

### A Note From the Publisher

Information is the currency of the twenty-first century, but until now there has not been a group of practitioners dedicated to consulting on the legal, strategic and policy issues this new medium raises for consumers, corporations and citizens. That is why Hunton & Williams founded the Center for Information Policy Leadership.

The Center for Information Policy Leadership provides a unique combination of strategic consulting, legal and policy development services for the information industry. Led by internationally known privacy experts, the Center assists companies with the development of a global privacy strategy.

The Center's approach shatters the paradigm of traditional legal advice by combining a privacy, security and intellectual property think tank, with a strategic information policy consulting practice.

The Center for Information Policy Leadership leverages Hunton & Williams unparalleled legal assets to better serve clients, consumers and society at large. We are moving beyond thinking of information as a purely legal problem and developing an enterprise approach to maximize the appropriate use of information.

The articles in this issue highlight the Center leaders' expertise on various facets of one of the most pressing of information issues: privacy. I am sure you will find them illuminating.



Thurston Moore  
Managing Partner

## Introducing the Center for Information Policy Leadership @ Hunton & Williams

Martin E. Abrams, Executive Director

Picture the world a hundred years ago, as capitalism spread the Industrial Revolution to every corner of the planet. This first wave of globalization promised a whole new world order in which everybody linked to everybody else in economic relationships, but which could not come to fruition without rules for the movement of capital — and the development of modern monetary policy.

Today our world currency is increasingly information, and we are in the same position as our forebears. Until we formulate rules to enable the easy movement of information, we can't take full advantage of the possibilities of a global world. It took over a hundred years to discover the rules for the movement of capital, and the false starts made along the way, from the failure of the Bank of the United States to the Great Depression, caused much real suffering. In the same way, the wrong rules for information will imperil all the social gains of becoming an information-based society and economy — and we don't have the kind of time our forebears did.

To jump-start the process of finding the right rules, Hunton & Williams created the Center for Information Policy Leadership, a place where appropriate information policy can be developed and refined in the same way that monetary policy has evolved to facilitate economic growth. We are interested in moving beyond questions to answers.

The Center for Information Policy Leadership is both a privacy, security and intellectual property think tank and a strategic information policy business consulting practice. Our policy perspectives are tempered by practical business process knowledge, gained from our corporate experience and our continued active participation in the debate on how to appropriately reap all of the benefits of our information economy. I am not an attorney and the Center doesn't engage in the practice of law. Rather, we leverage The Hunton & Williams established Privacy and Information Management practice — the most innovative group of its kind in the legal profession — to provide strategic

consulting and thought leadership on all aspects of information policy, including privacy, security, intellectual property and the many ways to generate value from consumer data.

The drawback to a typical lawyering approach is that it's based on compliance. It's not business-oriented. It's what I call a "you can't" approach: pure compliance only tells you what's prohibited, without the ability to answer the really important question: "If I can't do that, what can I do?" The Center is different. We're solution-oriented: to move beyond questions to answers is to focus on what will work. We're practical — we're all experienced in real business and technological practices. We're moving beyond thinking of information as a purely legal problem and developing an enterprise approach to appropriately reap all of the benefits of our information economy. And because we believe that our thought leadership and strategic advice have to reinforce each other, we've created a consulting methodology called PRISM (Policy Refinement & Information Solutions Management).

PRISM enables a company to develop a value-based, enterprise-wide information management cost effective program to meet its legal, business and policy needs, based on best practices and consistent with the company's culture. Just as a prism combines the diverse colors of the rainbow to create a single brilliant illuminating beam, the Center uses dialogue to focus the manifold insights of thought leaders, privacy officers, other executives, consumer advocates, policy makers, academics and others. The result is a deep understanding of the data collection, storage, use, protection and communication practices of complex organizations.

The Center helps policy executives, corporate lawyers and other business leaders:

- anticipate and resolve complex privacy and security problems
- build stronger, more interactive relationships with their customers, investors, regulators and consumer advocates
- develop tools and solutions through peer relationships with other senior policy leaders and outside experts
- influence future standards, laws, and media stories.

We achieve our goals through focused industry discussion groups on various information policy topics as well as broader dialogue groups of industry leaders, consumer advocates and policy makers on information policy topics. Current programs include:

### The CRM Education Project

The Customer Relationship Management Education Project is a monthly industry discussion group and semi-annual public dialogue group that explores the use of information and information technology in marketing, customer service and fulfillment as well as the nature of the public's interest in customer relationship management. The Project members are developing policy models to ameliorate the friction between individuals' multiple interests in the data flows that support marketing.

### The Global Concerns Project

The Global Concerns Project enables government officials, multinational companies and scholars to explore new policy models to reduce the tension that exists between traditional data protection regimes and the need for robust data flows in our global information-based economy. Participants examine the barriers to successful adoption of information-based processes and existing policy models, develop basic tools to achieve balance between privacy, security, individual opportunity and corporate growth, and generate policy models to serve as the basis for new legal approaches to global privacy protection.

These objectives are achieved through an ongoing series of industry discussions and public symposia. Current discussion topics include global customer relationship management, the US-EU safe harbor arrangement and alternatives to omnibus data protection laws, harmonization of international data protection laws, the economic implications of data protection, the impact of technology convergence on data protection, and emerging data protection regimes in the Asia-Pacific and Latin American regions.

### The CPO Solutions Project

The Chief Privacy Officer Solutions Project provides chief privacy officers, general counsel and other senior executives with solutions to some of the challenges that face large corporations that collect or use large sets of customer, consumer or employee data. Our focus is on the development of tools necessary to be successful as a privacy policy leader rather than on current events or new public policy. Privacy executives participate in conference calls, networking sessions and highly targeted training programs to explore new approaches to the problems associated with security, communications, data flow audits, consolidation of internal policies, vendor and customer management, documentation, access and correction requirements, implementing opt-out or opt-in regimes, privacy training, accountability and responding to enforcement actions and adverse consumer or media scrutiny.

### The Regulated Industries Project

Companies in the financial, insurance and healthcare industries are now required to implement omnibus privacy provisions of Gramm-Leach-Bliley and/or HIPAA as well as to manage new risks associated with Fair Credit Reporting Act compliance examinations. The Regulated Industries Project enables companies in these highly regulated industries and their trade associations

understand and manage the strategic, tactical and operational issues related to compliance with complex and comprehensive privacy and security regulations. Participants explore management of the risks associated with credit and insurance marketing as well as the use of health information under GLB and HIPAA, the new FCRA compliance examination process, the tension between GLB and the FCRA for notices and affiliate sharing, the friction between drafting accurate notices and readable notices, state proposals to expand the requirements of GLB and HIPAA, and complex opt-in and out-of choice schemes for use of financial and medical data.

This special issue of *Spotlight* features articles by Center leaders showcasing our major capabilities, strategic consulting initiatives and thought leadership. Peggy Eisenhauer, the privacy and information management practice group leader, explains how companies can structure enterprise-wide privacy policies, and why they need them; Oscar Marquis, the financial privacy practice leader, describes the problems posed by GLB and the FCRA for notices and information sharing; Lisa Sotto, our privacy regulatory practice leader explains the current state of privacy regulation in the insurance industry; and Lucas Bergkamp, the international data protection practice leader, presents his analysis of the Internet's impact on data protection in the European Union. I hope you find it enlightening.

# Why You Need An Enterprise-Wide Privacy Policy

Peggy Eisenhauer



Today, when information fuels the growth of every business, corporations develop and maintain their competitive advantages by using consumer data appropriately and aggressively. To be successful, companies must develop coherent and comprehensive information management strategies, and the linchpin of a profitable information management vision is an enterprise-wide privacy program. With the Internet driving down the cost of collecting, storing, manipulating and distributing personal data, and with the value and utility of data increasing as our ability to leverage it improves, there are very few disincentives to collecting data on U.S.-based consumers—except the public concern, inflamed by eager newspapers and politicians (it’s always an election year for someone) over privacy violations. That public fear is driven by three conflicting desires and attitudes:

1. People want to be secure—but feel vulnerable;
2. People want a sense of control—but see chaos; and
3. People want all the benefits of a digital age—but don’t understand how those benefits depend on the flow of information they want to keep “private.”

The conflict between these attitudes leads to the central dilemma confronting every business that uses customer information. In order to satisfy consumers’ desire for trust and autonomy, companies must use information with restraint; but in order to satisfy both the consumer and shareholder demand for added value from new technology, companies must use information robustly.

It’s not hard to understand how to resolve the dilemma in the abstract. On the basis of its own distinctive corporate culture and values, each company must formulate its own program for achieving some basic corporate policy goals, including:

- Development of internal corporate information policy values;

- Development and implementation of cost-effective, data use and privacy procedures that maximize customer and business partner confidence as well as revenue and business practices flexibility;
- Advocacy and compliance with U.S. and international privacy and data protection laws and self-regulatory schemes;
- Communication of the corporate values and policies to internal and external audiences;
- Proactive monitoring, affirmation and education.

But putting these goals into practice can be a bewilderingly complex job. There are simply too many different interests and constituencies to deal with: industry and international trade associations, digital signature and seal providers, the media, competitors, consumer advocates and consumers. That isn’t even counting a bevy of regulators including Congress, state legislatures and Attorneys General, the Federal Trade Commission, other federal agencies, and their counterparts in Canada and the European Union, all contributing to a rat’s nest of regulation that includes self-regulatory schemes and online privacy seals, federal laws (such as the Fair Credit Reporting Act, Gramm-Leach-Bliley, the Children’s Online Privacy Protection Act and the new HIPAA healthcare privacy rules), state initiatives (including the Drivers Privacy Protection Act) and

international data protection laws. Throw in non-privacy laws that can impinge on the area, such as the various unfair trade practices acts which create enormous liability for companies that post privacy statements or send privacy notices but whose practices don’t

exactly match the text that they’ve drafted, and you have alphabet soup. Can you spell “unpalatable”?

Not only are there too many players, there are too many places where privacy issues can arise. Not just in the actual development of privacy policies, but in any





technology-related transaction, including development of new products/markets/channels/geographies; development of advertising materials and promotional campaigns; preparation of agreements covering marketing, data sharing, promotion, e-commerce and outsourcing; resolution of consumer complaints, litigation and investigations by enforcement authorities; due diligence in the merger and acquisition process and disclosures to securities regulators and venture capitalists.

Add to all this the need to balance the legal and business sides of the equation (legal compliance is essential, of course, but a company's privacy values and policies should be determined by its business context), and it's evident that no company can solve the central dilemma on a piecemeal, case-by-case basis. Corporations today can scarcely do without a privacy policy thought leader to understand and help define corporate information policy values.

The Hunton & Williams privacy lawyers help corporate privacy executives manage the muddle in many different ways. For example, we can:

- Provide traditional legal advice regarding compliance with laws;
- Give business advice regarding best practices, business risks and benefits;

- Craft enterprise-wide solutions that meet consumer and policy expectations while providing the company with appropriate data flow opportunities;
- Help establish the right balance for the company, given the company's culture and corporate goals.

We also facilitate the company's ongoing process of developing an enterprise-wide privacy program by helping the company to:

1. Consider its corporate culture and values;
2. Understand its data collection and sharing practices—and make sure that everyone else in the company understands them too;
3. Brainstorm about long-term data, technology and product goals;
4. Analyze industry practices and the regulatory climate, then evaluate the legal and business risks and advantages of policy choices;
5. Formalize implementation controls, testing and documentation;
6. Prepare consumer-oriented privacy notices that educate in plain English and that serve as business and marketing tools for customers, investors and other stakeholders;
7. Establish an “affirmation-education cycle” to help the company monitor law and media for needed adjustments.

The result is a solution, not a set of *ad hoc* decisions, geared to corporate business objectives with an eye towards legal compliance, crafted with a customer orientation and clearly articulated to all audiences.

Hunton & Williams' PRISM approach allows us to create values-based information management programs that meet legal, business and policy needs in a manner consistent with the company's culture. The PRISM approach enables companies to reduce cost by managing privacy issues effectively and maximizing their return on investment in information and information technologies. The Hunton & Williams privacy experts—lawyers who provide strategic business consulting on all aspects of information policy, business people who truly understand how information flows drive revenue—can provide business-oriented solutions that balance the need for free flows of information with the desire for customer and consumer autonomy to resolve the central dilemma.

# Challenges To E-Commerce Posed By Europe's Data Protection Legislation

Prof. Lucas Bergkamp  
Jan Dhont

The European Union has long been concerned about threats to privacy. In 1995, the EU legislative body adopted general principles on individual privacy and data protection in Directive 95/46/EC (the "Data Protection Directive" or "the Directive"). Applying the Directive to on-line data processing is fraught with difficulties, not all of which were resolved by a November 2000 report from the EU Privacy Working Party.

## The Data Protection Directive: Basic Provisions

The Data Protection Directive applies to the processing of personal data regardless of the technical means used, including the Internet. The Directive:

- imposes restrictions on personal data processing;
  - grants individual rights to "data subjects," including protection from certain nonconsensual uses of personal data;
  - sets forth specific procedural obligations, including notification of processing operations to national authorities.

## Scope and Key Definitions

The directive's definitions raise many questions. For instance:

- The definition of "processing" is so broad that virtually all data operations from "cradle" (collection) to "grave" (destruction) are deemed to be the processing of data;
- Identifying a "data controller," defined as "the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data," is difficult in an open network.
- "Personal data" as that term is defined in the Directive, *i.e.* "any information relating to an identified or identifiable natural person" is also difficult to ascertain.

Consider user-related data—electronic data generated when a user connects to and uses the Internet, such as an IP number. If the IP number is not person-specific but assigned only for a particular session, and changes regularly, it does not constitute "personal data." Most access providers, however, demand the user's name and address before offering their services. In these cases, the IP number and traffic and navigation data (e.g. URLs) might constitute "personal data" as that term is defined in the Directive—if the specific individual to whom these data pertain can be traced.

*continued on page 12*



# The Impact of Privacy Requirements on the Insurance Industry

Lisa J. Sotto

During the next several years, providers of consumer insurance products will face increasingly complex federal and state privacy requirements. With the first compliance deadline having passed on July 1, 2001, privacy laws and regulations have already become a critical business issue. This article provides a broad overview of the current state of United States privacy laws<sup>1</sup> and regulations that will affect insurance providers.<sup>2</sup>

## I. Gramm-Leach-Bliley Act

On November 13, 1999, Congress enacted the Gramm-Leach-Bliley Act (“GLB” or “Act”).<sup>3</sup> Title V of the Act contains comprehensive federal privacy protections for consumers and applies to all financial institutions, including insurance companies. Insurers need to have substantially complied with GLB’s requirements by July 1, 2001.

The Act’s privacy provisions establish new requirements applicable to “nonpublic personal information.” The federal agencies implementing GLB believe that any information obtained by a financial institution in connection with providing a “financial product or service” is protected, even if the information is not typically considered to be financial in nature.

To comply with GLB, financial institutions must:

- provide clear and conspicuous notice of their information-sharing policies to customers annually;<sup>4</sup>

- clearly provide consumers the right to opt out of having their nonpublic personal information shared with nonaffiliated third parties;
- refrain from disclosing to any nonaffiliated third party marketer, other than a consumer reporting agency, an account number or similar form of access code to a consumer’s credit card, deposit or transaction account; and
- abide by regulatory standards to protect the security and confidentiality of customer records and information.

These provisions do not preempt more stringent state law privacy protections. With respect to insurers, GLB mandates enforcement by the state insurance authority of the state in which the insurer is domiciled. If a state fails to adopt regulations to enforce the Act, it will lose its authority to override certain federal insurance consumer protections.

## A. State Insurance Authorities: Compliance with GLB

Congress instructed state insurance departments to provide privacy safeguards, equivalent to those in GLB, for individuals in their dealings with the insurance industry. State authorities have responded principally with two model enactments, the National Association of Insurance Commissioners (“NAIC”)’s Privacy of Consumer Financial and Health Information Regulation (the “Regulation”), and the Financial Information Privacy Protection Model Act, adopted by the National Conference of Insurance Legislators. Both generally track GLB, but contain one significant variation: they distinguish “financial” information from “health” information. Under the Regulation, for example, a “licensee” (insurers, producers or others who are or should be licensed pursuant to state insurance laws) may

1) The five “fair information practice” principles—notice, choice, access, security and enforcement—initially announced by the Federal Trade Commission (“FTC”) have evolved into the *de facto* standard for corporate privacy assessments. Even though they are not mandated by law, all companies need to take these principles into account when devising a privacy compliance program.

2) In addition to U.S. requirements, each company should consider whether it needs to comply with the European Union’s Directive on the Protection of Personal Data, Directive 95/46/EC and the related safe harbor principles of the U.S. Department of Commerce.

3) Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999) (“GLB”).

4) A “customer” is defined as any person to whom a financial institution provides a product or service.

disclose nonpublic personal financial information to nonaffiliated third parties only if the consumer does not opt out. With respect to nonpublic personal health information, a licensee is prohibited from disclosing such information without specific authorization, i.e., an “opt-in,” from the customer or consumer whose information is sought to be disclosed. The exceptions to disclosure are so broad, however, that they effectively allow nearly unlimited operational use of covered health information, except for certain marketing uses.

## II. HIPAA

The U.S. Department of Health and Human Services (“HHS”) recently issued its final rule (the “Rule”) implementing the privacy requirements of the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”).<sup>5</sup> Covered entities generally must comply with the Rule by April 14, 2003.<sup>6</sup>

The Rule applies directly to (i) health plans (including “health insurance issuers” such as insurance companies), (ii) health care clearinghouses, and (iii) health care providers who transmit health information in electronic form. The Rule generally covers uses and disclosures of “protected health information,” defined as certain types of “individually identifiable health information.” It requires health plans and health care providers to provide individuals with written notice informing them of how protected information will be used and disclosed, as well as with a right of access to inspect, copy and amend protected health information maintained in designated record sets. It establishes restrictions on requests for, and use and disclosure of, protected health information—in most cases, to the minimum necessary to serve the purpose of the use, disclosure or request. It distinguishes between “consent” and “authorization.” Generally, providers must get consent from patients for routine

disclosures of medical information and special patient authorization for non-routine disclosures.

To comply with the Rule, covered entities will need to modify their current practices in a number of ways. These include designating a privacy officer who will be responsible for the development and implementation of the covered entity’s privacy policies and procedures; revising consent and authorization forms; developing procedures for storing information to enable data tracking and access; entering into carefully drafted contracts with business associates; and training employees as to the Rule’s requirements. Covered entities also will need to provide a process for individuals to make complaints concerning the covered entity’s privacy procedures and its compliance with such procedures.

## III. Conclusion

To comply with GLB and the HIPAA Rule, each insurance provider should consider implementing a multi-faceted compliance program that contains both legal and business components. This compliance program should begin with a survey to determine which state’s laws apply. Simultaneously, the company needs to conduct an assessment of its uses and disclosure of personal information, and prepare the necessary notices, consents and authorizations. Each company also will need to devise a method by which to track opt-outs so opt-out information is not illegally disclosed, and implement a system to respond to changes in its information-sharing practices. Now that the July 1, GLB compliance deadline has passed insurers that have sent out their GLB notices can begin to implement the systemic changes necessary for continued compliance with GLB and consider how they will comply with the onerous requirements of the HIPAA Rule.

<sup>5</sup> Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. 160 and 164).

<sup>6</sup> Small health plans have an extra year to comply.

# Sorting Through Privacy Notices Under The Fair Credit Reporting Act and Gramm-Leach-Bliley

Oscar Marquis

Are privacy notices getting out of hand? The regulatory requirements have become so complex that financial institutions cannot comply with the law and still prepare notices that consumers can understand. Such convolution defeats the purpose—and, ironically, is not really required by the underlying law.

Under the Gramm-Leach-Bliley Act (GLB), financial institutions must tell their customers that their information

may be shared with affiliates and nonaffiliates. The customers have a choice over information sharing with nonaffiliates, but no choice with respect to affiliates. Under the Fair Credit Reporting Act (FCRA) notice requirements, [contained in pending regulations reported at 16 C.F.R. Part 600], financial institutions have to tell their customers that some information covered by the GLB may be shared with affiliates.

Furthermore, under the FCRA, customers can forbid this sharing with affiliates. But they have no choice under FCRA about nonaffiliates sharing. GLB—information shared with affiliates—no choice. FCRA—information shared with affiliates—choice. GLB—information shared with nonaffiliates—choice. FCRA—information shared with nonaffiliates—no choice. How can a consumer keep it straight?

And what information is covered? Under GLB, it's “nonpublic personal information,” which the regulators essentially define

as all account application information, and the subsequent account history. Under FCRA it's “opt out information,” which the regulators define as information from third parties or from an application. The proposed regulations specifically exclude account history.

How can a consumer make heads or tails out of this morass? How can a financial institution provide a meaningful notice that explains what is covered, what choices there are, and how the financial institution may use the information? Is this logjam really necessary?

The FCRA notice isn't necessary for most financial institutions—only for “consumer reporting



agencies.” In part, the problem is a desire by regulators to make privacy a competitive issue; to make institutions compete based on how they share and use customer information. Although it may not have been the objective of Congress, regulators clearly hope that some financial institutions will not share customer information with third parties and use that as a marketing advantage.

The regulators found a rationale for the notice in the FCRA amendments of 1997. The definition of “consumer report” was modified to exclude account history information. It also excluded certain information shared with affiliates, such as the consumer report obtained when the account was opened, or information from an application, if institutions notified customers and provided an opportunity to opt out of the information sharing with affiliates. So certain communications that would otherwise be consumer reports are not consumer reports if the notice and opt-out choice were provided. This means that the definition simply does not apply to communications that are not consumer reports. Therefore, no disclosure of such communications is necessary under the FCRA.

And therein lies the point: in general, financial institutions do not issue consumer reports to affiliates. The regulators forgot that to be a consumer report, information must, in addition to having a bearing on credit eligibility, be communicated by a

consumer reporting agency. To be sure, the definitions in FCRA are somewhat circular. But they are clear that a consumer reporting agency is defined as an entity that collects certain information “for the purpose of furnishing consumer reports to third parties.” In other words, an entity can collect information that has a bearing on the creditworthiness factors, obtain it to establish credit eligibility, maintain account history or experience information and communicate all of it but still not be a consumer reporting agency if the information was not collected for the purpose of furnishing consumer reports. It is not collected for the purpose of furnishing consumer reports if it is not communicated to third parties to serve as a factor in establishing credit eligibility. That is the unique element that defines why courts, secretaries of state, schools that issue transcripts, reference services and others are not consumer reporting agencies.

The bottom line for financial institutions: the final regulations should recognize what the law says and make clear what kinds of communication are covered. Then a financial institution will not need to be concerned with the complex FCRA notice rules if it does not assemble information for the purpose of furnishing consumer reports. Information can be communicated among affiliates for collection purposes, for processing, for servicing the account, for marketing or any other non-eligibility purpose. The morass of never-ending and ever more confusing notices can be avoided.

## Senior Policy Advisor Joins Center



Fred H. Cate, Professor of Law and Ira C. Batman Faculty Fellow at the Indiana University, joined the firm in July 2001 as a senior policy advisor. Fred is a senior fellow in the Center. Widely regarded as the leading voice for the free flow of

information in digital age, Cate is a leading architect of the global privacy solutions that are emerging from the Center.

Cate is the author of many articles and monographs and has appeared on CNN, PBS, and many local television and radio programs. During the 2000 presidential campaign he was a policy advisor on

privacy and information control issues to George W. Bush.

Cate frequently testifies before Congress and federal regulatory agencies on topics such as privacy in electronic communications, privacy and the commercial world and financial privacy. Most recently, he appeared before the Senate Committee on Commerce, Science & Transportation in July 2001 to argue that hard consumer behavior data shows that most consumers don't actually want to exercise choice. Therefore the costs of opt-in to both consumers and businesses are too high; opt-out gives consumers control of data without placing costs on other consumers.

continued from page 7



### The Directive: Territorial Scope of Application

The Directive's territorial scope is broad. The Working Party has opined that the Directive is applicable to controllers that are not established in the EU

but process data submitted over the Internet by data subjects in a Member State, because the data controller "uses equipment" in the territory of a Member State in this situation (where "use" excludes the mere transmission of data). However, the Internet makes this broad interpretation of "use of equipment" questionable and impractical. If a United States company uses a server located in the EU to host its web site, the Directive would apply, even if no data of EU nationals are processed.

### User Autonomy and the Right to Consent

The Directive's purpose is the protection of individual privacy. Accordingly, the "unambiguous consent" of the data subject is necessary for the processing of personal data by a third party. Necessary but not sufficient: under the Directive, data processing must also be fair and take into account the data subject's interests. (These terms are not further defined.) The distinction is relevant to individual privacy preference schemes, under which an Internet user consents to a service provider's collecting personal data if the site's declared privacy practices and other conditions satisfy the user's requirements. User consent, however, does not necessarily mean a web site's privacy practices will be deemed "fair" and balanced under EC law.

### Users' Right to Information About Uses of Their Data

Hyperlinking, "cookies" and chattering of browsers are generally deemed impermissible if the Internet user is not adequately informed. The Working Party has taken the position that Internet software and hardware

products should:

- provide Internet users information about the data that they intend to collect, store or transmit;
- provide information about the purpose for which the data are necessary; and
- enable a data user to easily access any data collected about him at any later stage.

### A Threat to Direct On-line Marketing?

The data subject has the right, free of charge and without stating a reason, to object if processing is done for purposes of direct marketing, both off-line and on-line. Under forthcoming legislation, however, the consent of each individual prospect would be required for unsolicited e-mail communications for direct marketing purposes. This proposed regime would have a chilling effect on direct on-line marketing.

### U.S. Companies Need a Culturally Sensitive Information Management Strategy

The Data Protection Directive creates a complicated regime for the protection of privacy, encompassing virtually all data relating to a person. Key definitions raise issues for data processing on the Internet. The fairness standard necessitates a balancing of the controller's and data subject's interests in each individual case. All this means serious legal uncertainty and exposure to the broad discretionary powers of national data protection authorities for on-line marketers and e-traders.

Corporations that handle personal data from European residents therefore need to assess their practices and policies carefully. Adequate information management policies and strategies are essential, but dealing with European consumers also requires an understanding of the regulatory environment and sentiment. US corporations should keep in mind that consent is not necessarily enough. The restrictions set forth in the law are broad, and there are no regulations that provide further guidance on their scope. Dealing with the government agencies that interpret these laws is an art in itself. Managing data of Europeans thus is a formidable management challenge.

*Hunton & Williams, a major international law firm, publishes this newsletter to highlight the opportunities and challenges businesses face in the global economy and to illustrate innovative solutions to help companies achieve their objectives.*

*For more information about the Center for Information Policy leadership at Hunton & Williams, please visit [www.policyleaders.com](http://www.policyleaders.com) or call Marty Abrams at 404-888-4274*

[www.hunton.com](http://www.hunton.com)