the State of Ohio Chief Privacy Officer Advisory Board. She is a founding member of the Public Policy Steering Committee of EPCglobal, a standards organization that utilizes Radio Frequency Identification (RFID). She has participated in multi-industry and consumer efforts to create EPC and RFID guidelines for responsible use of the technology for item-level tagging. She is a chapter author in the book, “RFID: Applications, Privacy and Security” edited by Simson Garfinkel and Beth Rosenberg and a frequent speaker on Global Privacy topics as well as EPC/RFID.

Sandy’s career spans over 30 years at the Procter & Gamble Company, with global, regional and local assignments in the U.S. (Ohio & Alabama), Germany and Belgium.

Martha K. Landesberg

Director of Policy and Counsel
TRUSTe

Martha Landesberg is Director of Policy and Counsel for TRUSTe. Prior to joining TRUSTe in 2003, Ms. Landesberg was Of Counsel to the law firm of Dorsey and Whitney, LLP, where she advised multi-national clients on U.S. and international data protection issues and assisted them as they developed corporate privacy policies. Ms. Landesberg was a Senior Attorney in the Federal Trade Commission’s Division of Financial Practices for six years, during which she led the staff team that conducted the Commission’s 1998 and 2000 surveys of commercial Web sites’ information practices, and was a leader of the team that drafted the Commission’s Children’s Online Privacy Protection Rule.

Ms Landesberg holds a B.A. from Yale University, a Master’s Degree in Education from Stanford University, and a J.D. from the University of Cincinnati College of Law.

Jesús Orta Martínez

Deputy Director-General of Digital Economy, Ministry of the Economy
Government of Mexico

Jesús Orta is the Deputy Director-General of Digital Economy at the Ministry of the Economy in the Federal Government of Mexico. He has served in this position for three years. Prior to his present appointment, he was the Director of Digital Economy for four years. Mr. Orta has been responsible for the IT industry and electronic commerce policy and regulation at the federal level for the last seven years. In that capacity, he led the design and currently heads the operation of the National Program for the Development of the Software and IT Services Industry (PROSOFT), which is the country’s overall public policy to develop the IT services sector in Mexico.

He is also responsible of coordinating policy strategies, instruments, and projects targeted to develop the IT market and electronic commerce in Mexico, working closely with local governments and the private sector. The scope of his responsibilities also include heading the

trade negotiations for the IT services sector and electronic commerce on behalf of the Government of Mexico in bilateral and multilateral negotiations, as well as IT innovation policy.

Mr. Orta is currently the Chairman of the APEC Electronic Commerce Steering Group and serves as Head of Delegation for the Mexican Government at the OECD's Information, Communications and Computer Policy Committee.

Lokke Moerel

Partner

De Brauw Blackstone Westbroek

Lokke Moerel is a partner in the intellectual property / information, communication & technology department of De Brauw Blackstone Westbroek. Lokke recently returned from the ITC department of Linklaters London, where she was the partner heading up the teams for world wide outsourcings, software implementation and e-business projects.

In the Netherlands, she represents a number of prominent international software, hardware and chips companies in both their contentious and commercial IT issues (including outsourcing). She has particular expertise in online procurement and e-commerce. She advises on issues such as online payment systems, marketing of online financial services, online advertising, online gambling and applicable law and jurisdiction. She is a well sought after speaker on international forums on these specific topics. She has written and contributed to the standard practitioners' works in this field and recently published a textbook on online advertising.

Lokke was a member of the board of the Dutch Association of Information Technology Lawyers.

Michelle O'Neill

Deputy Under Secretary for International Trade,

International Trade Administration

U.S. Department of Commerce

Michelle O'Neill was named Deputy Under Secretary for International Trade in November 2005. In this capacity, she oversees the daily operations of the International Trade Administration (ITA), which has an annual budget of \$400 million and 2,300 employees. O'Neill returns to ITA with an impressive professional record and a long history of government service, including 17 years of prior ITA service.

Before rejoining the ITA leadership team, O'Neill served as Deputy Under Secretary of Commerce for Technology. Beginning in July 2004, O'Neill served as the chief operating officer of the Technology Administration, which includes the National Institute of Standards and Technology.

Between June 2000 and July 2004, O'Neill was the Deputy Assistant Secretary for Information Technology Industries in ITA. In addition to serving as the lead advocate for U.S. information

and medical technology companies, O'Neill played an instrumental role in U.S. e-commerce policy, including establishing the U.S. government's first Office of Electronic Commerce.

In addition to her headquarters assignments, O'Neill served overseas as a Senior Commercial Officer with ITA's U.S. and Foreign Commercial Service. From August 1995 to February 1998, O'Neill was the Commercial Attache to the U.S. Mission to the Organization for Economic Cooperation and Development (OECD) in Paris. O'Neill returned to Washington in February 1998, serving as the chief of staff to the Under Secretary for International Trade until March 2000.

Prior to serving overseas, O'Neill worked in the office of Deputy Under Secretary for International Trade Timothy J. Hauser, serving as his executive assistant, between January 1992 and January 1995. From January to August 1995, O'Neill served as a Brookings Legislative Fellow with the House Ways and Means Trade Subcommittee; from September 1990 to March 1991, O'Neill was detailed to the White House Office of Policy Development.

From 1987 to 1990, she worked in ITA's Office of Antidumping and Countervailing Duty Investigations. O'Neill began her government career as a Presidential Management Intern in 1987.

O'Neill has received the Department's Silver Medal for her work on the APEC Privacy Framework; she also received a Silver Medal in 2004 for resolving a major China market access barrier, and in 2001, for developing the U.S. government portal, www.Export.gov. In 2004, International Economy Journal's "Who's Who in China Economic Policy" listed O'Neill. O'Neill won a Departmental Bronze Medal in 2003, for improving Chinese market access for U.S. IT firms. In 2001, O'Neill received the William A. Jump Award for exemplary service in public administration.

O'Neill received her B.A. degree from Sweet Briar College (1985), and her M.A. from the LBJ School of Public Affairs (1987).

Tanguy Van Overstraeten

Partner

Linklaters, LLP

Listed among Belgian leading individuals in Communications & IT (Chambers Global 2007), Tanguy is heading Linklaters Technology Media & Telecommunication (TMT) group in Brussels (Belgium). He has developed a thorough practice in the field of information technology contracts and regulatory, focusing on data protection projects and compliance audits as well as outsourcing. With a strong corporate background, he has a long-standing experience in advising multinationals on local and international large-scale transactions and regulatory projects in a wide variety of industry sectors.

Among recent data protection projects, he has advised a U.S. leading manufacturer of construction and mining equipment in connection with employee monitoring for the use of e-

mails and Internet as well as the implementation of a whistle-blowing scheme. He has also led the data protection compliance program of a multinational pharmaceutical company and assisted a U.S. payment card company in negotiating with the European Data Protection Working Party Article 29.

Tanguy is a member of the Digital Economy Committee of the American Chamber of Commerce to the European Union and Vice-Chair of the ICT Committee of the British Chamber of Commerce in Belgium. He regularly contributes in conferences related to data protection, most recently at the conference organized by Privacy Laws & Business on “Global Warning! Privacy Climate Changes Ahead” (July 2007, St. John’s College, Cambridge, U.K.). He is also teaching data protection and privacy laws at the Solvay Business School (University of Brussels, Belgium) and has published numerous legal articles on privacy matters.

Tanguy is a graduate of the University of Brussels (1987). A fellow of the Belgian American Educational Foundation (1990), he holds a LL.M. degree from the University of Chicago Law School (1991).

Harriet P. Pearson

Vice President, Regulatory Policy and Chief Privacy Officer
IBM Corporation

One of the Fortune 1000's first chief privacy officers, Harriet has since 2000 been responsible for IBM's global information policies and practices. In 14 years at IBM, she has held executive leadership roles in Governmental Programs, Human Resources, Communications and Legal. Outside of the company, she is a board member of the International Association of Privacy Professionals; the Center for Information Policy Leadership; and Anatolia, the American College of Thessaloniki, Greece. She holds an adjunct appointment at Georgetown University, where she teaches a graduate class on trust, privacy and security, and she serves on the Steering Committee for the Data Security Council of India.

A practicing attorney and Certified Information Privacy Professional, Harriet graduated from Princeton University and the UCLA School of Law. A first-generation American, she speaks Greek fluently. She lives in the Washington, D.C. area with her family and sings barbershop in her spare time with the Potomac Harmony Chorus, an award-winning chapter of Sweet Adelines International.

Francesco Pizzetti

President
Italian Data Protection Authority

Mr. Francesco Pizzetti is currently President of the Italian Data Protection Authority. He is Full Professor of Constitutional Law in the University of Turin, Italy, Faculty of Law, and Professor in the Link University of Malta in Rome.

Mr. Pizzetti acted as advisor in constitutional law and public administrative law to Italian governments in the 1987 to 2001 period, and from 1990 to 1993 he was Deputy-Major of the city of Turin.

From 1996 until 1998, he served as the Secretary to the Italian “State-Cities and Local Autonomies Conference” (“Conferenza Stato-Città-Autonomie locali”) and the “Unified Conference” (“Conferenza Unificata”).

Mr. Pizzetti was Director of the Italian Superior School of Public Administration (“Scuola Superiore della Pubblica Amministrazione”) from 1998 until 2001.

From 1996 until now, Mr. Pizzetti has been the President of the Commission for Agreements between the State and Religious Confessions (“Commissione per le Intese tra lo Stato italiano e le Confessioni religiose”).

He is currently a member of the Council of the Presidency of the Italian Administrative Judiciary (“Consiglio di Presidenza della Giustizia amministrativa”).

Mr. Pizzetti is a member of the Board of Directors of the Italian Association of Constitutional Law. He has performed extensive research on issues and topics related to the Italian and European Constitutional Law, with particular regard to the Italian Republic’s Constitutional Reform, the Italian federalism, and the development of a complex system of governance within the European institutional framework and legal order. He has also authored several scientific papers, articles, contributions and books on constitutional law and administrative reformation, including *Federalismo, regionalismo e riforma dello Stato* [Federalism, Regionalism, and Reforming the State], Giappichelli, Turin, 1996 and 1997, and *La costituzione europea* [The European Constitution], Astrid, Il Mulino, Bologna, 2004 (F. Bassanini and G. Tiberi eds.).

Artemi Rallo

Director

Spanish Data Protection Agency

Dr. Artemi Rallo is a professor of Constitutional Law at the Jaume I University of Castellón, where he was also Head of the Constitutional Law Department (1993-1998). He has performed research activities at international centers such as the International Human Rights Institute with its seat in Strasbourg; the Theory of State Department of La Sapienza University (Rome); and the Centre de Recherche de Droit Constitutionnel at the Paris I-Panthéon-Sorbonne University. He is the author of numerous monographs, collective books, and scientific articles in specialized national and international magazines.

Dr. Rallo has participated in national and international research lines and projects on contemporary transformations of the public administration, featuring independent administrations, on electoral guarantees, the threats to informative pluralism, the issues of present Parliament, protection of fundamental rights in the process of European integration and the processes of political decentralisation in the Member States of the European Union.

Dr. Rallo has collaborated with European institutional support programmes in Latin America, aimed at promoting political decentralisation and strengthening of the parliamentary institutions, the Executive Power and the Judicial Power. Since February 2007, he has been Director of the Spanish Data Protection Agency.

Dr. Rallo achieved graduate in Law with Extraordinary Prize Honours (1988) and Doctor in Law from the University of Valencia (1990).

Marc Rotenberg

President, Electronic Privacy Information Center

Marc Rotenberg is Executive Director of the Electronic Privacy Information Center (EPIC) in Washington, DC. He teaches information privacy law at Georgetown University Law Center and has testified before Congress on many issues, including access to information, encryption policy, consumer protection, computer security, and communications privacy. He testified before the 9-11 Commission on "Security and Liberty: Protecting Privacy, Preventing Terrorism." He has served on several national and international advisory panels, including the expert panels on Cryptography Policy and Computer Security for the OECD, the Legal Experts on Cyberspace Law for UNESCO, and the Countering Spam program of the ITU. He currently chairs the ABA Committee on Privacy and Information Protection. He is the former Chair of the Public Interest Registry, which manages the .ORG domain. He is editor of The Privacy Law Sourcebook and co-editor (with Daniel J. Solove and Paul Schwartz) of Information Privacy Law (Aspen Publishing 2005).

Mr. Rotenberg is a graduate of Harvard College and Stanford Law School. He served as Counsel to Senator Patrick J. Leahy on the Senate Judiciary Committee after graduation from law school. He is the recipient of several awards including the World Technology Award in Law.

Jennifer Stoddart

Privacy Commissioner of Canada

Jennifer Stoddart was appointed Canada's Privacy Commissioner, effective December 1, 2003, on unanimous resolutions adopted by both the House of Commons and the Senate, for a seven-year term. Since her arrival, she has led the Office's institutional renewal, and has also reoriented it toward its multi-disciplinary approach to preventing privacy breaches in the public and private sectors, and to protecting and promoting the privacy rights of Canadians.

Ms. Stoddart was previously President of the Commission d'accès à l'information du Québec, an organization responsible for both access to information and the protection of personal information. She has held several senior positions in public administration for the Governments of Québec and Canada. Ms. Stoddart has been active in the Canadian Bar Association, the Canadian Institute for the Administration of Justice, and has also lectured on history and law.

Miriam Wugmeister

Partner

Morrison & Foerster, LLP

Ms. Wugmeister counsels clients regarding the collection, use, and transfer of personal information as organizations seek to comply with international data protection laws. She regularly advises global companies on multinational privacy compliance efforts including: the consolidation of human resources data; global technology use and monitoring policies; centralization of customer data; and the implications of various national laws on direct marketing initiatives.

Ms. Wugmeister also has had significant experience in all areas of employment and labor law, and regularly counsels clients ranging from emerging growth companies with fewer than ten employees to Fortune 500 companies with thousands of employees. She advises clients about matters involving personnel policies, employee discipline issues, employment discrimination, reductions-in-force, wage & hour laws, employee privacy issues, and traditional labor issues. She has broad experience litigating, arbitrating, and mediating employment matters.

Ms. Wugmeister also speaks widely on privacy and data protection issues.