

**Hearing on
Internet Privacy: The Impact and Burden of EU Regulation
September 15, 2011**

**Testimony of Paula J. Bruening
Vice President, Global Policy
Centre for Information Policy Leadership
Hunton & Williams LLP**

**before the
U.S. House of Representatives Committee on Energy and Commerce
Subcommittee on Commerce, Manufacturing and Technology**

Distinguished Chairman, honorable committee members, I am Paula J. Bruening, Vice President for Global Policy of the Centre for Information Policy Leadership. I am honored to testify on The Internet: The Impact and Burden of the EU Regulation.

The Centre for Information Policy Leadership is a think tank and policy development organization located in the law firm of Hunton & Williams LLP. The Centre was established to develop innovative, pragmatic solutions to privacy and information security issues that reflect the dynamic and evolving nature of information-intensive business processes and at the same time respect the privacy interests of individuals. The Centre's member companies include leading organizations in health care, information services, retail, technology, financial services and consumer products.

Since its establishment, the Centre has addressed such issues as conflicting national legal requirements, cross-border data transfers and government use of private sector data, with a view to the impact of the future direction of business practices and emerging technologies on those issues. The Centre has spoken about these issues before the U.S. Department of Commerce, the Federal Trade Commission and congressional committees at workshops and hearings. It has been an active participant at the Organisation for Economic Co-operation and Development and

the Asia-Pacific Economic Cooperation forum. Currently the Centre leads the work of the Accountability Project, now concluding its third year. That project engages the expertise of an international group of government representatives, regulators, privacy experts, businesses and advocates to design a responsible, innovative approach to information privacy and data protection based on the fair information practice principle of accountability. The Centre's work has influenced privacy laws and regulation in the United States and abroad.

The Centre and its 41 member companies believe that difficult information policy issues must be resolved responsibly if we are to fully realize the benefits of an information economy. Centre experts and staff, however, speak only for themselves. As I prepared this testimony, I consulted with Centre colleagues and Centre members; however, my comments today reflect my views and do not necessarily reflect the views of Centre member companies, Hunton & Williams LLP, or any firm clients.

As we examine the question of the impact and burden of EU regulation, it is important to bear in mind that privacy laws are enacted in a manner consistent with local law and reflect the local culture of privacy. United States legal tradition differs markedly from that of Europe, and the American concept of privacy is influenced deeply by the First Amendment and strongly held beliefs about free expression. As we consider privacy law in Europe, we do so from an American perspective. Europeans similarly view American law from their own vantage point.

It is equally important to remember that technological changes that have occurred since 1995 have affected data protection in Europe — and every other privacy protection system — dramatically. Were the Centre to assess privacy protections in Canada, Australia or any other

established privacy regime, we would likely find limitations in those laws as well brought about by the evolution of technology.

I. Summary: While the EU Data Protection Directive (the Directive) is based on well-established and relevant principles of fair information practices, it applies them in a way that is not sufficiently flexible to promote the rapid innovation necessary for competitiveness and economic growth and to protect individual privacy.

Innovations in technology; rapid increases in data collection, analysis and use; and the global flow of and access to data have made an unprecedented array of products, resources and services available to consumers. These developments in no way diminish an individual's right to the secure, protected and appropriate collection and use of their information. Yet the manner in which those protections are provided is often challenged by the dynamic, increasingly international environment for information.

The principles of fair information practices upon which the European Directive is based remain respected, relevant and tested guidance for the appropriate use and protection of data.¹ But the global flow, innovative uses and market demands for data test the way in which the Directive applies those principles. In this environment, individuals maintain the right to secure and protected processing and storage of their data that does not compromise their privacy. At the same time, protection must now be sufficiently flexible to allow for rapidly changing technologies, business processes and consumer demand.

¹ The Privacy Act of 1974 95 U.S.C. Sec 552a and the Organization for Economic Cooperation and Development's "Guidelines on the Protection of Privacy and Transborder Data Flows" are also based on principles of fair information practices.

<http://www.oecd.org/document/18/0,3746,en_2649_34255_1815186_1_1_1_1,00&&en-USS_01DBC.html>

The European Commission's 2010 consultation on a possible reform of the Directive² recently signaled a growing recognition that some aspects of the EU approach are not optimal.³ In some cases, the Directive imposes administrative requirements that do little to further privacy but that place significant burdens on companies — and on regulators. In others, the manner in which the Directive implements certain principles of fair information practices does not reflect the realities of the current data environment, and results in *pro forma* compliance that does not necessarily yield good privacy outcomes. Perhaps most significantly, the Directive is often perceived as impeding or slowing the global flow and sharing of data so necessary to innovation and international competitiveness.

In November 2010, the Commission released a communication that acknowledged that rapid technological developments and globalization have profoundly changed the data environment, and brought new challenges to data protection.⁴ It noted the need to streamline and modernize the Directive, taking particular account of the challenges resulting from globalization and new technologies.

This testimony highlights key areas where the Directive is dated. It is not intended to be a complete analysis of European data protection law.

² Consultation on the Commission's Comprehensive Approach on Personal Data Protection in the European Union. <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

³ In 2009, the European Commission launched a review of the current legal framework on data protection, starting with a high-level conference in May 2009, followed by a public consultation running until the end of 2009. Targeted stakeholders' consultations were organized throughout 2010.

⁴ On November 4, 2010 the European Commission released a communication outlining its preliminary proposals to revise the EU Data Protection Directive (95/46/EC), entitled "Communication From the Commission to the European Parliament, the Council, the Economic and Social Committee and the committee of the Regions, A Comprehensive Strategy on Data Protection in the European Union." <http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf>.

II. The Directive imposes administrative notification requirements that often do little to advance privacy, but that place significant burdens on companies.

The Directive imposes on data controllers, *i.e.*, those persons responsible for data, the obligation to notify EU Member State data protection authorities of the processing of personal data.⁵ Such notification is required when information systems are created and modified, and when personal data is transferred outside the European Union. This notification requirement increases the administrative burden on industry, enhancing neither the security of data nor the privacy of individuals. National data protection authorities must invest significant resources into managing and responding to this notification process.

Moreover, the Directive requires companies transferring personal data to countries outside the EU not considered to have adequate data protection to notify the data protection authorities of the transfer and, in some cases, obtain prior approval.⁶ Such approval can easily take six months to obtain, and at the cost of significant resources for the company and the data protection authority.

Both organizations and regulators today are constrained by personnel and budget limitations. Complying with notification requirements diverts scarce company resources away from more productive activities that would enhance internal privacy programs and practices that would yield better privacy for consumers. Monitoring those notifications requires that regulators focus attention on good actors and away from companies that have demonstrated non-compliance and warrant close oversight.

⁵ EU Directive, Article 18.

⁶ EU Directive, Article 18 (e) and national data protection laws implementing this article.

It should be noted that the lack of harmonization across EU Member States exacerbates the burden of this requirement. Each of the 27 Member States' notification requirements differ to some extent from the others — sometimes in contradictory ways — and companies must comply with each.

III. Compliance with the Directive's requirement that organizations have a legal basis to process data does not always result in effective data protections or good privacy outcomes.

The Directive requires that organizations establish a legal basis for processing personal data,⁷ and enumerates six criteria by which processing is determined to be legitimate.⁸ The most significant of these criteria is informed consent of the data subject. To obtain such consent, companies must specify in their privacy policy the purpose for which the data will be processed. However, the ways in which data may be used evolve rapidly and may not be readily anticipated by companies. When data holds such broad and unanticipated potential, companies will hesitate to specify its criteria for processing, for fear of limiting their options to use data in unforeseen ways in the future. Such a requirement encourages instead creation of such broad privacy policies aimed at granting license to undertake any data activity companies see fit.⁹

⁷ Under the provisions of the Directive, processing includes the act of initial collection of data. EU Directive, Article 2 (c).

⁸ Criteria for making data processing legitimate include: 1) unambiguous consent by the data subject; 2) processing necessary to fulfillment of contract to which the data subject is a party; 3) processing necessary for compliance with a legal obligation to which the controller is subject; 4) processing necessary to protect the data subject's vital interests; 5) processing necessary to carry out a task in the public interest in the official authority vested in the controller or in a third party to whom data are disclosed; 6) processing necessary for purposes of the legitimate interests pursued by the controller or third party to whom data re disclosed, except where such interests are overridden by the interests of the fundamental rights and freedoms of the data subject. EU Directive, Article 7.

⁹ Because the most important legal basis for processing is informed consent of the data subject, individuals will be put in the position to police the market against bad actors on the basis of their understanding of highly complex and broad notices.

IV. The Directive does not in many cases serve the global nature of data flows, and does not sufficiently take into account the way in which data is collected, used, stored, shared and accessed.

The global flow of data drives today's information economy. Innovation, efficiency and service depend on rapid and reliable access to data, irrespective of its location. Digital technologies and telecommunications and information networks provide seamless, low-cost access to data around the world. Remote storage and processing of data "in the cloud" dramatically change and greatly enhance the way individuals and organizations access information and software services.

The Directive's rules applying to the transfer of data to third countries do not work well in this emerging data ecosystem. They require that data only be transferred to countries that are found by the Commission to have attained status as providing "adequate" protections for personal data. Fewer than 10 countries have been found to be adequate.¹⁰

Other legal mechanisms are available to support the transfer of data under the terms of the Directive, but these are cumbersome.¹¹ The one flexible mechanism for data transfer from

¹⁰ The European Commission has so far recognized Argentina, Canada, Faeroe Islands, Guernsey, Isle of Man, Jersey, the State of Israel, Switzerland and the US Department of Commerce's Safe Harbor Privacy Principles as providing adequate protection.

¹¹ Other legal mechanisms include unambiguous consent by the individual, participation in the U.S./EU Safe Harbor, transfer pursuant to fulfillment of a contract and model contracts for specific transfers. EU Directive, Article 7. Obtaining unambiguous consent is only possible when there is an equal relationship between the individual and the organization and cannot be used as the basis to transfer human resources data. EU/U.S. Safe Harbor is a bilateral process only available for transfers of data between the U.S. and the EU. Fulfillment of a contract is only available where the transfer of data is directly related to carrying out the terms of the contract. Model contracts must be reviewed and approved by the regulator and can take as long as six months to approve.

Europe is Binding Corporate Rules.¹² Gaining approval for BCRs is a lengthy and costly process, however, for both data protection agencies as well as companies, and does not scale to market demand.

The Directive also hinders the ability of organizations to engage in advanced processing activity such as analytics. Analytics involves an organization's broad analysis of data to determine what information the data itself can yield, its predictive value and whether it is sufficiently reliable that a company would act upon those findings. Analytics hold the potential to support powerful innovation, but the Directive's criteria for a legal basis for processing does not support their use.¹³

V. The Centre for Information Policy Leadership encourages consideration of alternative approaches to privacy and data protection that are based on fair information practices but that better reflect the realities of the evolving data environment.

The limitations of the Directive, as well as those of other regimes,¹⁴ suggest that other approaches to privacy and data protection would provide more effective protections for

¹² Binding Corporate Rules (BCRs) were developed by the European Union Article 29 Working Party to allow multinational corporations, international organizations and groups of companies to make intra-organizational transfers of personal data across borders in compliance with EU data protection law. BCRs were developed as an alternative to the U.S./EU Safe Harbor (which is available to US organizations only) and the EU Model Contract Clauses. BCRs typically form an intra-corporate global privacy policy that satisfies EU requirements and may be available as an alternative means of authorizing transfers of personal data outside of Europe.

¹³ Analytics represent another instance in which organizations may write broad and somewhat vague privacy policy notices to attempt to encompass a practice within the scope of the data subject's consent. See Section III.

¹⁴ Japan undertook a review of its Personal Information Protection Act (PIPA) in 2006, one year after its enactment. Canada's periodic review of Personal Information Protection and Electronic Documents Act (PIPEDA) is currently underway. The Australia Law Reform Commission (ALRC) reported its findings about the need for change in that country's data protection law in 2008, and the government issued its response in 2009. Draft changes to the law were issued in 2010.

consumers and enhanced flexibility for organizations to make optimal, yet responsible, use of data.

Current discussions in the United States and in international forums have considered several approaches that hold great potential for achieving this goal. We encourage the committee to consider these as it continues its work on privacy protections in the United States.

An *accountability* approach has figured prominently in policy deliberations both in the United States and abroad. Accountability is characterized by its focus on setting privacy-protection goals for organizations based on criteria established in current public policy and on allowing organizations discretion in determining appropriate measures to reach those goals. An accountability approach enables organizations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customer. It relies upon credible assessment of the risks (assisted by, *inter alia*, the use of privacy impact assessments), the use of data may raise for individuals and responsible mitigation of those risks.¹⁵

The essential elements of accountability may be summarized as:

- Organization commitment to accountability and adoption of internal policies consistent with recognized external criteria.
- Mechanisms to put privacy policies into effect, including tools, training and education.
- Systems of internal ongoing oversight and assurance reviews, and external verification.
- Transparency and mechanisms for individual participation.

¹⁵ This analysis is often referred to as one aspect of “privacy by design.”

- Means for remediation and external enforcement.¹⁶

The Centre also encourages the committee to consider work currently underway on a *use-and-obligations* approach.¹⁷ This model establishes the use rather than the collection of data as the primary driver of a data collector's obligations related to notice, choice, and access and correction. Under current implementation of fair information practices, consumer choice or consent to use data in certain ways establishes a company's responsibilities. A use-and-obligations model shifts responsibility for disciplined data use to the data collector and all holders of data, imposing requirements for transparency and notice, consumer choice, and access and correction on the data collector, based on the way the data is to be used.

The model takes into account all of the uses that may be required to fulfill the consumer's expectations and meet legal requirements. It imposes on organizations obligations based on five categories of data use: 1) fulfillment; 2) internal business operations; 3) marketing; 4) fraud prevention and authentication; and 5) external, national security and legal. It recognizes both aspects of a company's obligations, as articulated in fair information practices. The first includes the actions organization must take to facilitate individual participation — transparency (notice), choice, and access and correction. These ensure that an individual can know what data about him an organization is collecting or holds; can make choices about its use when practicable and

¹⁶ For a comprehensive discussion of an accountability approach to privacy protection, see "Data Protection Accountability: The Essential Elements," October 2009, <<http://www.ftc.gov/os/comments/privacyroundtable/544506-00059.pdf>>; and "Demonstrating and Measuring Accountability: A Discussion Document," October 2010 <http://www.huntonfiles.com/files/webupload/CIPL_Accountability_Phase_II_Paris_Project.PDF>.

¹⁷ The use-and-obligations approach is discussed fully in "A Use and Obligations Approach to Protecting Privacy: A Discussion Document," <http://www.huntonfiles.com/files/webupload/CIPL_Use_and_Obligations_White_Paper.pdf>.

appropriate; and can access and correct it in appropriate circumstances. The second includes the internal steps an organization takes to effectively manage data to minimize risk to both the organization and the individual — collection limitation and use minimization; data quality and integrity; data retention; security; and accountability.

VI. Conclusion

The limitations of the Directive discussed in this testimony highlight the challenges raised by advances in technology; innovative, complex business models; and the demand for nearly instantaneous movement of data around the globe. But in this rapidly evolving environment for data, notions of privacy remain based in local mores and cultures. Meeting the needs of the digital economy does not require countries to adopt each other's privacy values and approaches to protection, but to find ways to make those systems interoperable — respecting local privacy traditions while promoting the robust, protected flows of data necessary for a prosperity and economic growth.