

304 Global Privacy Issues

Laura Keidan Martin

Partner

Katten Muchin Zavis

Timothy J. Mahota

General Counsel

Integral Development Corporation

Kathleen A. Murray

Senior Counsel

Fireman's Fund Insurance Company

Steven M. Roberts

Partner in Charge—KPMG LLP

National Regulatory and Compliance Advisory Services

Faculty Biographies

Laura Keidan Martin

Laura Keidan Martin is a partner in the Health Care Department of Katten Muchin Zavis(KMZ), Chicago, and is cochair of KMZ's Antitrust Practice Group. She is also a member of the KMZ Health Care Compliance Group and HIPAA Task Force.

Ms. Martin's broad-based health care practice includes mergers and acquisitions, physician integration strategies, provider joint ventures, and e-health startups. She has counseled hospitals, health care management companies, managed care entities, venture capital firms and a variety of other health care clients, helping them structure their affiliations, mergers, acquisitions, joint ventures, marketing practices, and management arrangements to comply with state and federal regulatory requirements ranging from fraud and abuse to privacy requirements. She is assisting several clients in the development of corporate compliance plans and HIPAA policies. Ms. Martin also provides antitrust advice to clients in a number of industries, ranging from high-tech to manufacturing.

Ms. Martin has delivered speeches at numerous national forums on a variety of topics, including health care joint ventures, criminal conspiracies in the health care industry, fraud and abuse and antitrust compliance plans. She is a past articles editor of the ABA Section of Antitrust Law's *Antitrust Health Care Chronicle*, and she is a member of the Chicago and American Bar Associations, as well as the American Health Lawyers Association and the Illinois Association of Health Care Attorneys.

Ms. Martin earned her BA with high distinction from the University of Michigan and graduated *cum laude* from Harvard Law School.

Timothy J. Mahota

Timothy J. Mahota is general counsel for Integral Development Corporation in Mountain View, California. He is responsible for the overall legal services to this international software company serving the financial services industry. His areas of specialization are securities law, ERISA, information technology, and licensing.

Prior to joining Integral, Mr. Mahota served as general counsel to Mercer Global Advisors, Inc., a national investment advisor and broker-dealer. Before that, Mr. Mahota served as an attorney at the Securities and Exchange Commission (Enforcement) and at the Pension Benefit Guaranty Corporation.

Mr. Mahota serves on the Department of Labor's ERISA Advisory Council by appointment for former Secretary of Labor Alexis Herman. Mr. Mahota is the chair of ACCA's ERISA Subcommittee, is on the *ACCA Docket* Advisory Committee, and participates in numerous securities organizations.

Mr. Mahota received a BA from John Carroll University, a JD from Ohio State University, an LLM in securities regulation and Certification in Employee Benefits Law from Georgetown University Law Center.

Kathleen A. Murray

Kathleen A. Murray is senior counsel with Fireman's Fund Insurance Company in Novato, California. Her primary areas of responsibility include employee benefits and executive compensation.

Prior to joining Fireman's Fund, Ms. Murray was associate general counsel with the California State Automobile Association in San Francisco.

Ms. Murray serves as vice chair of the ERISA subcommittee of ACCA's Labor and Employment Law Committee and is treasurer and a member of the board of directors of ACCA's San Francisco Bay Area Chapter. She is also a member of the Cyberspace Law Committee of the State Bar of California, the Western Pension and Benefits Conference, and the Bar Association of San Francisco. Ms. Murray has been active with a number of educational institutions in San Francisco, including San Francisco Infant School, Pacific Primary School, San Francisco Day School, and Lick Wilmerding High School.

Ms. Murray received a BA from the University of Michigan and a JD from Hastings College of the Law.

Steven M. Roberts

Steven M. Roberts is a principal and partner in charge of KPMG LLP and has executive responsibility for regulatory and compliance advisory services, which is comprised of professionals working in various industries that are most affected by government regulations and reporting requirements. This network provides major U.S. and international clients with information and direction that lets them anticipate and respond quickly and accurately to new and more complex federal and state regulatory developments. Mr. Reynolds is actively involved in financial services regulatory and compliance advisory services, and is the lead partner for those services that are offered to banks, securities firms, and insurance companies.

Prior to joining KPMG, Mr. Reynolds was the assistant to Paul A. Volcker, chair of the board of governors of the Federal Reserve System, and previously chief economist for the U.S. Senate Committee on Banking, Housing, and Urban Affairs. He also was vice president for government affairs at American Express, responsible for federal government issues affecting banking, trade, taxes, and travel and tourism.

Mr. Reynolds holds a BA from Rutgers University and an MS and PhD from Purdue University.



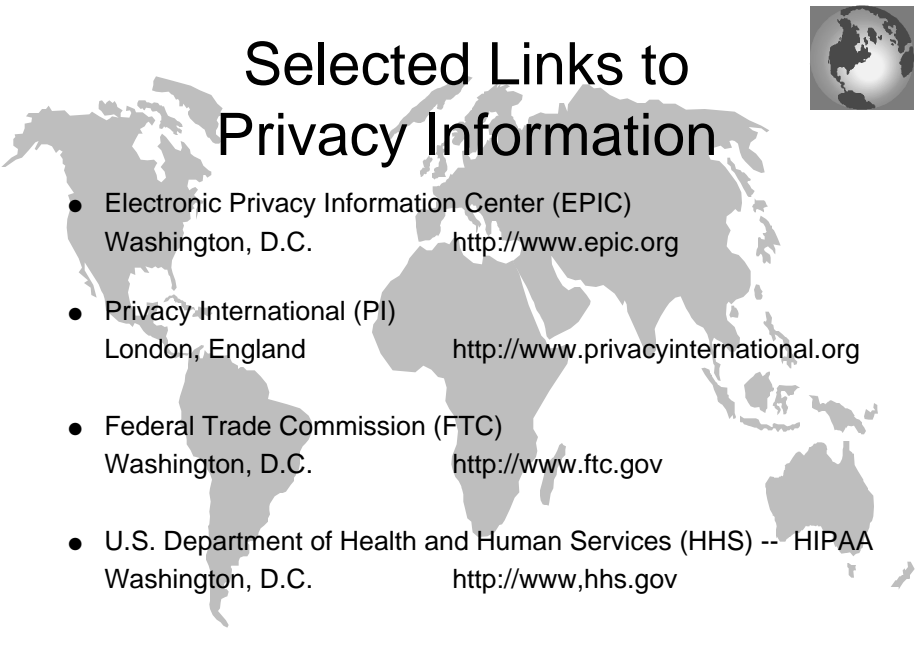
Global Privacy Issues

American Corporate Counsel
Association
October 16, 2001
San Diego, CA




The Privacy Revolution

- International in scope
- Laws and regulations are proliferating
- Definitions of protected information vary
- Compliance is costly
- Consumer awareness is growing



Selected Links to Privacy Information

- Electronic Privacy Information Center (EPIC)
Washington, D.C. <http://www.epic.org>
- Privacy International (PI)
London, England <http://www.privacyinternational.org>
- Federal Trade Commission (FTC)
Washington, D.C. <http://www.ftc.gov>
- U.S. Department of Health and Human Services (HHS) -- HIPAA
Washington, D.C. [http://www,hhs.gov](http://www.hhs.gov)



INTRODUCTIONS

Financial Services Privacy Issues
Steven M. Roberts
KPMG, LLP, Washington, D.C.

HIPAA Overview
Laura Keidan Martin
Katten Muchin Davis, Chicago, IL

European Union Data Protection Issues
Tim Mahota
Integral Development Corporation, Mountain View, CA

Moderator
Kathleen Murray
Fireman's Fund Insurance Company, Novato, CA

Global Privacy Issues Financial Services

American Corporate Counsel Association
Annual Meeting, San Diego, CA
October 16, 2001

Steven M Roberts, Partner

KPMG LLP

Sroberts@kpmg.com

KPMG LLP

Privacy

"You have zero privacy anyway.

Get over it."

Scott McNealy, Sun Microsystems

KPMG LLP

Privacy

"On the Internet, even more than in other areas of our lives, trust is the real currency"

Scott McNealy, Sun Microsystems May 29,2001

KPMG LLP

What Privacy Is

- Access and control over information about people or institutions in all media
- Records of their preferences for managing this information

KPMG LLP

What Privacy Isn't

- Security – enables private information to stay private
- Intellectual property – entails the ownership and use of content

KPMG LLP

The Gramm Leach Bliley Act – Title V

- Discloser of privacy policies and practices
- Notification of policies and practices to customers at least annually
- Customers opportunity to "opt-out" of sharing of their personal non-public financial information with non- affiliated third parties
- Program, approved by BoDs to protect the security and confidentiality of customer records
- Service providers must keep information secure and confidential

KPMG LLP

The Gramm Leach Bliley Act – Title V

- Regulations adopted by federal financial services regulators for financial services providers other than insurers- FRB, OCC, OTS, SEC, NCUA, FTC, CFTC, Treasury
- NAIC adopted model law in October 2000
- Effective date for compliance was November 13, 2000, compliance required by July 1, 2001
- States can enact rules that are more stringent than federal law and regulation

KPMG LLP

Legislation affecting Financial Services

- HIPAA relating to medical information privacy
- European Privacy Data Directive effective 1/25/98 – no "safe harbor" for financial services companies
- Canada
- Pending federal legislation
- Pending state legislation

KPMG LLP

Financial Services Privacy Lawsuits

State A.G.'s and FTC bringing unfair or deceptive trade practices, fraud, breach of contract suits

- Minnesota AG - US Bancorp of Minneapolis
- MY AG - Chase Manhattan for not abiding by own policies and procedures concerning sharing of confidential information
- Minnesota AG - Fleet Mortgage for illegally sharing of confidential information with telemarketers

KPMG LLP

Privacy also covers

- FTC has indicated that law firms are covered by GLBA when they receive confidential customer information
- FDIC has indicated that accounting firms are covered by GLBA as services providers

KPMG LLP

Why Should Privacy Be Important to Our Companies?

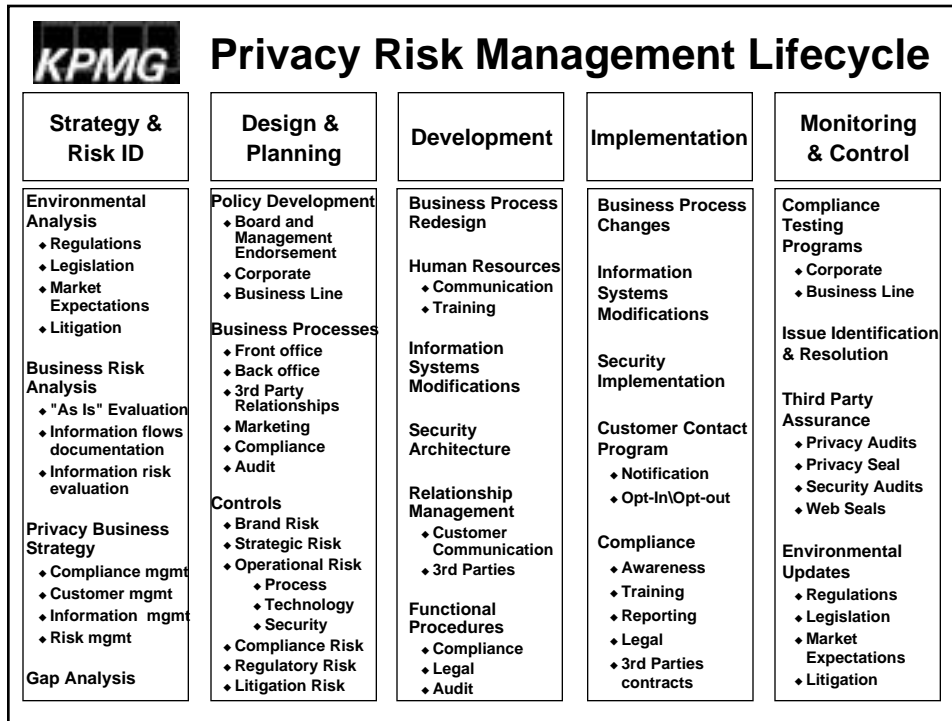
- Risk mitigation
 - ✓ Compliance
 - ✓ Litigation and enforcement
 - ✓ Reputation
- Process and cost efficiency
- Asset protection
- Constituent trust


KPMG LLP


Privacy – Mandatory Issues

- Understand your flows and uses of information about customers
- Know the scope of information and processing efficiency
- Mitigate privacy risks
- Build covenant of trust with customers

KPMG LLP



	Katten Muchin Zavis
	<i>Global Privacy Issues: HIPAA Overview</i> <i>Presented by Laura Keidan Martin</i> ACCA Annual Meeting 2001 San Diego, CA October 16, 2001

	K M Z
	<i>Overview of Presentation</i> <ol style="list-style-type: none">1. What is HIPAA2. Who is Affected3. The Privacy Rules4. Business Associate Rule5. Penalties6. HIPAA Compliance

K M Z

What is HIPAA?

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a sweeping regulatory initiative covering patient privacy, security standards and transaction codes.
- The privacy regulations became final on April 14, 2001 and covered entities have until April 14, 2003 to comply.

K M Z

HIPAA Impact

- Most significant health care regulatory scheme since establishment of Medicare.
- Potentially four times cost of Y2K compliance for covered entities.
- Cost to the economy for all HIPAA compliance could be as high as \$2 Trillion.

K M Z

Who is regulated by HIPAA - Covered Entities

- HIPAA directly regulates three types of covered entities:
 - Health Care Providers, including employees with on-site clinics, that engage in certain electronic transactions.
 - Health Plans, including employer-sponsored group health plans that have 50 or more participants or are administered by a third party.
 - Health Care Clearinghouses, including TPAs and billing companies.

K M Z

Who is affected by HIPAA - Business Associates

- Business Associates: HIPAA indirectly regulates any entity that does business with a covered entity and has access to individually identifiable health information.
 - Employers: Employers are considered "business associates" of their sponsored health plans -- to the extent the employer receives PHI from the plan.

K M Z

What Information is Covered?

- The Privacy Rules apply to all individually identifiable health information maintained by a Covered Entity (also known as "protected health information" or "PHI").
- The Privacy Rules cover PHI in all media: electronic, paper or oral.

K M Z

The Basic Privacy Rule

- A Covered Entity (and its Business Associates) cannot access, use or disclose PHI without a properly executed consent or authorization form from a patient unless an exception applies.

K M Z

Consent vs. Authorization

- Consent must be obtained by providers for the access, use or disclosure of protected health information for the purposes of treatment, payment and health care operations.
 - This requirement does not apply to health plans or their business associates.
- Authorization must be obtained for the access, use or disclosure of protected health information for any other purpose.
- Authorizations must be for a specific purpose and limited duration.
- Even with appropriate consent or authorization, a "minimum necessary use" rule applies.

K M Z

The Business Associate Rule

- A covered entity may disclose protected health information to a business associate and may allow a business associate to create or receive protected health information on its behalf, if the covered entity obtains "satisfactory assurance" that the business associate will safeguard the information

EXCEPTION:

- The business associate rule does not apply when a covered entity needs to disclose protected health information to a provider for treatment purposes.

K M Z

Business Associate Contracts

- The privacy rules require Covered Entities to enter into special contracts with Business Associates.
 - The "Plan Sponsor" exception allows an employer to instead amend Plan documents.
- Business Associate contracts must contain specific provisions to protect the confidentiality and privacy of health information.
 - Mandated provisions include prohibition of non-compliant disclosures, privacy safeguards, reporting requirements and access requirements.

K M Z

Business Associate Contracts (continued)

- Covered entities must terminate the contract or report to HHS in the event of a business associate breach.
- Covered Entities can be held vicariously liable for their Business Associate's privacy breach if:
 - 1. The entity fails to impose mandatory contract provisions; or
 - 2. The entity knew of a material breach and does not take reasonable steps to cure the breach or terminate the contract.

K M Z

Employers & HIPAA

- To the extent employers interact with PHI from their plans, the interaction must be HIPAA compliant.
- Employers can elect to perform functions on behalf of plans as Business Associates OR elect a "certification" process under the "Plan Sponsor" exception.
- If an employer elects certification, then group health plan documents must be modified to contain the same restrictions and conditions as a Business Associate contract and a "certification" must be delivered to the plan.

K M Z

Plan Sponsor/Group Health Plan Obligations

- Privacy obligations include policies and procedures for:
 - minimum necessary use
 - consent and authorization
 - privacy notices to covered individuals
 - patient right to inspect, copy and amend records
 - right of accounting
 - privacy officer
 - documentation of actions

K M Z

Plan Sponsor/Group Health Plan Obligations (continued)

- A group health plan may disclose PHI to the participant or for payment or health care operations
- Other purposes require authorization
- All business associates to the group health plan must have a contract limiting their use and disclosure of PHI and requiring compliance with the plan's HIPAA obligations
- ERISA does not preempt HIPAA/state laws may be preempted

K M Z

HIPAA and Employers

- Examples of activities that could place protected health information in an employer's possession:
 - claims submission
 - review of denied claims
 - questions from TPAs regarding plan interpretation
 - advocating a claim for an employee
 - use of medical data for other welfare plans
 - audit reports and data analysis
 - wellness program
 - disease management program
 - workers' compensation
 - on-site clinic

K M Z

Penalties

- Civil fines: not more than \$100 for each violation, up to a total per calendar year for all violations of an identical requirement or prohibition of \$25,000.
- Criminal penalties:
 - 1. Up to \$50,000 and/or imprisonment for up to one year for knowingly using PHI inappropriately;
 - 2. Up to \$100,000 and/or imprisonment for up to five years for inappropriately accessing PHI under "false pretenses;" and
 - 3. Up to \$250,000 and/or up to ten years imprisonment for inappropriately accessing PHI for "commercial advantage" or to do malicious harm.

K M Z

Penalties: Private Litigation

- Private privacy litigation theories:
 - 1. Patients as third-party beneficiaries to business associate contracts (including contracts between employers and their health plans).
 - 2. State invasion of privacy tort.
 - 3. Federal ERISA claims based on breach of fiduciary duty.

K M Z


The Basic Elements of a "HIPAA Compliance Program" under the final rules are:


- Appointment of a privacy officer and security officer
- Implementation and maintenance of appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information
- Development of detailed privacy and security policies and procedures
- Training of all workforce members on privacy and security policies and procedures

K M Z

HIPAA Compliance Programs (continued)

- Establish a system to report privacy and security complaints
- Quick response to investigate potential privacy and security breaches
- Discipline for individuals and Business Associates who are found to have breached the privacy policies
- On-going auditing and monitoring of the organization's privacy and security initiative and auditing of use of code sets

	<table border="1"><tr><td data-bbox="998 289 1084 321">K</td><td data-bbox="1084 289 1170 321">M</td><td data-bbox="1170 289 1276 321">Z</td></tr></table> <h3 data-bbox="553 373 1149 415"><i>HIPAA Imperatives for Employers</i></h3> <ul data-bbox="553 464 1242 779" style="list-style-type: none">• Determine if "covered entity"/perform risk assessment• Amend sponsored health plan documents• Develop authorizations for any contemplated use outside of payment or healthcare operations• Determine need for compliance plan, policies and procedures• Develop business associate contracts for vendors and other business partners who will have access to PHI	K	M	Z
K	M	Z		

	<table border="1"><tr><td data-bbox="998 1123 1084 1155">K</td><td data-bbox="1084 1123 1170 1155">M</td><td data-bbox="1170 1123 1276 1155">Z</td></tr></table> <h3 data-bbox="553 1455 1032 1507">Appendix/Definitions</h3>	K	M	Z
K	M	Z		

K M Z

Health Care Provider

- Health care provider is a provider of medical or health services and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

K M Z

Health Care Provider: What is health care?

- The privacy regulations further define HEALTH CARE to mean care, services or supplies related to the health of an individual, including, but not limited to the following:
 - any preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual or that affects the structure or function of the body; and
 - the sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

K M Z

When a Health Care Provider is a Covered Entity

- All health care providers are not covered entities.
- A health care provider is not a covered entity unless it transmits health information in an electronic format in any of the following triggering transactions:
 - health care claims or equivalent encounter information
 - health care payment and remittance advice
 - coordination of benefits
 - health care claim status

K M Z

Health Care Provider as Covered Entity

- Triggering Transactions (cont'd)
 - enrollment and disenrollment in a health plan;
 - eligibility for a health plan;
 - health plan premium payments;
 - referral certification and authorization;
 - first report of injury;
 - health claims attachments; and
 - other transactions that the Secretary may further prescribe by regulation.

K M Z

Health Plan

- A health plan is an individual plan or group health plan that provides for, or pays the cost of, medical care. The following types of health plans are specifically included in the definition:
 1. a group health plan
 2. a health insurance issuer
 3. an HMO
 4. the Medicare Program
 5. the Medicaid Program
 6. a Medicare supplemental policy issuer
 7. a long-term care policy issuer (excluding nursing home fixed-indemnity policy issuers)
 8. an employee welfare benefit plan or any other arrangement that offers health benefits to employees of two or more employers
 9. the veterans health program
 10. the CHAMPUS Program
 11. the Indian Health Service Program, etc.

K M Z

Health Care Clearinghouse

- A health care clearinghouse is an entity that performs either of the following two functions:
 - 1. Processes or facilitates the processing of health information received from one entity in a nonstandard format into a standard format; or
 - 2. Receives information in a standard format from one entity and processes the information into a nonstandard format.

K M Z

Health Care Clearinghouse

- Examples of a health care clearinghouse:
 - Billing companies
 - Coding services
 - Third-party administrators
 - Any service that translates non-standard data into standardized data

K M Z

Business Associates

- Business Associates are entities that perform functions on behalf of a covered entity AND create, receive or have access to individually identifiable health information maintained by the covered entity.
- The Business Associate rule also includes vendors to covered entities who provide certain defined services (e.g., accounting, legal, consulting) AND who have access to individually identifiable health information.

K M Z

Who is a Business Associate?

- Examples of Business Associates:
 - Management companies
 - Claims processing services
 - Referral services
 - Software vendors that provide maintenance
 - DME vendors that interact with health information on an on-going basis
 - Any consultant who interacts with health information
 - Temp agencies
 - Storage facilities

K M Z

Protected Health Information

- The Privacy Rules define individually identifiable health information as any "health information" which:
 - (a) is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
 - (b) relates to the past, present, or future physical or mental health or condition; the provision of health care; or the past, present, or future payment for the provision of health care; and that:
 - i) identifies the individual; or
 - ii) in which there is a reasonable basis to believe that the information can be used to identify the individual

K M Z

Differences Between Consent and Authorization

- Consents can be obtained at the time care is provided and have no expiration date.
- Consents provide broad authority to the Covered Entity (and its Business Associates) to access, use or disclose PHI for treatment, payment or health care operations (as these activities may be defined in the Covered Entity's "privacy notice).
- Authorizations must be obtained for any access to PHI which is not for the purposes of treatment, payment or health care operations and must identify to whom the PHI will be disclosed AND must delineate the PHI in a "specific and meaningful fashion."
- Individuals may revoke authorizations at any time.
- The definitions of treatment, payment and health care operations are critical for understanding when an organization has authority to access PHI.

K M Z

The Minimum Necessary Use Rule

- Even if a Covered Entity has obtained the necessary consent and authorization forms, the "minimum necessary use" rule must be followed:
 - A Covered Entity must make reasonable efforts to limit use or disclosure of protected health information to the minimum necessary amount to accomplish the intended purpose of the use of the information.
 - Accessing, using or disclosing protected health information beyond the minimum necessary use is a violation of the privacy rules.

K M Z

"Satisfactory Assurance" & Business Associate Contracts

- Business associate contracts must contain the following provisions:
 - 1. The business associate must not further use or disclose the protected health information they maintain in their relationship with the covered entity in any fashion that would violate the privacy regulations if the use or disclosure were to have been undertaken by the covered entity directly.
 - 2. The business associate must not use or disclose the protected health information in any manner inconsistent with the contract, even if the contract sets out rules which are more restrictive than the requirements of the privacy regulations.

K M Z

"Satisfactory Assurance" & Business Associate Contracts *(continued)*

- 3. The business associate must use appropriate safeguards to protect the information, even if in order to protect the information the business associate must adopt physical and technology safeguards not explicitly cited in the contract.
- 4. The business associate must report to the covered entity any use or disclosure of the protected health information that is inconsistent with the contract.
- 5. The business associate must assure that it will obtain the same satisfactory assurances from subcontractors as the business associate is giving to the covered entity.

K M Z

"Satisfactory Assurance" & Business Associate Contracts *(continued)*

- 6. The business associate must agree generally to provide the individual subjects of protected health information a right of access to inspect and obtain a copy of their health information.
- 7. The business associate must amend an individual's protected health information as that individual may request amendment and such amendment may be appropriate.
- 8. The business associate must make available to the individual a log of disclosures of protected health information.

K M Z

"Satisfactory Assurance" & Business Associate Contracts *(continued)*

- 9. The business associate must agree to allow HHS to have access to its books, practices and records related to the handling of protected health information.
- 10. At termination of the contract, the business associate must return to the covered entity or destroy any protected health information, if feasible.
- 11. The contract must authorize the covered entity to terminate the contract if the covered entity determines that the business associate has materially breached the terms of the contract.

Why is the European Union Privacy Directive and resulting member country privacy laws such as the UK Data Protection Act, as well as the EU/U.S. Safe Harbor important to you?

- Their provisions apply to EU individual's data transferred to or processed within the U.S.
- Their provisions are significantly different than the U.S. privacy laws you are used to dealing with

The Directive, The Laws & The Harbor - How this all came about

- EU Comprehensive Approach – Duty of the State to protect individual's private information
- The EU data privacy directive created
- Resulting EU Member privacy laws incorporating principles of the Directive
- including prohibition from transferring personal data to countries outside of the EU
- which do not maintain "adequate" privacy protections.
- Faced with the flow of EU personal data to the U.S. being cut-off, the EU/U.S. Safe Harbor was negotiated.

The EU's Privacy Directive – "Directive 95/46/EC"

- The Directive broadly controls the manner in which personal data is collected, maintained and used.
- Applies to personal data of EU citizens and member countries required to enact legislation incorporating its principles.

The EU's Privacy Directive – "Directive 95/46/EC"

- Principles:
 - Processed fairly and lawfully
 - Collected only for "specified, explicit and legitimate" purposes
 - Not processed in a way incompatible with those purposes.
 - Kept accurate and where necessary up to date.
 - Kept in a form which permits identification of the person
 - Only kept for so long as necessary in light of the reason it was collected.
- Exceptions

The EU's Privacy Directive – "Directive 95/46/EC"

- Sensitive Information
- Importance of Data Controllers
- Transborder Data Flows
- Rights of Individuals With Regard to Their Information

UK DATA PROTECTION ACT

- Same principles as the Directive
- Key Definitions
 - Data Controller
 - Data Subject
 - Personal Data
 - Processing
- Individual's Rights

UK DATA PROTECTION ACT

- The Eighth Principle – Trans-border Data Flows
 - Is it personal data?
 - Is it transferred?
 - Is it to a country with adequate level of protection? – 6 factors
 - Are there any applicable exceptions to the adequacy requirement?
- Alternative way to comply – Model contract

EU/U.S. Safe Harbor

- set of privacy principles along with 15 frequently asked questions that give added context to the principles
 - Principles:
 - Notice
 - Choice
 - Transfers of Information to Third Parties
 - Access
 - Security
 - Data Integrity
 - Minimum Enforcement Requirements

EU/U.S. Safe Harbor

- Exceptions
- Procedure for Compliance with Safe Harbor
 - Self-Certification
 - Alternative: Model Contract

EU/U.S. Safe Harbor

- PRACTICAL ISSUES – To Sign Up or Not to Sign Up
 - Risks
 - Benefits
- Reasons For Caution
 - Not Many Sign Up Yet (Competitive Disadvantage?)
 - Too Early – More Changes to Come?
 - Bad Precedent
 - Cost
- Some Alternative Practices To Think About
- Want more detail – Take a look at the "HELPFUL RESOURCES" in the materials

TEN THINGS YOU SHOULD TAKE AWAY FROM THIS PRESENTATION

- The EU Privacy Directive is a comprehensive approach to privacy protection based upon the Government's duty to protect privacy whereas the U.S. employs a sectoral approach where privacy is a right of the individual. The EU has determined that the U.S. has inadequate personal data privacy protections.
- The Directive is the basis for EU member country laws and all EU countries are required to pass privacy legislation containing its principles, including a prohibition against transfer of personal information to countries outside of the EU with inadequate privacy laws.
- The UK Data Protection Act 1998 was implemented based upon the EU Privacy Directive and includes the prohibition against transfer of personal information to third countries with inadequate privacy laws, the so-called "Eighth Principle."

TEN THINGS YOU SHOULD TAKE AWAY FROM THIS PRESENTATION (Continued)

- Like most statutes, to really understand the impact of the Act it is important to know the definitions to its key terms (Data Controller, Data Subject, Personal Data and Processing), and always look for one of the exceptions to the Eighth Principle so that you can transfer the data regardless if it is to a country with inadequate privacy protection.
- The Safe Harbor is an agreement between the U.S. and the EU wherein if a company certifies (and maintains compliance) with a series of privacy principles including notice, choice, transfers to third parties, access, security, data integrity and enforcement, then it will not be prevented from receiving personal data from the EU just because the U.S. has inadequate data privacy protection.
- Two ways to comply: self-certification by signing up at the Department of Commerce website, and using Model Contracts.

**TEN THINGS YOU SHOULD TAKE AWAY FROM THIS
PRESENTATION (Continued)**

- Companies must carefully weigh the costs and benefits before entering the Safe Harbor in light of the extent of personal data they are gathering and the extent of their dealings in Europe.
- The main benefit of the Safe Harbor is certainty that data flows will continue uninterrupted.
- The downsides to agreeing to the Safe Harbor are that not many have signed up and due to the major disagreements about the Safe Harbor there may be changes to come. There is also significant cost to complying with the Safe Harbor and once you enter the Safe Harbor then you are bound by its principles for the information you gathered while you were in the Safe Harbor.
- For more guidance see the FAQs attached to the Safe Harbor, and the resources listed in Section VII of this paper or in the endnotes.

I. INTRODUCTION¹

Privacy law, like many areas of international law, is dependant upon the particular country at issue. Recently there has been an explosion of new national privacy laws which has created "a maze of often conflicting provisions and a potential compliance nightmare for not just for e-commerce, but for any company doing business across borders with individual consumers."²

However, the European Union ("EU") has made a bold stride which attempts to gain substantial uniformity of privacy laws directly within the EU and indirectly outside of the EU. The extraterritorial reach of the European Union's privacy directive, i.e. Directive 95/46/EC (the "Directive"), has caused both praise and consternation in the business community and with consumer groups. In any event it has forced corporate counsel to understand and deal with it.

Even if your company does not operate overseas, you will undoubtedly be impacted by the provisions of these recent privacy enactments since they differ substantially from United States ("U.S.") law and control significant amounts of personal data which is processed for and distributed to the U.S.³ It is important to grasp the fundamentals and monitor developments with regard to privacy law so that you are able to spot the issues and advise your client or bring in needed resources.

II. THE DIRECTIVE, THE LAWS & THE HARBOR—HOW THIS ALL CAME ABOUT

While the U.S. employs targeted privacy protections for sensitive areas, such as those involving financial services and medical records, the EU uses a comprehensive approach to protecting personal information of individuals.⁴ There has been much discussion as to why the Europeans favor this broader approach. Some have testified that still existing sensitivity to the vast data collection practices employed in Nazi Germany has driven the EU to consider data protection as a fundamental human right.⁵ Others have speculated that it is the technology age which is driving the EU to protect individual's information and its collection and processing.⁶

Regardless of what the specific or combination of drivers are, the EU issued the Directive, that required EU member nations to enact privacy laws (or amend existing laws) to comply with the provisions of the Directive.⁷ The Directive put restrictions on personal data transferred within the EU but also on transfers of personal data outside of the EU, so called "trans-border data flows."⁸ EU member countries were prohibited from the transfer of personal data to nations outside of the EU who do not have, according to the EU, "adequate" privacy protection laws.⁹ Each EU member country was required to enact implementing legislation by October 1998.¹⁰ So far most EU nations have complied with the Directive, such as the UK with its Data Protection Act of 1998.¹¹

The U.S. saw a potential disaster with this Directive and the resulting EU member country laws restricting data flow outside of the EU. Thus, "[t]he U.S. strongly lobbied the EU and member countries to find the U.S. system adequate."¹² The U.S. argued that it incorporates a sectoral approach to privacy protection, which tailors the privacy burden to the type of information being protected, e.g. higher privacy for medical data.¹³ However, the EU Commission in charge of the EU privacy effort was not convinced due, in part, to the fact that the U.S. has "no independent privacy oversight agency,"¹⁴ and "no comprehensive privacy protection law for the private sector."¹⁵ The EU concluded that privacy law in the U.S. is a patchwork of federal laws

covering some specific categories of information"¹⁶ Therefore, the EU determined that the U.S. has inadequate personal data privacy protection as compared to their universal data protection laws.¹⁷

Because many U.S. companies raised difficulties and doubts about complying with the EU adequacy standard,¹⁸ and faced with the fact that the \$350 billion U.S.-EU trade flow could be threatened by the cut-off of personal data from and to the EU, the U.S. pursued the solution of a Safe Harbor.¹⁹ It was hoped that a Safe Harbor would end uncertainty and "provide a more predictable framework for such data transfers."²⁰ In other words, in order to enable U.S. companies to comply with the Directive and not suffer adverse consequences under EU countries data protection laws (e.g. UK Data Protection Act), the U.S. entered into the Safe Harbor agreement with the EU.²¹

Basically, for those companies who enter the Safe Harbor, they may receive personal data from EU member countries without undue fear of the transmitter of the information violating that particular country's data protection legislation by transferring personal data to a country with inadequate privacy protection.²² Entering the Safe Harbor is completely voluntary through a process of self-certification by the company to adhere to a set of privacy principles outlined in the Safe Harbor.²³ Specifically, the companies in the Safe Harbor would then have a presumption of adequate privacy protection and they could continue to receive personal data from the European Union."²⁴ In other words, if you comply with the Safe Harbor then you will be presumed to comply with the Directive (and resulting EU country's data protection laws) concerning the adequacy of your company's privacy protection. It would then be the burden of the particular EU country to overcome any presumption that the company did not comply with the principals certified by the company in committing to the Safe Harbor and thus prove that the transborder personal data flow should be cut off due to inadequate privacy protection.²⁵

Those companies that choose not to enter the Safe Harbor run the risk of having data flows from EU member nations summarily restricted or cut-off.²⁶ The challenge for corporate counsel appears to be assisting their clients in carefully weighing the costs and benefits of the Safe Harbor versus the risks and associated costs of loss of data for noncompliance.

III. THE EUROPEAN UNION'S PRIVACY DIRECTIVE

A. Overview

The EU's comprehensive privacy legislation, Directive 95/46/EC ("Directive"), went into effect on October 25, 1998.²⁷ The Directive aims at ensuring the unimpeded movement of personal data while at the same time guaranteeing the protection of the interests of individuals."²⁸ To prevent abuses of personal data and ensure that individuals are informed when their information is being collected and used, the Directive governs those who collect, hold or transmit personal data as part of their business or activities. In particular, the Directive states that the data may be collected only for specified, explicit and legitimate purposes, and may only be kept if it is relevant, accurate and up-to-date.²⁹

The Directive's most important impact on the U.S. is that it requires that EU countries may only allow personal data to be transferred only to countries which have adequate privacy protection laws.³⁰

B. The Directive

1. The Basics

The Directive broadly controls the manner in which personal data is collected, maintained and used. The Directive applies to all individuals,³¹ but there are exceptions for data processed just for personal reasons, household activities, national defenses or law enforcement.³² Personal data must be processed fairly and lawfully and collected for "specified, explicit and legitimate" purposes and not further processed in a way incompatible with those purposes.³³ The data must be accurate and where necessary kept up to date.³⁴ The personal information must be kept in a form which permits identification of the person whose data it is and for only so long as necessary in light of the reason it was collected.³⁵

The appropriate purposes for collecting an individual's personal information are for reasons to which the person clearly consents, or for the performance of a contract to which the person is a party, or compliance with a legal obligation, or to protect the vital interests of the person (e.g. life and health), or which is in the public interest, or for the "legitimate interest" of the intended recipient of the personal information.³⁶ However, this "legitimate interest of the recipient" cannot override the interests or fundamental rights of the data subject ... This provision establishes the need to strike a reasonable balance... between the business interest of the data controllers and the privacy of the data subjects."³⁷

The Directive also establishes the concept of fairness through the principle of full disclosure.³⁸ Individuals must have the right to choose as to whether they will give personal information.³⁹ Also, individuals have a right to know who is collecting the information and for what reason it is being collected.⁴⁰

2. Sensitive Information

In the case of sensitive data, such as an individual's ethnic or racial origin, political or religious beliefs, trade union membership or data concerning health or sex life, the Directive establishes that it can only be processed with the explicit consent of the individual, where it is mandated by employment law, or if needed and the person cannot consent (such as to identify a dead person), or in specific cases such as where there is an announced important public or governmental interest (e.g. for medical or scientific research), where alternative safeguards have been established.⁴¹

3. Importance of Data Controllers

"Data Controller" is a term of art in EU privacy law which means the person or entity which collects or processes an individual's personal information or who determine the reasons the information is gathered.⁴² The data controller has certain obligations put on it as a result of its

role in processing the personal data. First, the data controller must comply with the specific laws of the EU country it is established in or where its information processing equipment is, even if the processing starts somewhere else.⁴³

Specifically, data controllers must: 1) process the individual's data fairly and lawfully, 2) collect and use data only for explicit, clear and legitimate purposes, 3) collect only data that is relevant to the lawful purpose for which it is collected, 4) keep the data accurate (and if important to the reason for which it is collected, then also keep the data up to date), 5) enable individuals whose data is collected to have the ability and means to correct or delete incorrect information about themselves, and 6) only keep the information as long as it is necessary to complete the purpose for which it is collected.⁴⁴ Finally, data controllers must have reasonable procedures in place for disaster recovery and to prevent unauthorized access to or processing of the data.⁴⁵

4. Transborder Data Flows

As stated above, the Directive enables EU countries to pass their own legislation which allows them to cut off the transfer of personal information to a third country that does not offer an adequate level of privacy protection for personal data.⁴⁶ The EU may make determinations of which countries have "adequate" privacy protection but the ultimate burden of this decision is on the data controller, which must do its own assessment. However, the data controller does not have to determine the adequacy of the country's (outside of the EU) privacy protection when the person has given clear consent to the transfer, or if the transfer is necessary for performing a contract to which the person is a party, or if the transfer is legally required or in the public interest or if the transfer is needed to protect the vital interests of the person whose information is given, or the transfer is intended to provide lawful public information.⁴⁷

5. Rights of Individuals With Regard to Their Information

Under the Directive, individuals have the right to see the data being stored about them and to know where that information was obtained and may also have information about them corrected or not used if incorrect.⁴⁸ A precursor to this right is that persons are entitled to know the identity of the data controller, and why the data is being used.⁴⁹ Finally, they also have the right to know who will receive the data and "the logic involved in any automatic processing."⁵⁰

6. Impact

The EU has proudly stated that the Directive will establish a clear and stable regulatory framework necessary to guarantee free movement of personal data, while leaving individual EU countries room for maneuver in the way the Directive is implemented.⁵¹ Sentiment in the U.S. is somewhat less enthusiastic.

"While its goals may be laudable, there are a number of fundamental problems with the European Directive. First, it was conceived over a dozen years ago when there was no World Wide Web and information technology was dominated by mainframe computers not distributed information networks, laptops, and digital assistants. As a result, the Directive is often rigid or silent in dealing with privacy issues growing out of new

technology and business models. Many European States have had great difficulty translating it into domestic law. Second, one can read the European Personal Data Protection Directive from end to end and not find the word "privacy". Personal data protection is an obligation of the State toward its citizens. In America we believe that privacy is a right that inheres in the individual. We can trade our private information for some benefit. In many instances Europeans cannot. This can have important implications when it comes to e-commerce. But the most troubling aspect of the Directive for the United States is the requirement that personal data only be transmitted from Europe to countries that have "adequate" privacy regimes. In effect, the Directive would embargo European personal data to any country whose privacy policies the EU had not approved. Imagine. No transatlantic bank transactions, credit card purchases, airline and hotel reservations, no internet or catalogue sales, no ability of U.S. firms to manage personnel in their European operations, and visa versa. Fortunately, the European Commission recognized that this could hurt Europe as much as the United States. This was the background for the Safe Harbor negotiations that lasted more than two years."⁵²

IV. UK DATA PROTECTION ACT

A. Overview

Due to the strong relationship between business in the UK and the U.S., it is appropriate to take a look at privacy legislation in the UK enacted as a result of the EU Privacy Directive. The Data Protection Act 1998 repeals the 1984 Data Protection Act and makes the UK's privacy laws comply with the requirements of the Directive.⁵³ In addition to the requirements of the Directive as stated above, it is important to note that the UK Act applies to private as well as governmental data controllers. Also, it requires that data controllers register with a special agency created to oversee privacy enforcement in the UK, i.e. the Office of the Information Commissioner.⁵⁴ As with the Directive, the most important aspect of the UK Act is that the UK prohibits the transfer of personal data to a country outside of the EU with inadequate privacy laws.⁵⁵

B. The Act

i. Eight Principles

The Data protection Act contains eight basic principles which apply to anyone processing personal data of individuals within the UK: 1) only fairly and lawfully process the personal information; 2) process the information only for the lawful purpose for which it is collected; 3) make sure that the personal information is relevant to the purpose for which it is collected and does not contain any more information than is needed to complete the process for which it is collected; 4) make sure that the personal information is accurate; 5) do not keep the personal information longer than necessary to do the processing; 6) only process personal information in accordance with the individual's rights as outlined in the Act; 7) maintain reasonable security measures designed to keep the information protected from unauthorized use; and 8) do not transfer personal information to countries without adequate privacy protection.⁵⁶

ii. Key Definitions

a. Data Controller

Data Controller is the person who processes the information and/or determines for what reason the information is being collected and/or processed.⁵⁷ It is important to establish whether or not someone is a data controller because it is data controllers who are required to comply with the data protection principles.⁵⁸

b. Data Subject

The Data Subject is the person whose personal information is being processed. The rights under the Data Protection Act flow to the Data Subject.⁵⁹

c. Personal Data

Personal Data is broadly defined as data that is identifiable to an individual.⁶⁰ In other words, the Act covers information that is structured either to a particular person (e.g. by name) or information that makes a specific person easily identifiable (e.g. some process which can link the information to the name).⁶¹ Personal data can be anonymized so it is no longer Personal Data but this is difficult to achieve because the data controller can't retain any method to link the person's information to the particular person.⁶² Interestingly, Personal data covers both facts and opinions about the individual and also includes information regarding the intentions of the data controller towards the individual.⁶³

d. Processing

Process is broadly defined and takes place when any operation or set of operations is carried out on personal data.⁶⁴ Specifically, processing means obtaining, recording or holding the personal information or carrying out any operation on the personal information.⁶⁵

Processing of a Data Subject's Personal Information by a Data Controller is only permitted when: 1) the individual consents to the processing, 2) the processing is necessary for the performance of a contract with the individual, 3) the processing is required under a legal obligation, 4) the processing is necessary to protect the vital interests of the individual, 5) the processing is necessary to carry out public functions, or 6) the processing is necessary in order to pursue the legitimate interests of the data controller or third parties, unless it could prejudice the interest of the individual.⁶⁶ When processing sensitive personal information, e.g. race, ethnicity, political opinions, religion, union status, health, sex life or criminal background, it must be only done when the data controller has the explicit consent of the individual, is required by law to process the data for employment reasons or when the information is needed to protect the vital interests of the data subject or another, or is necessary for administration of justice or legal action.⁶⁷

iii. Individual's Rights

Individuals have the right to know the information that is gathered and maintained about them.⁶⁸ They also have the right to have inaccurate information (and the opinions/decisions based thereon) corrected and if not corrected, to have the inaccurate information destroyed.⁶⁹ Also there is the right to stop processing where it is causing or will likely cause substantial damage or distress to anyone, or to stop (i.e. opt-in) direct marketing.⁷⁰ Also there is a right to compensation for damage.⁷¹ Finally, except for certain exempt decisions, a Data Subject can stop automated decision making based upon his or her personal information where such decision "significantly affects the individual."⁷² The process for this is for the Data Subject to make an application to a court of competent jurisdiction with damages available for violation by the Data Controller of the Act.⁷³

iv. The Eighth Principle – Trans-border Data Flows

The eighth principle of the Act states: "Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data."⁷⁴ The key questions are: 1) "is it personal data", 2) is it "transferred", 3) is it to a country with "adequate level of protection," and lastly 4) are there any applicable exceptions to the adequacy requirement?⁷⁵

1. Is it Personal Data?

See discussion above.

2. Is it being Transferred?

The Act does not define "transfer" but the meaning of the word as determined by the UK Data Commissioner is that it means transmission from one place or person to another place or person.⁷⁶ Importantly, transfer is not equivalent to transit. In other words, personal information which is transmitted through a non-EU country is not transferred to the non-EU country unless there has been a "substantive processing operation" conducted on the personal information in that non-EU country.⁷⁷

3. Is there an Adequate Level of Protection?

The decision process for determining whether a country has adequate personal information privacy protection is basic risk analysis. As the risk of personal information not being protected increases, then a finding of inadequacy is more likely.⁷⁸ The factors that go into assessing whether a county's laws will sufficiently protect the personal information being transferred to the country are: 1) The nature of the personal data, i.e. the more sensitive the data the higher level of protection needed, 2) The origin of the data, e.g. if the information is just processed in one country but then sent back to country of origin then less protection is needed, 3) The final destination of the data, e.g. is the information ultimately going to reside in a country with lax protection, 4) the purposes and the period of processing, i.e. the more sensitive the purpose and

the longer the information will be processed, the more safeguards need to be in place in the country to which the information is being transferred, 5) the extent and nature of the legal protections in the country, and 6) what security procedures the Data Controller has in place for the data in that country.⁷⁹

As stated previously, the Data Controller is required to determine whether the country to which the personal information is being transferred has adequate privacy laws unless the EU has already determined the issue in which case the Data Controller can rely on the EU's determination.⁸⁰ The Data Commissioner has stated that "the data controller is required to make a judgment as to whether the level of protection afforded by all the circumstances of the case is commensurate with the potential risks to the rights and freedoms of data subjects in relation to the processing of personal data."⁸¹ Furthermore, the Data Commission outlined as a good practice approach that "data controllers are not expected to do exhaustive legal research but should focus on countries which show a real and obvious danger to the rights and freedoms of individuals in relation through the processing of personal data."⁸² Also, it is worth remembering that the country in question needs only "adequate" privacy protection not necessarily "equivalent" to the Data Controller's country's privacy protection regime.⁸³

4. Are there any Exceptions?

The eighth principle does not apply (i.e. one can transfer to a country with inadequate protection) when: 1) The person consents to the transfer,⁸⁴ or 2) The transfer is necessary for performing a contract with the person or to enter into a contract between the person and the data controller,⁸⁵ or 3) The transfer is necessary for performing a contract between the controller and a third party which was entered into because of the person (i.e. at the person's request or the contract is in the person's interests), or 4) The transfer is necessary for reasons of substantial public interest,⁸⁶ or 5) The transfer is necessary in connection with legal proceedings or obtaining legal advice,⁸⁷ or 6) The transfer is necessary in order to protect the vital interests of the person,⁸⁸ or 7) The transfer is part of public database, or 8) The transfer is approved by Office of the Information Commissioner.⁸⁹

A Data Controller should look first to making a determination as to the adequacy of the country's privacy protections instead of just immediately relying on an exception.⁹⁰ Also corporate counsel should note that there is no exception for transferring data in response to "legal compulsion", e.g. subpoena, etc. "It might of course be that the transfer is necessary for reasons of substantial public interest or is necessary in connection with legal proceedings but this will not necessarily be so...A judgment will have to be made based on the circumstances of the particular case and nature of the legal requirement."⁹¹

5. Is there an alternative basis for the transfer, i.e. Model Contracts?

Data Controllers can fulfill the adequacy need for transfers of personal information to countries that don't have adequate privacy protections by entering into a contract with the recipient which contains approved model contract language that is designed to provide adequate protection.⁹²

The model contracts contain language which meets the Data Protection Act principles as to the right to notice, consent, access and legal remedies.⁹³

"There are several different types of contract between a data controller in the UK and a recipient of personal data in another country which can be used to facilitate a transfer. In some cases the contract is comprehensive and avoids the need for the data controller to make its own assessment as to whether the circumstances of a particular transfer or set of transfers ensure adequate protection. In other cases the contract might be less comprehensive and is used to bring what the data controller has assessed to be a not wholly adequate level of protection provided by the circumstances of a transfer up to an adequate level. The main types of contracts are: 1) contracts based on standard terms approved by the European Commission (EC standard contracts), 2) contracts based on standard terms approved by the UK Data Protection Commissioner (UK standard contracts), 3) contracts drawn up by the data controller to bring protection up to an adequate level (non-standard contracts), and 4) one-off arrangements authorized by the UK Data Protection Commissioner as ensuring adequate safeguards⁹⁴ (authorized arrangements)."⁹⁵

Use of the contracts protect the Data Controller and recipient for the purposes of meeting the adequate protection requirement and EU countries are bound to recognize their effect.⁹⁶ Whether to use the contract to meet the eighth principle is completely voluntary but the contract must contain clauses sufficient to meet the Directive and the EU member country's privacy act.⁹⁷ In addition to the model contracts, EU countries data protection authorities may authorize transfers on a case by case basis when they are satisfied the data enjoys "adequate protection".⁹⁸

C. Enforcement

The Office of the Information Commissioner in the UK enforces the Data Protection Act of 1998.⁹⁹ To understand the Commissioner's enforcement approach it is helpful to know the context surrounding the Commissioner's views of the Data Protection Act. The Commissioner has stated:

"The Directive from which the 1998 Act is derived requires member states to protect the fundamental rights and freedoms of natural persons, in particular, their right to privacy with respect to the processing of personal data. It is my view that where businesses and organizations build in compliance with the rules designed to ensure respect for the privacy of their customers, clients and employees into their business practices this does not impose an unnecessary burden. Indeed, I am pleased that organizations increasingly see the need to follow proper information handling procedures as a key requirement of their business activity. I am therefore optimistic that data controllers will find the requirements of the 1998 Act fit with other requirements and that they will recognize the benefits as well as the importance of taking seriously the need to respect the privacy of personal information"¹⁰⁰

"Those countries that refuse to adopt meaningful privacy laws may find themselves unable to conduct certain types of information flows with Europe [because they are outlawed by the particular country's data protection act] particularly if they involve sensitive data."¹⁰¹ The Office of the Information Commissioner has substantial power to enforce the Data Protection

Act in that it may conduct investigations and gather relevant information, impose remedies "such as ordering the destruction of information or ban its processing," and pursue litigation.¹⁰² The Information Commissioner also keeps the register of data controllers and databases.¹⁰³

V. EU/U.S. SAFE HARBOR

A. Overview

The different approaches to privacy protection of the EU and U.S. ultimately led the EU to determine that U.S. privacy law was inadequate. In order to avoid the significant economic impact of having data flow restricted or cut-off,¹⁰⁴ the EU and U.S. negotiated a Safe Harbor from the EU Privacy Directive and corresponding EU nation privacy laws.¹⁰⁵ The Safe Harbor agreement went into effect in July of last year. The Safe Harbor comprises a set of privacy principles relating to notice, choice, transfers to third parties, access, security, data integrity and enforcement along with 15 frequently asked questions that give added context to the principles.¹⁰⁶ The Safe Harbor provisions are only for use by U.S. companies who receive personal information from the EU, in order to enable them to comply with the "adequacy" requirement of the Directive.¹⁰⁷ Companies that certify their compliance with the Safe Harbor principles would be presumed to be in compliance with EU data privacy requirements and therefore would not suffer adverse consequences for being located in the U.S., a country which has been determined by the EU as having inadequate privacy laws.¹⁰⁸ The Safe Harbor took over two years to negotiate and was entered into as a "authorized arrangement" allowed by the "model contracts" alternative to the Directive and resulting EU member nation laws (see section **IV.B.iv.5. supra**).¹⁰⁹

Ambassador David L. Aaron summarizes the positions of the EU and U.S. in developing the Safe Harbor in the following quote:

"Let me briefly describe how the Safe Harbor accord emerged and what it is and is not. The first thing we established was that the United States was not going to negotiate a Treaty or an Executive Agreement that would apply the EU Directive in the U.S. What we were prepared to do was issue guidance to the American business community on how to conduct commercial relations with other countries. This comes under the existing authority of the Department of Commerce. In the past we have provided such guidance to help protect U.S. firms doing business in places like the Soviet Union, China and elsewhere. The second thing we made clear is that we were not going to accept the jurisdiction of European law in the United States. Indeed we agreed that the Safe Harbor would be silent on jurisdiction. We were prepared to have voluntary, self regulation within the framework of existing U.S. law. We were not going to pass new legislation. Third, the Europeans had to recognize that were trying to adopt the Directive to the most advanced information economy on earth. Accordingly the actual provisions of the Safe Harbor had to be more flexible and address real world information practices on a reasonable basis. Fortunately, we had the precedent of privacy principles that we and the Europeans had agreed upon in the OECD many years ago. This became a touchstone of the discussions. The European Commission accepted these points but had a bottom line of their own. They insisted on what they considered a high level of privacy protections

for European personal data as provided by their Directive. It was their information and; they had the right to control its dissemination. The result was the Safe Harbor accord of last year."¹¹⁰

The U.S. government supports the Safe Harbor and has stated "[i]t bridges the differences between EU and U.S. approaches to privacy protection and will ensure that data flows between the U.S. and the EU are not interrupted" because "a carefully constructed and well-implemented system of self-regulation...can protect privacy rights."¹¹¹

B. The Key Provisions

There is no mandate that U.S. companies join the Safe Harbor.¹¹² Companies are free not to comply but then risk action by EU countries from which personal information is transferred pursuant to their privacy legislation (e.g. UK Data Protection Act 1998) or the cut-off of personal data flows from information providers located in an EU country. Also important to remember is that the Safe Harbor principles are self-regulating in that they are not U.S. law.¹¹³

i. Principles

Basically, there are seven principles which a company must comply with in order to be within the Safe Harbor.¹¹⁴ The principles are those stated below (as stated in the U.S. Department of Commerce's Safe Harbor website):¹¹⁵

1. Notice: A company has to give persons notice of the purpose they are collecting the information and to what kinds of other organizations it discloses information to. Also the company must have a notice showing how people can contact the company with complaints or questions and how the person can limit or prevent the disclosure of his/her information.¹¹⁶
2. Choice: Persons must have the ability to choose whether they allow a company to disclose their information to a third party. Moreover, persons must have the ability to tell companies that they do not want their information used for a purpose other than the one that the information was collected for. If the information is deemed "sensitive" then the choice must be via a opt-in procedure, i.e. the person must give affirmative consent to it being given to third parties or used for another purpose.¹¹⁷ The choice to opt out of allowing personal info to third parties must be given to persons at any time with reasonable limits which allow the company to comply.¹¹⁸
3. Transfers of Information to Third Parties: Other than as stated in the Notice and Choice requirements above, agents of companies who will be receiving information from a company, may receive that information only if they ascribe to the Safe Harbor principles.¹¹⁹
4. Access: Companies must give people access to their personal information and an ability to correct erroneous information. The exceptions are if the burden of providing such access is greater than the risks associated with the erroneous information or where access to the information would violate another persons rights.¹²⁰ The duty to provide access to a person of the information stored about that person is subject to a reasonableness standard.¹²¹

Much like responding to discovery requests, a company does not need to provide access to its database or put it in another form other than how it is stored, and may charge a non-excessive fee and put reasonable limits on the number of times or frequency access may be requested.¹²²

Factors to consider are the level of detail of the request (i.e. vague or ambiguous), and the expense and burden of the access versus the significance of the information used to make significant decisions about the person.¹²³ Also, there is no need to provide access to publicly available information.¹²⁴ Companies may require sufficient identifying information from the requestor but must not excessively delay providing information to the requestor.¹²⁵ Companies, however, must always make good faith efforts to provide access to the information and redact information when certain information needs to be protected (e.g. confidential commercial information).¹²⁶

5. **Security:** Companies must protect the personal information from tampering, destruction or unauthorized access. The protections, however, don't have to be absolute, but only what is reasonable.¹²⁷

6. **Data Integrity:** Companies must have reasonable procedures designed to keep the information reliable, accurate, complete and current. Also, procedures should be designed to keep only information which is relevant to the purpose for which it is collected.¹²⁸

7. **Minimum Enforcement Requirements:** The Safe Harbor contemplates a combination private sector/government three pronged enforcement mechanism.¹²⁹ First, a "readily available and affordable independent" forum must be available for persons so that their complaints can be investigated and remedied.¹³⁰ Second, there must be a procedure in place so that companies actually adhere to the Safe Harbor principles. Third, there must be sanctions for companies that do not adhere to the principles.¹³¹ To meet the first two enforcement prongs, the Department of Commerce will maintain a list of companies that certify compliance with the Safe Harbor.¹³² This presumption as to compliance with the Safe Harbor is augmented by the Department of Commerce removal of a company that does not comply with the principles, which in turn subjects the company to enforcement actions from the U.S. (i.e. False Statements Act (18 U.S. C. Section 1001)¹³³) and restrictions from the EU.¹³⁴ Companies must also maintain records of their Safe Harbor practices for any regulatory audit and surprisingly there is no time limit on the amount of time that a company must maintain the records of its compliance, even if the company eventually leaves the Safe Harbor.¹³⁵ U.S. law will be the law governing disputes related to the Safe Harbor (unless the company affirmatively consents to be governed by EU or an EU Country's law).¹³⁶

ii. Exceptions

There are several exceptions where a company, even though publicly committing to the Safe Harbor, is not required to follow its provisions. First, strict compliance is not required when it would contradict the interests of national security, public interest or law enforcement requirements.¹³⁷ Also, if statutes or case law create conflicting obligations, then compliance to the Safe Harbor may give way to compliance with the law but only to the extent necessary to comply with the law.¹³⁸ Third, if the Directive or applicable EU country law allows for

exceptions then those exceptions will apply to compliance with the Safe Harbor but only in comparable contexts.¹³⁹ Finally, in order to take advantage of these exceptions, a company must disclose (e.g. in their privacy policy) in which instances these exceptions will regularly arise in gathering user's personal information.¹⁴⁰

C. Procedure for Compliance with Safe Harbor

i. Self-Certification Approach

A company may self-certify that it complies with the Safe Harbor by way of a letter signed by a corporate officer which states that it will adhere to the Safe Harbor principles and has a description of the types of personal information the company maintains and processes. Also, it must issue a privacy policy containing the provisions of the Safe Harbor which policy may either be its own policy or it may join a self-regulatory organization¹⁴¹ wherein its principles comply with the Safe Harbor requirements.¹⁴² The company must do this certification every year.¹⁴³ "The Safe Harbor status is granted to the company at the time it completes the self-certification."¹⁴⁴ U.S. companies may sign up for the Safe Harbor at <http://web.ita.doc.gov/safeharbor/shreg.nsf/safeharbor?openform>. Companies should have information listed at http://www.export.gov/safeharbor/sh_registration.html in order to complete the certification. A company may leave the Safe Harbor at any time, but its provisions apply forever to the personal information processed while the company was in the Safe Harbor.¹⁴⁵

ii. Model Contract Approach

Companies can also use a model contract that contractually obligates the company to the Safe Harbor principles. The contract is intended to be entered into by the data exporter and the data importer and provides that the contract may be enforced by individuals whose personal data is being transferred.¹⁴⁶ The contract binds the data importer and data exporter to comply with obligations of the Safe Harbor.¹⁴⁷ For example, the data importer promises to offer individuals rights of access to and correction of data held and promises that if the transfer involves sensitive data, the individual has been informed that the data is being transferred to a country with inadequate data protection laws.¹⁴⁸ (See discussion B.iv.5. *supra* for further detail).

The model contract approach is not without its downsides. First, it can be an expensive and burdensome way to comply with the Safe Harbor in that a contract would have to be entered into with each data supplier.¹⁴⁹ Also, it is arguable that the compliance standards built into the contracts can be severe.¹⁵⁰ For example, the individuals or data subjects are considered third party beneficiaries to the contracts and are able to assert joint and several liability against either the data supplier or data recipient for "any act incompatible with the obligations contained in the standard contractual clauses" (however, this liability between the parties may be mitigated by an indemnification provision).¹⁵¹ Concomitantly, there may be practical difficulties to the enforcement of a contract with parties located in different countries.¹⁵²

A copy of the draft contract is available at www.europa.eu.int/comm/internal_market/en/media/dataprot/news/annexen.pdf and at http://europa.eu.int/eur-lex/en/dat/2001/l_181/l_18120010704en00190031.pdf

D. Interpretations as stated in FAQs

The Safe Harbor contains additional clarity in the form of Frequently Asked Questions (FAQ). Some noteworthy guidance is stated below:

i. "Sensitive Information."

Companies may process sensitive information without complying with the principles of the Safe Harbor only: 1) if the information is in the vital interests of the person or another person, 2) if the information is necessary to establish legal claims and defenses, 3) if the information is necessary to provide medical care or diagnosis, 4) if the information is collected by a foundation, association or any other non-profit body with a political, philosophical, religious or trade union aim but only if the information relates to the members of the organization (or those who have regular contact with the organization) and only if it's not transferred to a third party without the consent of the person, or 5) If the information is necessary to carry out the company's' duties relating to employment law, 6) if the information is related to data that is made public by the person.¹⁵³

ii. "Journalist Exception"

"Personal information gathered for publication, broadcast or other forms of public communication of journalistic material, whether used or not, as well as information found in previously published material disseminated from media archives", are not subject to the Safe Harbor requirements.¹⁵⁴

iii. "Secondary Liability"

"There is no liability incurred by information transmitters, e.g. ISP's , telecommunication companies who merely transmit the information for another entity but who do not determine the purpose for which the information is gathered and who do not determine the means of process the personal information."¹⁵⁵

VI. PRACTICAL ISSUES – To Sign Up or Not to Sign Up

Although the U.S. Department of Commerce states that "the Safe Harbor framework offers a simpler and cheaper means of complying with the adequacy requirements of the Directive, which should particularly benefit small and medium enterprises,¹⁵⁶" it is not clear whether companies should rush to jump on board the Safe Harbor. The fact that companies are slow to respond to the opportunity of the Safe Harbor may indicate that a critical look at the Safe Harbor is warranted.

A. Risks of Not Being on Board and Benefits of Entering the Safe Harbor

i. Risks

Clearly the number one risk of not complying with the Safe Harbor provisions is the potential cut-off of data flow from the EU. When a data protection authority in the EU has determined that a U.S. company is violating the Safe Harbor principles or there is a substantial likelihood that the principles will be violated, and determines that individuals may be vulnerable to imminent risk or significant damage, then the data flow may be cut off but only after the EU country makes all reasonable efforts to provide the relevant U.S. company with notice and an opportunity to respond.¹⁵⁷ In addition, U.S. firms may be subject to prosecution in the EU for violations of the Safe Harbor principles if there is jurisdiction over the company in the EU and the company does not follow the Safe Harbor provisions.¹⁵⁸

"The Commission is closely monitoring the results of U.S. companies applying the "Safe Harbor" principles. The E.U. executive body continues to insist that it will not hesitate to revoke its agreement with the United States and push for the blockage of trans-Atlantic data flows if strict rules based on access to data for private citizens are violated" or if there are an insufficient amount of U.S. companies that sign up for the Safe Harbor.¹⁵⁹ "If the agreement is abandoned, EU firms will have to set up contracts with all U.S. companies to which they send consumer data or clear it with the individuals concerned or cut off the data flow."¹⁶⁰

ii. Benefits

On the other hand, If more U.S. companies join the Safe Harbor it will reduce the chance that any U.S. firms will be targeted by the EU and may avoid more stringent future regulations.¹⁶¹ Also, the Safe Harbor provides a understandable, predictable and comprehensive approach to data privacy. No longer are companies faced with the prospect of complying with different data privacy laws in each EU country in order to have personal data flow from the EU to the U.S.¹⁶² If a company complies with the Safe Harbor, a finding of adequacy is automatic.¹⁶³ The listing of those companies certifying compliance with the Safe Harbor also provides transparency and thus efficiency to participants in transferring personal data to the U.S.¹⁶⁴

B. Reasons For Caution

i. Not Many Sign Up Yet (Competitive Disadvantage?)

As of the writing of this paper, very few U.S. companies had signed up for the Safe Harbor which has required the Department of Commerce to put on road-shows to drum up interest and avoid embarrassment.¹⁶⁵ "Most of the companies that have signed up, with a few exceptions, are small to medium size businesses.¹⁶⁶ Many larger Fortune 500 type companies are still "investigating their options or taking a 'wait and see' approach" said Jeff Rohlmeier, a trade official at the Commerce Department.¹⁶⁷ One Commerce Department official admitted that more would have to agree to be governed by the Safe Harbor to satisfy the Europeans."¹⁶⁸

The fact that many large corporations are carefully considering whether or not to enter into the Safe Harbor is an indicator that U.S. companies should carefully weigh the costs and benefits of

doing so. One large cost is that once you enter the Safe Harbor, data transferred during that period is always subject to the Safe Harbor principles even if you subsequently leave the Safe Harbor. This could force a company to deal with its data using two distinct databases.

ii. Too Early – More Changes to Come?

No one is totally happy with the Safe Harbor and there is such considerable disagreement on the whole privacy issue that there is significant likelihood that the current Safe Harbor is not the final solution to the problem.¹⁶⁹

"Privacy advocates and consumer groups both in the U.S. and Europe are highly critical of the European Commission's decision to approve the agreement, which they say will fail to provide European citizens with adequate protection for their personal data."¹⁷⁰ "The Safe Harbor agreement 'lacks an adequate means of enforcement,'" Marc Rotenberg, executive director of the Electronic Privacy Information Center in Washington added "[w]e think this needs some legal bite. Right now, it's a system that basically allows companies to self-certify without any real expectation of government oversight."¹⁷¹ Likewise, many commentators on the other side of the issue have criticized the Safe Harbor as being too restrictive or impracticable.¹⁷² The criticism has best been evidenced during the House of Representatives Energy and Commerce Subcommittee on Commerce, Trade and Consumer Protection hearing. "The European Union is insisting that [its regulations] be treated as the de facto global standard."¹⁷³ Also, the EU is not even solidly behind the Safe Harbor. The European parliament on July 5th 2000 expressed its opposition to the Safe Harbor deal.¹⁷⁴ "In early July [2000] the European Parliament approved a forceful resolution that the agreement needed to be renegotiated in order to provide adequate protection."¹⁷⁵

There may also be change on the U.S. front. "It remains to be seen whether U.S. legislators will complement the Safe Harbor provisions by enacting any one of several dozens policy bills."¹⁷⁶ A key member of the U.S. House Commerce Committee urged the Bush administration to review the impact of the European Union's tough data privacy rules on U.S. companies, saying they could have costly implications for companies based here.¹⁷⁷ U.S. Rep. Clifford Stearns (R-Fla.), the chairman of the House subcommittee on Commerce, Trade and Consumer Protection, also warned during a crowded hearing here that the EU's Privacy Directive could have a "potentially regressive impact on international commerce." Also, Billy Tauzin, R-La., Chairman of the committee said he would work with the Bush administration to consider not taking part in the EU Privacy Directive.¹⁷⁸ This criticism seems to be bolstered by evidence showing the ineffectiveness of the EU data privacy laws.¹⁷⁹ Overall, there seems to be rising sentiment on the U.S. side that the EU "needs to get its own house in order before imposing its will upon the rest of the world."¹⁸⁰

For now, the Safe Harbor is holding firm against demands to scrap the privacy protections. The EU Commission rejected Bush Administration concerns about the directive imposing "unduly burdensome requirements that are incompatible with real world operations."¹⁸¹ But the EU Commission did "promise to re-open negotiations on the arrangement if the remedies available to European citizens prove inadequate."¹⁸² Therefore "[t]he future of the Safe Harbor data protection agreement between the EU and the U.S. looks uncertain."¹⁸³

C. Bad Precedent

Personal data covers both facts and opinions about the individual and also includes information regarding the intentions of the data controller towards the individual, e.g. the individual is a bad credit risk. This poses a significant problem if it is determined that corporate processes which contain confidential or trade secret information could be disclosable solely because they relate to the processing of personal information.¹⁸⁴ In other words, it could be argued that the credit analysis algorithm that a company uses in denying an individual credit is disclosable as part of the opinion contained within "Personal data."

D. Cost

Cost is another consideration that must be weighed in determining whether to enter the Safe Harbor. It is apparent that complying with the Safe Harbor will increase a corporation's costs.¹⁸⁵ For example, Redmond, Washington-based Microsoft reportedly spent approximately U.S.\$500,000 complying with the conditions of the Safe Harbor doctrine, which covers infrastructure and training to ensure compliance with the Safe Harbor principles with data that is processed electronically, through contracts, phone calls and other correspondence.¹⁸⁶

E. Some Alternative Practices To Think About

As an alternative to entering the Safe Harbor, you may want to consider:

1. Appointing a privacy officer to assess and monitor privacy policies and regulatory changes, suggest modifications to policies and educate personnel on best practices. It is a good idea to comply with what you say you are doing regardless if you join the Safe Harbor. Also, having someone in charge of privacy is fast becoming the industry standard.¹⁸⁷
2. Having a contingency or disaster recovery plan in the event a data supplier cuts off the supply of data.
3. Joining industry privacy groups for guidance and assistance and to obtain data protection guidelines.¹⁸⁸ Also, you will have greater impact in making privacy laws workable by joining these organizations which help develop the privacy standards.¹⁸⁹

VII. HELPFUL RESOURCES

Here are some websites, books and seminars where you can find further detail on the subject.

A. EU Privacy Directive

Full text of the Directive 95/46/EC. www.europa.eu.int; http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html; http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

The European Commission's website. http://www.europa.eu.int/comm/index_en.htm.

Standard contractual clauses for the transfer of personal data to countries outside of the European Union pursuant to the Directive along with further interpretation of the Directive.

http://europa.eu.int/eur-lex/en/dat/2001/l_181/l_18120010704en00190031.pdf

B. UK Data Protection Act

Text of the Data Protection Act of 1998.

www.legislation.hmso.gov.uk/acts/acts1998/19980029.htm.

Office of the Information Commissioner in the UK www.dataprotection.gov.uk
www.europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm.

Information on the UK Data Protection Act of 1998 and the Commission that enforces it.

www.dataprotection.gov.uk

Overview of EU Data Protection Directive with listing of Data Protection Commissioners in the EU. <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>

www.elexica.com has a good overview of the DPA, "Data Protection – The New Statutory Regime: A Summary of the Main Provisions of the Data Protection Act of 1998, 5/31/00. Cost is 10 GBP.

Some good guidance for data controllers subject to the UK Data Protection Act 1998 can be found at www.ccta.gov.uk/dpr/dpdoc.nsf and

<http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>.

C. EU/U.S. Safe Harbor

Text of the EU/U.S. Safe Harbor. www.ita.doc.gov/td/ecom/menu.html;
http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm;
www.ita.doc.gov/td/ecom/menu.html; and www.export.gov/safeharbor/.

This site provides information to enable U.S. companies to "evaluate and then join" the EU/U.S. Safe Harbor. Also has list of companies participating in the Safe Harbor

www.export.gov/safeharbor

Here is the form used by companies to annually certify compliance with EU/U.S. Safe Harbor

<http://web.tia.doc.gov/safeharbor/shreg.nsf/safeharbor?openform>

For further discussion on U.S. concerns with the Safe Harbor see Mr. Jonathan Winer, Counsel Altson and Bryd LLP Subcommittee on Commerce, Trade, and Consumer Protection Hearing

[The EU Data Protection Directive: Implications for the U.S. Privacy Debate](http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm) March 08, 2001

<http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm>

D. Miscellaneous

Here is the EU's "One-Stop-Shop" for EU Law.

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/915|0|RAPID&lg=EN

www.privacyinternational.org Privacy International is a human rights group formed in 1990 as a watchdog on surveillance by governments and corporations.

www.gbd.org/ie/2000/privacy.html. The Global Business Dialogue on Electronic Commerce is a world-wide CEO driven effort to develop policies that promote global electronic commerce for the benefit of business or consumers everywhere. They provide guidelines on compliance with the Directive.

You can also review security policies at various sites, including the www.privacyalliance.com; www.privacy.org; www.truste.com from there you can follow links to other sites.

ACCA Docket , the Journal of the American Corporate Counsel Association Vol 19 No. 5, "Regulation of Electronic Commerce in Europe: A Corporate Counsel Guide by Simon G. Zinger p.49 (very good listing of European Union sites providing updates and detailed examination of regulatory efforts.) www.acca.com.

www.house.gov/commerce/hearings/03082001-49/08082001.htm. List of witnesses and their testimony at the EU Data Protection Directive: Implications for the U.S. Privacy Debate hearing before the House of Representatives Subcommittee on Commerce Trade and Consumer Protection of the Committee on Energy and Commerce.

Annual BNA Public Policy Forum Cyber security & Privacy. For more information email pike@pf.com

Annual Privacy & Data Protection Summit sponsored by the Privacy Officers Association is an annual privacy conference. Get more details at www.privacyassociation.org

www.epic.org The Electronic Privacy Information Center is a public interest research center in Washington, D.C. Their bookstore www.epic.org/bookstore has the Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar; and the Privacy Law Sourcebook 2000 United States Law, International Law and Recent Developments, Rotenberg, which besides being an overview of domestic and international privacy laws also contains an extensive listing of agencies addresses and privacy websites.

VIII. CONCLUSION – "TEN THINGS YOU SHOULD TAKE AWAY FROM THIS PRESENTATION"

1. The EU Privacy Directive is a comprehensive approach to privacy protection based upon the Government's duty to protect privacy whereas the U.S. employs a sectoral approach where privacy is a right of the individual. The EU has determined that the U.S. has inadequate personal data privacy protections.
2. The Directive is the basis for EU member country laws and all EU countries are required to pass privacy legislation containing its principles, including a prohibition against transfer of personal information to countries outside of the EU with inadequate privacy laws.
3. The UK Data Protection Act 1998 was implemented based upon the EU Privacy Directive and includes the prohibition against transfer of personal information to third countries with inadequate privacy laws, the so-called "Eighth Principle."
4. Like most statutes, to really understand the impact of the Act it is important to know the definitions to its key terms (Data Controller, Data Subject, Personal Data and Processing), and always look for one of the exceptions to the Eighth Principle so that you can transfer the data regardless if it is to a country with inadequate privacy protection.
5. The Safe Harbor is an agreement between the U.S. and the EU wherein if a company certifies (and maintains compliance) with a series of privacy principles including notice, choice, transfers to third parties, access, security, data integrity and enforcement, then it will not be prevented from receiving personal data from the EU just because the U.S. has inadequate data privacy protection.
6. Two ways to comply: self-certification by signing up at the Department of Commerce website, and using Model Contracts.
7. Companies must carefully weigh the costs and benefits before entering the Safe Harbor in light of the extent of personal data they are gathering and the extent of their dealings in Europe.
8. The main benefit of the Safe Harbor is certainty that data flows will continue uninterrupted.
9. The downsides to agreeing to the Safe Harbor are that not many have signed up and due to the major disagreements about the Safe Harbor there may be changes to come. There is also significant cost to complying with the Safe Harbor and once you enter the Safe Harbor then you are bound by its principles for the information you gathered while you were in the Safe Harbor.
10. For more guidance see the FAQs attached to the Safe Harbor, and the resources listed in Section VII of this paper or in the endnotes.

¹ I wish to thank Mary Kay Mahota and Samantha Standish, Esq. for their editorial assistance.

² Mr. Jonathan Winer, Counsel Altson and Bryd LLP, testifying before the House Subcommittee on Commerce, Trade, and Consumer Protection [The EU Data Protection Directive: Implications for the U.S. Privacy Debate](http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm) March 08, 2001 <http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm>.

³ Mr. Jonathan Winer, Counsel Altson and Bryd LLP, testifying before the House Subcommittee on Commerce, Trade, and Consumer Protection [The EU Data Protection Directive: Implications for the U.S. Privacy Debate](http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm) March 08, 2001 <http://www.house.gov/commerce/hearings/03082001-49/Winer103.htm>; See also "Internet Data Privacy: The Need For Caution" by Thomas M. Regan and Terry M. Henry in "Outside Counsel" Summer 2001 published by ACCA citing "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress" Federal Trade Commission, May 2000 ("A February 2000 survey of random websites by the Federal Trade Commission ("FTC") found that almost 97 percent collected some type of personally identifying information).

⁴ "EU-U.S. Clash over personal data: private right or commercial opportunity?" by Peronet Despeignes and Deborah Hargreaves, FT.com Financial Times, 3/29/01 www.globalarchive.ft.com/globalarchive/articles.html?id=010329000406.

⁵ "Key U.S. lawmaker calls for review of Europe's privacy laws" by Patrick Thibodeau, March 8, 2001, Computerworld http://computerworld.com/cwi/story/0%2C1199%2CNAV47_STO58406_NLTpm%2C00.html (quoting Stefano Rodota, the chairman of the EU committee that developed the data protection standard.)

⁶ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.8 ("The new capabilities of collecting, processing and making decisions based upon that information along with increased uses for surveillance has prompted demands for specific rules governing the collections and handling of personal information").

⁷ Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031-0050, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

⁸ Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281, 23/11/1995 p. 0031-0050, http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

⁹ www.export.gov/safeharbor "Welcome to the Safe Harbor".

¹⁰ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.9-10.

¹¹ Data Protection Act 1998, 1998 Chapter 29, ISBN 0 10 542998 8, <http://www.legislation.hmso.gov.uk/acts/acts/1998/19980029.htm>. However, a few EU countries have not passed legislation pursuant to the Directive, Ireland, Luxembourg, France and Germany. World Internet Law Report, March 2001, Vol. 2, Issue 3, BNA International page 5; But see Germany passed legislation in July 2001.

¹² Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.15.

¹³ www.export.gov/safeharbor "Welcome to the Safe Harbor."

¹⁴ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.230.

¹⁵ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.230-231; see also The Privacy Law Sourcebook 2000 United States Law, International Law and Recent Developments, Rotenberg, Electronic Privacy Information Center (Washington, D.C., 2000).

¹⁶ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.230-231; see also The Privacy Law Sourcebook 2000 United States Law, International Law and Recent Developments, Rotenberg, Electronic Privacy Information Center (Washington, D.C., 2000).

¹⁷ www.export.gov/safeharbor "Welcome to the Safe Harbor".

¹⁸ "European Union Oks Safe Harbor" by Jason Spingarn-Koff on Wired News www.wired.com/news/politics/0,1283,36671,00.html ("American financial, insurance, tourism and airline industries pursued for the Safe Harbor agreement so they could use personal data collected on European consumers."); see also Safe Harbor Principles Issued by the U.S. Department of Commerce on July 21, 2000, www.export.gov/safeharbor/shprinciplesfinal.htm; see also World Internet Law Report, March 2001, Vol. 2, Issue 3, BNA International page 5.

¹⁹ www.export.gov/safeharbor "Welcome to the Safe Harbor". ("The U.S., specifically the DOC and the FTC envisioning a potential personal data trade war, entered into negotiations with the EU to work out an agreement."); see also "European Union Oks Safe Harbor" by Jason Spingarn-Koff, Wired News, www.wired.com/news/politics/0,1283,36671,00.html.

²⁰ Safe Harbor Principles Issued by the U.S. Department of Commerce on July 21, 2000, www.export.gov/safeharbor/shprinciplesfinal.htm; see also World Internet Law Report, March 2001, Vol. 2, Issue 3, BNA International page 5.

²¹ www.export.gov/safeharbor "Welcome to the Safe Harbor."

²² www.export.gov/safeharbor "Welcome to the Safe Harbor."

²³ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.8.

²⁴Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.8.

²⁵www.export.gov/safeharbor "Safe Harbor Overview" and "Safe Harbor Benefits."

²⁶www.export.gov/safeharbor "Welcome to the Safe Harbor."

²⁷Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/shprinciplesfinal.htm.

²⁸ Baker & McKenzie European bulletin Vo 12 No. 3 p. 13.

²⁹ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt.

³⁰Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000

www.export.gov/safeharbor/shprinciplesfinal.htm.

³¹ "Data Protection in the European Union," page 5 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

³² "Data Protection in the European Union" – The European Legislation on Data Protection, page 4

<http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

³³ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

³⁴ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

³⁵ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

³⁶ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

³⁷ "Data Protection in the European Union," page 7 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

³⁸ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt.

³⁹ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt.

⁴⁰ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt.

⁴¹ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt; see also Data Protection in the European Union," page 7 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

⁴² "Data Protection in the European Union," page 5 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

⁴³ "Data Protection in the European Union," page 5 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

⁴⁴ "Data Protection in the European Union," page 5 <http://europa.eu.int/comm/dg10/publications/brochures/dialogue/data/en.pdf>.

⁴⁵ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

⁴⁶ See Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Article 25); Baker & McKenzie European bulletin Vo 12 No. 3 p. 13.

⁴⁷ Article 26 of the Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 6 and 7); see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP, www.hugheshubbard.com

⁴⁸ Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles 12-15; see also Regulation of the Internet in the European Union and the European Union Data Protection Directive, "From Bricks to Clicks: Legal and Business Issues of Taking your "Bricks and Mortar" business onto the Internet, 11/15/99 Fellas and Winterfeldt of Hughes Hubbard and Reed LLP,

⁴⁹ Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles Article 11.

⁵⁰ Directive http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html (Full text of the Directive 95/46/EC Articles Article 12.

- ⁵¹ European Commission Press Release IP/95/822 July 25, 1995 "Council Definitively Adopts Directive on Protection of Personal Data." www.privacy.org/pi/intl_orgs/ec/dp_EC_press_release.txt
- ⁵² Comments of Ambassador David L. Aaron, Senior International Advisor, Dorsey & Whitney testifying before the House Subcommittee on Commerce, trade and Consumer Protection "The EU Data protection directive: Implications for the U.S. Privacy Debate," 3/8/01, www.house.gov/commerce/hearings/03082001-49/Aaron102.htm.
- ⁵³ See Data protection Act 1984 and 1998, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; see also Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – (The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner); see also Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.224.
- ⁵⁴ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.224.
- ⁵⁵ Data protection Act 1998 The Eight Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) Section 5.1.
- ⁵⁶ See Data protection Act 1998 Part I Section 4 and attached schedules, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>
- ⁵⁷ See Data protection Act 1998 Part III, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁵⁸ See Data protection Act 1998 Section 4(4), <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>.
- ⁵⁹ www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>
- ⁶⁰ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁶¹ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; see also www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>
- ⁶² Commissioners website. See also Recital 26 of Directive 95/46/EC.
- ⁶³ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁶⁴ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; see also www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>.
- ⁶⁵ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁶⁶ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; see also www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>.
- ⁶⁷ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; see also www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>.
- ⁶⁸ See Data protection Act 1998 Part II, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁶⁹ See Data protection Act 1998 Part II, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁷⁰ See Data protection Act 1998 Part II, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁷¹ See Data protection Act 1998 Part II, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁷² www.ccta.gov.uk/dpr/dpdoc.nsf; <http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>
- ⁷³ See Data protection Act 1998 Part II, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>;
- ⁷⁴ See Data protection Act 1998 Part I with attached schedule, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.ccta.gov.uk/>; Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – section 3.1 (The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner).

⁷⁵ Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 3.1.

⁷⁶ Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 4.1.

⁷⁷ Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) 4.1; see also Data Protection Act 1998 "International Transfers of Personal Data Advice on compliance with the 8th data protection principle", for examples of valid consent language; see also Office of the Information Commissioner www.dataprotection.gov.uk. ("Transfer is not the same as transit. The 8th Principle only comes into play if data move to rather than simply pass through a country outside the UK. If personal data pass through country 'B' on the way from the UK to country 'A' or even on the way from one location in the UK to another in the UK, there is only likely to be a transfer to country 'B' if some substantive processing operation takes place en route. This would be the case if, for example, the data were accessed, combined with other data or altered. A transfer takes place not only if the information transferred is held as personal data in the UK but also if it is intended that it will be held as personal data after transfer. For example, the requirements of the 8th Principle apply if notes made about an identifiable individual, although not held on computer or as part of a relevant filing system in the UK, are telephoned or faxed to a colleague in another country with the intention that they will be entered on a computer or kept in a relevant filing system in that country. Putting personal data on a web site will almost certainly involve transfers to countries outside the UK. The transfers are to any countries from which the web site is accessed.")

⁷⁸For detailed examples on application of the adequacy test see Data Protection Act 1998 International Transfers of Personal Data Advice on compliance with the 8th data protection principle, "International Transfers of Personal Data: Advice on Compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk ("The Act indicates the sort of factors the data controller should take into account in reaching such a decision. These relate to the nature of the data being transferred, how they will be used and the laws and practices of the country to which they are being transferred. It implies some form of risk assessment. The data controller, must decide whether, in all the circumstances of the case, there is sufficient protection for individuals. In assessing adequacy a data controller should look not just at the extent to which data protection standards have been adopted but also at whether there is a means of ensuring the standards are achieved in practice and whether there is an effective mechanism for individuals to enforce their rights or obtain redress if things go wrong. It is recognized that a detailed analysis of adequacy in a non-EEA country will very often be impractical for a UK data controller. Such an analysis might be appropriate for a business that routinely transfers large volumes of data to a particular country. It is unlikely to be carried out by a data controller that might only occasionally transfer data to any of a wide range of countries. There are some cases where a data controller might reasonably conclude that adequacy exists without carrying out a detailed adequacy test. The first of these is where data are transferred for processing under the data controller's instructions to a processor outside the UK. This is likely to be a common situation. The UK data controller remains in control of the data even though the data have left the country to be processed elsewhere. Here the 7th Principle requires the data controller to have a contract with the processor committing the processor to adopt proper security measures and act only on instructions from the controller. Such a contract should be sufficient to deliver adequacy unless there is a particular reason to suppose it does not, for example the data are sensitive and the transfer is to an unstable country where the data are clearly at risk regardless of any contract that is in place. There might also be other cases where the nature of the data and the circumstances of the transfer coupled with the data controller's knowledge of the country of transfer and the particular recipient mean it is reasonable to conclude there is adequacy without the need for a detailed analysis. Some examples are discussed below").

⁷⁹ "Data Protection – The New Statutory Regime: A Summary of the Main Provisions of the Data Protection Act of 1998," 5/31/00 www.elexica.com; see also Data protection Act 1998 The Eight Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 6.1 commenting on the applicability of the principles of Article 25(2) of the EU Privacy Directive as implemented by the UK Data Protection Act 1998.

⁸⁰Data protection Act 1998; see also The Eight Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 13.1 (When countries are designated as adequate, details will be published on the Commissioner's web site <http://www.dataprotection.gov.uk>).

⁸¹ Data protection Act 1998; see also The Eight Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 8.1.

⁸² See Data protection Act 1998 Part IV, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and <http://www.hmso.gov.uk/acts> and; <http://wood.cta.gov.uk/>; Data protection Act 1998 The Eighth Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 14.4 (see this guide for best practices details)

⁸³Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.13.

⁸⁴See DATA PROTECTION ACT 1998; see also "International Transfers of Personal Data: Advice on Compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk ("Consent must be freely given. It can be made a condition for the provision of a non-essential service but consent is unlikely to be valid if the data subject has no real choice but to give his/her consent. For example, if an existing employee is required to agree to the international transfer of personal data any consent given is unlikely to be valid if the penalty for not agreeing is dismissal. Consent must also be specific and informed. The data subject must know and have understood what he/she is agreeing to. The reasons for the transfer and as far as possible the countries involved should be specified. If the data controller is aware of any particular risks involved in the transfer it should bring these to the data subject's attention.").

⁸⁵ See DATA PROTECTION ACT 1998; see also "International Transfers of Personal Data: Advice on Compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk (Transfers can be made when there is a contract between the data controller and the data subject and the transfer is necessary for performance of the contract, or the transfer is a necessary part of pre-contractual steps taken by the data controller at the request of the data subject. Or, a contract between the data controller and someone other than the data subject and the contract is entered into at the data subject's request (or in his/her interests), and the transfer is necessary for performance of the contract or the transfer is necessary for conclusion of the contract. The Commissioner takes the view that the determination of whether a transfer is "necessary" for the performance of a contract depends on the nature of the goods, services etc. provided under the contract rather than the business structure of the data controller. A transfer is not "necessary" if the only reason it is needed is because of the way a data controller has chosen to structure its business.").

⁸⁶ See DATA PROTECTION ACT 1998; see also "International Transfers of Personal Data Advice on compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk ("Transfers can be made where they are necessary for reasons of substantial public interest. This is most likely to be in areas such as crime prevention and detection, national security and tax collection. The Commissioner advises data controllers intending to rely on this exception to adopt a similar case by case test to that required by many of the exemptions in the Act, in particular Section 29 (the crime and taxation exemption). A transfer of any personal data should only take place to the extent that there would be likely to be substantial prejudice to the public interest if the transfer of those personal data did not take place. Further guidance on Section 29 is given in the Commissioner's Introduction to the 1998 Act.").

⁸⁷ See DATA PROTECTION ACT 1998; see also International Transfers of Personal Data Advice on compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk . ("Transfers can be made where they are necessary: in connection with any legal proceedings (including prospective proceedings) or for obtaining legal advice or otherwise for establishing, exercising or defending legal rights. It is clear that the legal proceedings do not necessarily have to involve the data controller or the data subject and that the legal rights do not have to be those of either the data controller or the data subject. Although the application of this exception is potentially quite wide, it is not immediately obvious where transfers might be necessary for "establishing, exercising or defending legal rights" if they are not in connection with legal proceedings or for obtaining legal advice.").

⁸⁸ See DATA PROTECTION ACT 1998; see also International Transfers of Personal Data Advice on compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk . ("This relates to matters of "life and death". For example, it would cover the transfer of relevant medical records from the UK to another country where an individual had been taken seriously ill or involved in a serious accident.").

⁸⁹www.elexica.com has a good overview of the DPA, "Data Protection – The New Statutory Regime: A Summary of the Main Provisions of the Data Protection Act of 1998, 5/31/00, Cost is 10 GBP; see also comments of David Smith, Assistant Commissioner, Office of the UK Information Commissioner testifying before the House Subcommittee on Commerce, Trade and Consumer Protection Hearing on 3/8/01, www.house.gov/commerce/hearings/03082001-49/Smith101.htm

⁹⁰ See DATA PROTECTION ACT 1998; see also International Transfers of Personal Data Advice on compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk

⁹¹ See DATA PROTECTION ACT 1998; see also International Transfers of Personal Data Advice on compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk

⁹² Data protection Act 1998; see also "The Eight Data Protection Principle and Transborder Dataflows – The data protection Commissioner's legal analysis and suggested "good practice approach" to assessing adequacy including consideration of the issue of contractual solutions (This is the preliminary view of the data protection Commissioner) section 17.1.

⁹³ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.14; see also European Union, Internal Market Directorate, Background Information: Transfer of data to non-EU countries – FAQ http://europa.eu.int/comm/internal_market/en/media/dataprot/backinfo/info.htm.

⁹⁴ http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/851|0|RAPID&lg=EN ("The Decision also does not prevent national Data Protection Authorities authorizing other 'ad hoc' contractual arrangements for the export of data out of the EU based on national law, as long as these authorities are satisfied that the contracts in question provide adequate protection for data privacy.").

⁹⁵ Data protection Act 1998 "International Transfers of Personal Data: Advice on Compliance with the 8th data protection principle" Office of the Information Commissioner www.dataprotection.gov.uk

⁹⁶ See [press release](#) on Data protection "Commission approves standard contractual clauses for data transfers to non-EU countries", IP/01/851 Brussels, 18 June 2001, at http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/851/0/RAPID&lg=EN (Member States must recognize that companies or organizations using such standard clauses in contracts concerning personal data transfers to countries outside the EU are offering "adequate protection" to the data, in compliance with the [Data Protection Directive](#).); See also Baker & McKenzie Global E-law Report 6/24/01.

⁹⁷ http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/851/0/RAPID&lg=EN (see IP/00/865). (Further information about this Decision and the standard contractual clauses, including exchanges of letters with business associations and the U.S. Departments of Commerce and Treasury, are available on the Europa website).

⁹⁸ http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/851/0/RAPID&lg=EN

⁹⁹ www.house.gov/commerce/hearings/03082001-49/Smith101.htm

¹⁰⁰ Comments of the Data Commissioner in "Introduction to the 1998 Act"; wood.cta.gov.uk

¹⁰¹ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.13.

¹⁰² Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.12.

¹⁰³ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.12.

¹⁰⁴ Former Secretary of Commerce William Daley <http://www.useu.be/ISSUES/dpriv0314.html> ("This data privacy success comes none too soon to support the growth of the almost 2 trillion dollar U.S.-EU trade and investment relationship, particularly in the rapidly growing business-to-business and retailing e-commerce sectors.")

¹⁰⁵ www.export.gov/safeharbor "Welcome to the Safe Harbor".

¹⁰⁶ http://europa.eu.int/comm/internal_market/en/media/dataprot/news/safeharbor.htm;
www.ita.doc.gov/td/ecom/menu.html; www.export.gov/safeharbor/.

¹⁰⁷ Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000

www.export.gov/safeharbor/shprinciplesfinal.htm (A company only has to apply the principles to personal information gathered after entering into the Safe Harbor, however, a company may apply the principles to all information retroactively if it wishes to do so.).

¹⁰⁸ Cover letter from Acting Under Secretary Robert S. LaRussa to U.S. organizations – July 21, 2000, www.export.gov/safeharbor/larussacovernote717.htm.

¹⁰⁹ "The standard contractual clauses contain a legally enforceable declaration ("warrant") whereby both the "Data Exporter" and the "Data Importer" undertake to process the data in accordance with basic data protection rules and agree that individuals may enforce their rights under the contract. So far, only Switzerland, Hungary and the U.S. 'Safe Harbor' arrangement have been recognized as providing adequate protection."

http://europa.eu.int/rapid/start/cgi/guesten.ksh?p_action.gettxt=gt&doc=IP/01/851/0/RAPID&lg=EN

¹¹⁰ Comments of Ambassador David L. Aaron, Senior International Advisor, Dorsey & Whitney, testifying before the House Subcommittee on Commerce, trade and Consumer Protection "The EU Data protection directive: Implications for the U.S. Privacy Debate", 3/8/01 <http://www.house.gov/commerce/hearings/03082001-49/Aaron102.htm>

¹¹¹ Cover letter from Acting Under Secretary Robert S. LaRussa to U.S. organizations – July 21, 2000, www.export.gov/safeharbor/larussacovernote717.htm ; See also Former Secretary of Commerce William Daley <http://www.useu.be/ISSUES/dpriv0314.html>

¹¹² www.export.gov/safeharbor "How Does an Organization Join."

¹¹³ "EU gives final OK to U.S. Safe Harbor privacy plan, by Elizabeth de Bony, IDG News Service/Brussels Bureau July 27, 2000.

¹¹⁴ www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm

¹¹⁵ <http://www.export.gov/safeharbor/>

¹¹⁶ Quote from www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹¹⁷ Quote from www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹¹⁸ Quote from (FAQs) FAQ 12 – Choice – Timing of Opt Out, www.export.gov/safeharbor/FAQ12Opt-OutFINAL.htm

¹¹⁹ Quote from www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹²⁰ Quote from www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹²¹ (FAQs) FAQ 8 – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm.

¹²² (FAQs) FAQ 8 – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm.

¹²³ (FAQs) FAQ 8 – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm.

¹²⁴ (see FAQ 8) – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm.

¹²⁵ (FAQs) FAQ 8 – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm

¹²⁶ (FAQs) FAQ 8 – Access, www.export.gov/safeharbor/FAQ8AccessFINAL.htm.

¹²⁷ www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹²⁸ www.export.gov/safeharbor "What Do the Safe Harbor Principles Require".

¹²⁹ www.export.gov/safeharbor "How and Where Will the Safe Harbor Be Enforced". See also www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm "How and Where will the Safe Harbor be enforced".

¹³⁰ www.export.gov/safeharbor ("How and Where Will the Safe Harbor Be Enforced" "As part of their Safe Harbor obligations, organizations are required to have in place a dispute resolutions system that will investigate and resolve individual complaints as and disputes and procedures of verifying compliance. In order to ensure compliance, the dispute resolution process must contain sufficient penalties (including suspension or revocation of participation from the privacy program) and publicity of non-compliance. There is no particular way in which a company must comply with a dispute resolution process as long as it contains the above parameters."); See also <http://www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm> (The dispute resolution, verification, and remedy requirements can be satisfied in different ways. "For example, an organization could comply with a private sector developed privacy seal program that incorporates and satisfies the Safe Harbor principles. If the seal program, however, only provides for dispute resolution and remedies but not verification, then the organization would have to satisfy the verification requirement in an alternative way. Organizations can also satisfy the dispute resolution and remedy requirements through compliance with government supervisory authorities or by committing to cooperate with data protection authorities located in Europe.").

¹³¹ www.export.gov/safeharbor "What Do the Safe Harbor Principles Require". See also Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.8.

¹³² <http://web.tia.doc.gov/safeharbor/shreg.nsf/safeharbor?openform>

¹³³ (FAQs) FAQ 6 – Self-Certification, www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm.

<http://www.ita.doc.gov/td/ecom/SafeHarborOverviewAug00.htm> ("Private sector self regulation and enforcement will be backed up by government enforcement of the federal and state unfair and deceptive statutes. The effect of these statutes is to give an organization's Safe Harbor commitments the force of law vis a vis that organization." The Department of Commerce will indicate on the public list it maintains of organizations self certifying adherence to the Safe Harbor requirements any notification it receives of persistent failure to comply and will make clear which organizations are assured and which organizations are no longer assured of Safe Harbor benefits. An organization applying to participate in a self-regulatory body for the purposes of re-qualifying for the Safe Harbor must provide that body with full information about its prior participation in the Safe Harbor"). For more examples see www.export.gov/safeharbor "How and Where Will the Safe Harbor Be Enforced".

¹³⁴ www.export.gov/safeharbor "What Do the Safe Harbor Principles Require"; see also Baker & McKenzie European bulletin Vo 12 No. 3 p. 13 ("EU member countries are allowed...to suspend the flow of personal data to U.S. companies under certain circumstances. These included cases where the U.S. body has said that a company is violating the principles, where there is a substantial likelihood that they will be violated and where data subjects may be vulnerable to imminent risk or grave harm. In such a case the member country must make all reasonable efforts to provide the relevant U.S. company with notice and an opportunity to respond. If the country fails in this responsibility the EU commission must inform the DOC immediately").

¹³⁵ (FAQs) FAQ 7 – Verification, www.export.gov/safeharbor/Faq7verifFINAL.htm

¹³⁶ Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm .

¹³⁷ Quote from Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm .

¹³⁸ Quote from Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm .

¹³⁹ Quote from Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm .

¹⁴⁰ Quote from Safe Harbor Privacy Principles Issued by the U.S. Department of Commerce on July 21, 2000,

www.export.gov/safeharbor/SHPRINCIPLESFINAL.htm .

¹⁴¹ See e.g. TrustE's program at <http://www.ecommercetimes.com/perl/story/4719.html>;

¹⁴² Frequently Asked Questions (FAQs) FAQ 6 – Self-Certification, www.export.gov/safeharbor/FAQ6SelfCertFINAL.htm;

www.export.gov/safeharbor "How Does an Organization Join"; see also Baker & McKenzie European bulletin Vo 12 No. 3 p. 14; see also Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.16. ("The principles require all signatory organizations to provide individuals with "clear and conspicuous" notice of the kind of information they collect, the purposes for which it may be used, and any third parties to whom it may be disclosed. This notice must be given at the time of collection of any personal information or "as soon thereafter as is practicable." Individuals must be given the ability to choose (opt-out of_ the collection of data where the information is either going to be disclosed to a third party or used for incompatible purpose. In the case of sensitive information, individuals must expressly consent (opt-in) to the collection. Organizations wishing to transfer data to a third party may do so if the third party subscribes to Safe Harbor or if that third party signs an agreement to protect the data. Organizations must take reasonable precautions to protect the security of information against loss, misuse and unauthorized access, disclosure, alteration and destruction. Organizations must provide individuals with access to any personal information held about them and with the opportunity to correct, amend, or delete that information where it is inaccurate. This right is to be granted only if the burden or expense of providing access would not be disproportionate to the risks to the individual's privacy or where the rights of persons other than the individual would not be violated.").

¹⁴³ www.export.gov/safeharbor "How Does an Organization Join"; see also www.ita.doc.gov/td/ecom/SafeharborOverviewAug00.htm; see also "Microsoft to Sign EU Privacy Accord" Lori Enos 5/16/01 www.ecommercetimes.com/perl/story/9752.html

¹⁴⁴ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.16. See also Baker & McKenzie European bulletin Vo 12 No. 3 p. 13.

¹⁴⁵ <http://www.ita.doc.gov/td/ecom/FRN2.htm>. "Specifically, self-certification procedure is as follows:

1. To be included on the Safe Harbor list, organizations must notify the Department of Commerce that they adhere to the Safe Harbor privacy principles developed by the Department of Commerce in coordination with the European Commission. The principles provide guidance for U.S. organizations on how to provide "adequate protection" for personal data from Europe as required by the European Union's Directive on Data Protection.

2. An organization's request to be put on the Safe Harbor list, and its appearance on this list pursuant to that request, constitute a representation that it adheres to a privacy policy that meets the Safe Harbor privacy principles. Organizations must also publicly declare and state in their privacy policies that they adhere to the Safe Harbor principles.

3. Adherence to the Safe Harbor principles and subscription to the list are entirely voluntary. An organization's absence from the list does not mean that it does not provide effective protection for personal data or that it does not qualify for the benefits of the Safe Harbor.

4. In order to keep this list current, a notification will be effective for a period of twelve months. Therefore, organizations need to notify the Department of Commerce every twelve months to reaffirm their continued adherence to the Safe Harbor principles.

5. Organizations should notify the Department of Commerce if their representation to the Department is no longer valid. Failure by an organization to so notify the Department could constitute a misrepresentation of its adherence to the Safe Harbor privacy principles and failure to do so may be actionable under the False Statements Act (18 U.S.C. § 1001).

6. An organization may withdraw from the list at any time by notifying the Department of Commerce. Withdrawal from the list terminates the organization's representation of adherence to the Safe Harbor principles, but this does not relieve the organization of its obligations with respect to personal information received prior to the termination.

7. If a relevant self-regulatory or government enforcement body finds an organization has engaged in a persistent failure to comply with the principles, then the organization is no longer entitled to the benefits of the Safe Harbor.

8. In order to sign up to the list, organizations may either send a letter signed by a corporate officer to the Department of Commerce or have a corporate officer register on the Department of Commerce's website (www.ita.doc.gov/ecom) that provides all information required in FAQ 6."

¹⁴⁶ "HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html; For more detail on the EU model contracts, see "Transferring Personal Data Overseas – the Contractual Solution :The European Commission has prepared a draft contract for use by businesses wanting to transfer personal data to countries outside the European Economic Area." October 2000 www.elexica.com.

¹⁴⁷ "HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html; For more detail on the EU model contracts, see "Transferring Personal Data Overseas – the Contractual Solution :The European Commission has prepared a draft contract for use by businesses wanting to transfer personal data to countries outside the European Economic Area." October 2000 www.elexica.com.

¹⁴⁸ "Transferring Personal Data Overseas – The contractual solution October 2000 (www.elexica.com) is the award-winning online legal resource produced by international law firm Simmons & Simmons.

<http://www.hipaadvisory.com/news/index.htm#yahoo0618>; see also <http://biz.yahoo.com/rf/010618/118144142.html>

¹⁴⁹ Comments of Ambassador David L. Aaron, Senior International Advisor, Dorsey & Whitney, testifying before the House Subcommittee on Commerce, trade and Consumer Protection "The EU Data protection directive: Implications for the U.S. Privacy Debate, 3/8/01 <http://www.house.gov/commerce/hearings/03082001-49/Aaron102.htm> ("One U.S. multinational company told me that if they took that route, they would have to negotiate over thousands such contracts.")

¹⁵⁰ "HP embraces U.S.-Europe 'Safe Harbor' privacy deal", by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html; A copy of the draft contract is available at www.europa.eu.int/comm/internal_market/en/media/dataprot/news/annexen.pdf; see also "EC Ok's Data Transfer Model Contract Despite U.S. Request to Delay Consideration" 4/2/01 World Securities Law Report E-mail Alert, Bureau of National Affairs, Inc. (The U.S. Government objected because it thought that the model contracts would inordinately expose U.S. firms to liability overseas).

¹⁵¹ http://europa.eu.int/eur-lex/en/dat/2001/l_181/l_18120010704en00190031.pdf (Standard contractual clauses for the transfer of personal data to countries outside of the European Union pursuant to the Directive).

¹⁵² "Transferring Personal Data Overseas – The contractual solution" October 2000 (www.elexica.com) is the legal resource produced by international law firm Simmons & Simmons. ("Also, there are difficulties in using this approach to deal with restrictions on cross-border transfers of data. Perhaps the most significant of these is the lack of any real incentive on the parties to comply. Even if the data subject has a contractual remedy, in many situations this will not be very helpful. A UK individual may have considerable practical obstacles to bringing an action for breach of contract against a U.S. company").

- ¹⁵³ Frequently Asked Questions (FAQs) FAQ 1 – Sensitive Information, www.export.gov/safeharbor/FAQ1sensitivedataFINAL.htm. These provisions in the FAQs are fairly broad and unfortunately there is not much interpretive guidance beyond the FAQ.
- ¹⁵⁴ Frequently Asked Questions (FAQs) FAQ 2 – Journalistic Exceptions, www.export.gov/safeharbor/FAQ2JournFINAL.htm.
- ¹⁵⁵ Frequently Asked Questions (FAQs) FAQ 3 – Secondary Liability, www.export.gov/safeharbor/FAQ3SecondaryFINAL.htm.
- ¹⁵⁶ www.export.gov/safeharbor "Safe Harbor Benefits."
- ¹⁵⁷ Baker & McKenzie European bulletin Vo 12 No. 3 p. 13.
- ¹⁵⁸ www.export.gov/safeharbor "Safe Harbor Benefits" (If you fall outside of the Safe Harbor then you risk having claims brought by European citizens against your company being brought in the EU which may be more hostile, whereas if you are within the Safe Harbor, then claims of the EU citizens (with very limited exceptions) must be brought in the U.S.); see also BNA World Internet Law Report 02/01 page 10 Vo. 2 issue 2.
- ¹⁵⁹ World Internet Law Report, March 2001, Vol. 2, Issue 3, BNA International page 5; see also "U.S. lawmakers criticize strong European privacy laws" Reuters www.siliconvalley.com/docs/news/tech/015586.htm; see also "Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01 www.newsbytes.com/news/01/162907.html (The EU has set July 1, 2001 as the deadline for EU companies to stop sharing data with companies in countries that do not have adequate privacy laws in place (i.e. in the U.S. who have not agreed to comply with the Safe Harbor); see also "Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01 www.newsbytes.com/news/01/162907.html (The turning off of data flows could lead to a trade war. Jonathan Winer, former U.S. assistant secretary of state for international enforcement.); see also "HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html (European authorities plan to review U.S. corporate compliance with the provisions this summer, and they possibly could begin enforcement actions against companies that haven't agreed to comply shortly thereafter.).
- ¹⁶⁰ Article by Gareth Morgan ZDNet News (UK), 3/16/01 www.zdnet.com/zdnn/stories/news/0,4586,2697328,00.html
- ¹⁶¹ "HP embraces U.S.-Europe 'Safe Harbor' privacy deal", by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html ("American companies have been sort of reluctant to be first out of the box for fear of being singled out for scrutiny by European authorities. Said Barbara Wellber, who was the principal negotiator of the agreement while she worked at the commerce department... The Safe Harbor agreement provides a manageable legal and ethical means to move data between the U.S. and Europe... If corporations are serious about following the self-regulation approach, rather than having to deal with privacy regulations then this is what they should be looking at"); see also "Microsoft to Sign EU Privacy Accord" Lori Enos 5/16/01 www.ecommercetimes.com/perl/story/9752.html see also article by Gareth Morgan ZDNet News (UK), 3/16/01 www.zdnet.com/zdnn/stories/news/0,4586,2697328,00.html
- ¹⁶² <http://www.ita.doc.gov/td/ecom/SafeharborOverviewAug00.htm>
- ¹⁶³ <http://www.ita.doc.gov/td/ecom/SafeharborOverviewAug00.htm>
- ¹⁶⁴ <http://www.ita.doc.gov/td/ecom/SafeharborOverviewAug00.htm>
- ¹⁶⁵ Safe Harbor is a Lonely Harbor by Declan McCullagh Wired News www.wired.com/news/politics/0,1283,41004,00.html?tw=wn20010105 ("only about a dozen firms so far have signed up to be certified by the Commerce Department and embarrassed department officials promise they'd try to gin up more interest.") "HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html ("Commerce Department officials have been trying to boost [the] number [of companies voluntarily certifying under the Safe Harbor] in order to bolster the legitimacy of the Safe Harbor deal."). See also U.S. Businesses Slow to Adopt EU Safe Harbor Agreement by Brian Krebs, Newsbytes www.newsbytes.com/news/01/160069.html.
- ¹⁶⁶ <http://www.newsbytes.com/news/01/167541.html> Intel Corp. [NASDAQ: INTC] has signed the European Union-U.S. "Safe Harbor" agreement Intel signed the agreement June 22.
- ¹⁶⁷ <http://www.newsbytes.com/news/01/167541.html> Intel Corp. [NASDAQ: INTC] has signed the European Union-U.S. "Safe Harbor" agreement Intel signed the agreement June 22. But see Intel Signs Up for EU 'Safe Harbor' Agreement, by Brian Krebs, Newsbytes.com, 7/2/01 "HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html; see also HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html.
- ¹⁶⁸ BNA World Internet Law Report 02/01 page 10 Vo. 2 issue 2.
- ¹⁶⁹ "EU-U.S. Clash over personal data: private right or commercial opportunity?" by Peronet Despeignes and Deborah Hargreaves, FT.com Financial Times, 3/29/01, <http://globalarchive.ft.com/globalarchive/articles.html?id=010329000406>.
- ¹⁷⁰ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.16; see e.g. Statement of the Transatlantic Consumer Protection Dialogue on U.S. Department of Commerce Draft International Safe Harbor Privacy Principles and FAQs, March 30, 2000, www.tacd.org/ecommercef.html#usdraft.
- ¹⁷¹ HP embraces U.S.-Europe 'Safe Harbor' privacy deal, by Patrick Thibodeau 2/16/01 Computerworld, http://computerworld.com/cwi/story/0,1199,NAV47_NLTpm_STO57787,00.html

¹⁷² See e.g. testimony before House Committee on Commerce www.house.gov/commerce/hearings/03082001-49/; see also "ASPs WARN: EU DATA PROTECTION LAWS FAIL TO KEEP PACE WITH TECHNOLOGY" Calls for EC to review urgently the outmoded data laws to protect individuals' rights and encourage business compliance" All About ASP Rome, 6 March 2001 <http://www.allaboutasp.org/pr-06mar01.cfm>

¹⁷³ www.house.gov/commerce/hearings/03082001-49/Winer103.htm (But see Rep. Edward J. Markey (D-Mass.) who disagreed, saying surveys indicate that Americans overwhelmingly favor strong privacy rules similar to Europe's. He accused Republicans and "a large corporate sector" of trying to block privacy measures that have been introduced here at both the federal and state levels. And Joel Reidenberg, a law professor at Fordham University in New York, said the EU's requirements could harmonize international privacy standards and provide "a benefit for American businesses" by giving them a single set of provisions to comply with instead of multiple rules. The EU's approach to privacy is also being followed by a growing number of other countries, Reidenberg said, adding that U.S. citizens are in danger of "becoming second-class in the privacy world at the global level); see also "Key U.S. lawmaker calls for review of Europe's privacy laws" BY PATRICK THIBODEAU (March 08, 2001) WASHINGTON, Computerworld

http://computerworld.com/cwi/story/0%2C1199%2CNAV47_STO58406_NLTpm%2C00.html;

¹⁷⁴ BNA World Internet Law Report 02/01 page 10 Vol. 2 issue 2.

¹⁷⁵ Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.15. see also European Parliament resolution on the draft commission Decision on the adequacy of the protection provided by the Safe Harbor Privacy Principles and related Frequently Asked questions issued by the U.S. Department of Commerce, www.epic.org/privacy/intl/EP_SH_resolution_0700.html; see also Article by Elizabeth de Bony, IDG News Service/Brussels Bureau July 27, 2000 ("Although the commission reached agreement with the us that system based on Safe Harbor principles did represent adequate levels of privacy, the European Parliament voted in July 2000 that the it did not give adequate protection. This created concern that the agreement might have to be renegotiated. The European Parliament opinion is however, non-binding so the Commission's agreement remains in effect."); see also ACCA Docket, the Journal of the American Corporate Counsel Association Vol 19 No. 5, "Regulation of Electronic Commerce in Europe: A Corporate Counsel Guide" by Simon G. Zinger p.49, 56.

¹⁷⁶ Safe Harbor is a Lonely Harbor by Declan McCullagh Wired News

www.wired.com/news/politics/0,1283,41004,00.html?tw=wn20010105.

¹⁷⁷ "Key U.S. lawmaker calls for review of Europe's privacy laws" BY PATRICK THIBODEAU (March 08, 2001) WASHINGTON, Computerworld

http://computerworld.com/cwi/story/0%2C1199%2CNAV47_STO58406_NLTpm%2C00.html

¹⁷⁸ Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01

www.newsbytes.com/news/01/162907.html

¹⁷⁹ "Industry Leaders Tackle Online Privacy Issue" By Rob Conlin, E-Commerce Times

www.ecommercetimes.com/perl/story/2897.html ("It is not clear that consumer privacy concerns are universal. As stated above, the EU has come from different circumstances which has driven certain conclusions about the level of privacy protection needed" (however, there has been no evidence of EU citizen sentiment on the issue of data privacy), but the U.S. has had a different experience. This may be why the data shows the following: In a survey of 4,500 web users regarding privacy issues, only 15% are unwilling to provide personal information to web marketers if that information improved their online experience. Over 50% said they would share personal information in exchange for better service. Also 73% said they find it helpful and convenient when a web site remembers basic information about them and 62% say they dislike web sites requesting personal information they have already provided. Finally 38 percent indicated that the website privacy policies were easy to understand (therefore not effective anyway)). See also "Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01 www.newsbytes.com/news/01/162907.html (A prime example is "In January, Consumers International, a UK-based group of 263 consumer organizations in more than 10 countries, released a report finding that many EU web sites do not comply with the directive. It said the most popular U.S. sites were more likely than EU sites to give users choices about joining company mailing lists or having information passed to third parties. Paraphrase quote of Jonathan Winer, former deputy U.S. assistant secretary of state for international enforcement; see also "Internet businesses 'breaking the law', see also www.itn.co.uk/news/20010403/business/02security.shtml (In a survey of 300 businesses, many were breaking provisions of the UK Data Protection Act and only 4% had received any legal advice on the issue."); see also "Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01 www.newsbytes.com/news/01/162907.html (Moreover, Many EU nations have not complied with the Directive, e.g. France, Germany, Ireland and Luxembourg.); but see "Germany implements the EU data protection directive" Baker & McKenzie Global E-Law Alert " 7/9/01.

¹⁸⁰ Paraphrase quote of Jonathan Winer, former deputy U.S. assistant secretary of state for international enforcement www.house.gov/commerce/hearings/03082001-49/Winer103.htm. See also "Lawmakers Cringe at prospect of Adopting EU Privacy Laws" by Brian Krebs, Newsbytes 3/8/01 www.newsbytes.com/news/01/162907.html

¹⁸¹ EU-U.S. Clash over personal data: private right or commercial opportunity?" by Peronet Despeignes and Deborah Hargreaves, FT.com Financial Times, 3/29/01 <http://globalarchive.ft.com/globalarchive/articles.html?id=010329000406>; see also "EU 'no' to data privacy delay" 5/6/01 Guy de Jonquieres FT.com Financial Times.

¹⁸² Privacy and Human Rights 2000 An International Survey of Privacy Laws and Developments, Banisar (EPIC and Privacy International 2000) p.15

¹⁸³ "U.S. Bailing Out of Safe Harbor Deal?" by Gareth Morgan ZDNet (UK), 3/16/01; by Gareth Morgan ZDNet (UK), 3/16/01
www.zdnet.com/zdnn/stories/news/0,4586,2697328,00.html
www.zdnet.com/zdnn/stories/news/0,4586,2697328,00.html.

¹⁸⁴ See Data protection Act 1998 Part I, <http://legislation.hmso.gov.uk/acts/acts1998/19980029.htm> and
<http://www.hmso.gov.uk/acts> and; <http://wood.cta.gov.uk/>; see also www.cta.gov.uk/dpr/dpdoc.nsf;
<http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>; www.cta.gov.uk/dpr/dpdoc.nsf;
<http://www.ogc.gov.uk/ogc/ogchelp.nsf/pages/redirect.html>.

¹⁸⁵ "Key U.S. lawmaker calls for review of Europe's privacy laws" BY PATRICK THIBODEAU (March 08, 2001)
WASHINGTON , Computerworld

http://computerworld.com/cwi/story/0%2C1199%2CNAV47_STO58406_NLTpm%2C00.html

¹⁸⁶ "Microsoft to Sign EU Privacy Accord" Lori Enos 5/16/01 www.ecommercetimes.com/perl/story/9752.html

¹⁸⁷ See e.g. "Earthlink boosts privacy efforts with new exec – The privacy officer bandwagon has taken on another passenger" by
Erich Luening 12/13/00 C/net News.com www.news.cnet.com/news/0-1005-200-4132109.html.

¹⁸⁸ www.pcworld.com/resource/printable/article/0,aid,16056,00,asp.

¹⁸⁹ "Industry Leaders Tackle Online Privacy Issue" By Rob Conlin, E-Commerce Times

www.ecommercetimes.com/perl/story/2897.html. However these are no panaceas, see e.g. "Privacy Organization Violates Own
Privacy Policy: Truste". Ecommerce Times www.ecommercetimes.com. See also www.privacycouncil.com; www.gbd.org/.

Katten Muchin Zavis

Health Information and HIPAA Compliance

FOR EMPLOYERS

In addition to health care providers and health care clearinghouses, the privacy regulations apply to health plans, including group health plans. Thus, employers that sponsor group health plans will be affected by the privacy regulations.

Background

The Department of Health and Human Services published final privacy regulations under the Health Insurance Portability and Accountability Act (HIPAA) on December 28, 2000. Group health plans must comply with the HIPAA privacy regulations by April 14, 2003. Even though that deadline is almost two years away, the complexity of the privacy regulations and the necessary involvement of third parties should persuade plans and their sponsoring employers to start acting immediately to ensure meeting the compliance deadline. This discussion is designed to give employers an overview of the issues they will need to address before the deadline arrives.

Protected Health Information

The privacy regulations are designed to prevent the inappropriate use or disclosure of protected health information (PHI). PHI includes any individually identifiable health information created or received by a group health plan or an employer that relates to a past, present or future physical or mental condition of an individual (or the provision of or payment for health care for that individual). PHI can be in electronic, written or oral form.

Participant Consent or Authorization

The privacy regulations place limitations on a group health plan's use or disclosure of PHI. However, a group health plan may, generally, disclose PHI without consent to the participant involved or to carry out payment or health care operations. For uses outside of payment or health care operations, authorization from the participant is required. In all but certain narrow circumstances, the use or disclosure of PHI must be limited to the minimum amount necessary to accomplish the intended purpose of the use or disclosure.

While a group health plan is not required to obtain a consent in order to use or disclose PHI for purposes of payment and health care operations, the plan may do so. A group health plan may condition

enrollment in the plan on an individual's provision of this consent.

Under the privacy regulations, an "authorization" must be for a specific purpose and of limited duration. An authorization is required for use or disclosure of PHI for any purpose not covered by an exception under the privacy regulations and any purpose not related to payment or health care operations. A group health plan may not condition enrollment in the plan on provision by an individual of any authorization.

Business Associates and the "Plan Sponsor Exception"

A group health plan may not disclose PHI to any business associate without a written contract providing assurances that the business associate will safeguard PHI. A "business associate" is defined as an entity or person who (1) arranges, performs or assists in the performance of a function of a group health plan involving the use or disclosure of PHI or any other function regulated by the privacy regulations; or (2) provides a service to the group health plan where the provision of the service involves PHI. Examples of potential business associates of a group health plan include entities providing claims processing or utilization review services for the plan, or entities performing actuarial, consulting or financial services for the plan which involve PHI.

The employer that sponsors a group health plan also qualifies as a business associate of the plan. However, a group health plan may avoid entering into a business associate contract with the sponsoring employer if it satisfies the requirements of the so-called "plan sponsor exception." That exception requires that the plan document be amended to include several specific provisions. The group health plan may disclose PHI to the employer only after receiving a certification from the employer that the plan document has been amended to include the required provisions.

- The HIPAA privacy regulations respond to greater demands for maintaining the personal privacy associated with an individual's confidential health information. The scope and complexity of the regulations require immediate attention by employers to ensure compliance with these privacy standards by 2003. Katten Muchin Zavis is prepared to help orchestrate or to assist in the implementation and integration of our clients' HIPAA compliance activities.

www.hipaalawyers.com

K

M

Z

Required Administrative Procedures

The privacy regulations require the institution of certain administrative procedures designed to ensure compliance with those regulations. First, the group health plan will need to designate a privacy official for implementing and overseeing the plan's privacy policy. Second, the group health plan must designate a contact person for receiving complaints concerning violations of its privacy policy. Finally, the group health plan must document its policies and procedures for complying with the privacy regulations.



Electronic Transaction Standards

Group health plans are also subject to final regulations issued pursuant to HIPAA that require the use of uniform code sets and formats for the electronic transmission of health care information for specified transactions (e.g., claims payment, eligibility). The purpose of this standardization is to reduce administrative burdens and to promote efficiency in processing health care claims.

Security

In addition to the privacy regulations, group health plans will also be subject to separate security standards under HIPAA. These standards are currently set forth in proposed regulations, and they cover administrative, physical and technical safeguards to ensure the security of PHI.

Workers' Compensation

Under HIPAA, workers' compensation and certain other forms of insurance (such as disability insurance) are "excepted benefits." Consequently, insurance carriers providing this type of coverage are not covered by the privacy regulations. These non-covered insurers typically seek PHI from group health plans to carry out their insurance functions. The privacy regulations permit the disclosure of PHI to a party responsible for payment of workers' compensation benefits or in accordance with state law.

Mergers and Acquisitions

The privacy regulations will likely impact the due diligence review of group health plans in the course of corporate transactions. A potential buyer will often review claims experience as part of its due diligence review. The privacy regulations permit the disclosure of PHI during due diligence review in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor is or will become subject to the privacy regulations.

On-Site Health Clinics

Some employers maintain on-site clinics and, thereby, maintain PHI as a secondary function of its business. In this case, the privacy regulations should apply to the clinic and any associated administrative services. An on-site clinic will be subject to the privacy requirements governing health care providers, rather than the privacy requirements governing group health plans.

Health Information and HIPAA Compliance Team for Employers

Jeffrey J. Bakker
Employee Benefits

Linda Lemel Hoseman
Employee Benefits

William E. Mattingly
Employee Benefits/HIPAA

Kathryn A. Roe
Health Care/HIPAA

Mark S. Weisberg
Employee Benefits

For more information, please contact:

William E. Mattingly
(312) 902-5266
william.mattingly@kmz.com

Practice Areas

KMZ has offices in Chicago, Los Angeles, New York and Washington, D.C. We offer 51 practice areas that have been carefully designed to complement, augment and protect our clients' businesses.

Advertising
Anti-Fraud Counseling and Litigation
Antitrust
Bankruptcy, Reorganization and Creditors' Rights
Business Litigation
Corporate
Corporate Insurance
Customs and International Trade
Employee Benefits and Executive Compensation
Entertainment
Entertainment Finance
Entertainment Litigation
Environmental
Finance and Structured Finance
Financial Institutions
Financial Markets and Products
Financial Services
Franchising, Licensing and Distribution
Governmental Affairs
Health Care
Health Care Compliance
Health Care Insolvency
Health Information and HIPAA Compliance
Intellectual Property
Intellectual Property Litigation
International Transactions and Litigation
Internet and E-Business
Investment Management
Joint Ventures, Strategic Alliances and Partnerships
Labor and Employment
Litigation and Dispute Resolution
Mergers and Acquisitions
Private Equity and Emerging Growth Companies
Product Liability
Public Finance
Publishing
Real Estate
Real Estate Development
Real Estate Finance
Real Estate Investment Fund Formation
Real Estate Litigation
Real Estate Taxation
Securities
Securities Litigation
Shopping Center and Retail Law
Sports Law and Sports Facilities
Tax Planning and Litigation
Taxation of Financial Products
Technology and New Media
Wealth Management and Planning
White Collar Criminal and Civil Litigation

Health Information and HIPAA Compliance

FOR EMPLOYERS

Frequently Asked Questions

PROTECTED HEALTH INFORMATION

Q When might an employer have access to protected health information?

A Examples of activities that could place protected health information in the employer's possession include:

- claims submission
- review of denied claims
- questions from a third party administrator regarding plan interpretation
- advocating a claim for an employee
- use of medical data for other welfare plans
- audit reports
- data analysis results
- employment-related matters
- wellness program
- disease management program
- workers' compensation
- on-site clinic

The complexity demonstrates the need for an employer to perform a gap analysis in order to assess what protected health information it receives from its group health plan and whether it should continue to receive such information.

CONSENTS AND AUTHORIZATIONS

Q When will a group health plan need to obtain consent to use or disclose protected health information?

A Although consent is not required for a group health plan to use or disclose protected health information for payment and health care operations, the plan may obtain an individual's consent – but only for those purposes. For example, if an employer sponsors more than one group health plan and those plans elect to obtain consent for purposes of payment and/or health care operations, those plans may obtain a joint consent (and must use a joint notice). A joint consent will allow the group health plans to share protected health information among the plans. A group health plan can condition enrollment on obtaining an individual's consent.

Q When might a group health plan want to get an authorization to use or disclose protected health information?

A group health plan must obtain an authorization to use or

A disclose protected health information for any purpose other than payment, health care operations or a purpose covered by an exception under the Final Privacy Rule. A group health plan may want to obtain an authorization permitting health care providers to disclose protected health information to the plan for payment of specific benefits. A group health plan can condition payment on receipt of this authorization, subject to satisfaction of certain requirements.

A group health plan will want an authorization permitting health care providers to disclose protected health information to the plan for plan operations. Group health plans *cannot* condition payment or enrollment on receipt of this authorization, but a health care provider *can* condition the provision of health care service that is solely for the purpose of creating protected health information (e.g., wellness care and disease management) for disclosure to the plan on receipt of this authorization.

Q When will an employer want to obtain an authorization to use or disclose protected health information?

A An employer will want to obtain an authorization any time the employer acts in a role other than that of a business associate. For example, if the employer wants to advocate a claim outcome under the control of the third party administrator or a health care provider, it must obtain an authorization.

RELATIONSHIP OF ERISA TO HIPAA

Q How does ERISA relate to HIPAA?

A ERISA does *not* preempt HIPAA. However, because HIPAA does not preempt state law that is more stringent than HIPAA or is otherwise saved under HIPAA, ERISA could be available to preempt state law. Because of the complexity of both HIPAA and ERISA, whether a state law is preempted by the application of those two federal laws will require considerable thought and a 50 state analysis.

BUSINESS ASSOCIATES

Q What are business associates to a group health plan?

A Like a business associate of other covered entities, a business associate of a group health plan refers to any entity or person who either (1) arranges, performs or assists in the performance of a function of a group health plan involving the use or disclosure of protected health information or any other function regulated by the Final Privacy Rule; or (2) provides a service to

(Continued on back)

K

M

Z

the group health plan where the provision of the service involves protected health information. Examples of business associates of a group health plan include third party administrators, pharmacy benefit managers and other similar vendors.

- Q** Is an employer a business associate of the group health plan sponsored by that employer?
- A** Yes, an employer may be a business associate of the group health plan that it sponsors.
- Q** What must a group health plan do in order to disclose protected health information to a business associate or to allow a business associate to receive protected health information on the plan's behalf?
- A** The group health plan must have a contract with the business associate that contains certain elements. Also, the group health plan must take reasonable steps to cure a contract breach when the plan knows of a pattern of activity or practice that constitutes a material breach of the contract.
- Q** Must a group health plan have a business associate contract with the employer sponsoring the plan?
- A** No, a group health plan is not required to have a business associate contract with the employer sponsoring the plan, provided that the plan satisfies the exception for plan sponsors or that the individual has authorized the employer's receipt of protected health information.
- Q** Should an employer disclose protected health information to the group health plan's business associates without each business associate having a business associate contract with the plan?
- A** No, an employer should not disclose protected health information to any business associate of the group health plan that does not have a business associate contract with the plan. By doing so, the employer could be held accountable for the business associate's use of the protected health information under ERISA and the Final Privacy Rule, as well as state law. Also, were an employer to do so, that would make compliance with the plan sponsor exception and the group health plan's notice more complicated since the permitted uses and disclosures must be described in the plan document and the notice. Further, the standard for enforcement for the group health plan would include knowledge of a contract breach as well as a fiduciary duty to monitor the employer and the business associate. For example, if an employer disclosed protected health information to a business associate of the group health plan that lacked a business associate contract, the plan would be required to monitor the business associate's use and disclosure of the protected health information. This would impose a higher standard on the group health plan than knowledge of the business associate's use and disclosure of protected health information.

ADMINISTRATIVE PROVISIONS UNDER THE FINAL PRIVACY RULE

- Q** Must a group health plan give a privacy notice?
- A** Yes, a group health plan must give a privacy notice, and there are specific requirements for its content. Of particular note is the requirement that the privacy notice include a statement that the group health plan may disclose protected health information to the plan sponsor (if applicable) and a statement of uses and disclosures permitted by the Final Privacy Rule and applicable state law.
- Q** How often must the privacy notice be given?
- A** Initially, the privacy notice must be given no later than April 14, 2003, to individuals covered by the group health plan. Thereafter, it must be given at the time of enrollment of new participants and within 60 days of a material revision to the notice. Once every 3 years, all participants must be notified of the availability of the notice and how to obtain a copy.
- Q** What are the personnel implications of the final privacy rule?
- A** The group health plan must designate a privacy officer.
- Q** What policies or procedures must a group health plan document?
- A** A group health plan must maintain policies and procedures to implement the Final Privacy Rule, and all such policies and procedures must be documented. Those policies and procedures may be designed to take into account the size and type of activities that relate to the use or disclosure of protected health information. Examples of what those policies and procedures would address might include:
- inspection, copying and amending records and receiving complaints
 - consent and authorization
 - notice
 - right of access
 - right to amend
 - right of accounting
 - privacy officer
 - documentation of actions

Health Information and HIPAA Compliance Team for Employers

Jeffrey J. Bakker
Employee Benefits

Linda Lemel Hoseman
Employee Benefits

William E. Mattingly
Employee Benefits/HIPAA

Kathryn A. Roe
Health Care/HIPAA

Mark S. Weisberg
Employee Benefits

For more information, please contact:

William E. Mattingly
(312) 902-5266
william.mattingly@kmz.com



A NEW COVENANT WITH
STAKEHOLDERS:
Managing Privacy as a
Competitive Advantage

PRIVACY RISK MANAGEMENT

© 2001 KPMG LLP, the U.S. member firm of KPMG International, a Swiss association. All rights reserved. 22650atl

“Privacy is not solely a risk issue. Nor is it only an operational issue. It has become a strategic business issue that is holistic. And one that needs to be applied enterprise-wide. If you do it right, its impact on customer trust can be enormous, and trust is ultimately the catalyst for trade.”¹

SECURITY TRANSFORMATION: DIGITAL DEFENSE STRATEGIES TO
PROTECT YOUR COMPANY’S REPUTATION AND MARKET SHARE

The following white paper was developed as part of a series by KPMG’s Assurance & Advisory Services Center.

© 2001 KPMG LLP, the U.S. member firm of KPMG International, a Swiss association. All rights reserved. 22650atl

TABLE OF CONTENTS

2	Introduction
5	The Current Environment: <i>Issues and Legislation Driving the Privacy Debate</i>
11	The Opportunity: <i>Creating Organizational Value Through Privacy Protection</i>
13	An Approach to Privacy Risk Management
20	Implications and Opportunities
21	Conclusion
22	Appendix I: <i>Understanding the Safe Harbor Provision of the European Union's Directive on Data Protection</i>
24	Appendix II: <i>An Interview With Karen Alnes, Wells Fargo</i>
26	Appendix III: <i>An Interview With KLM Royal Dutch Airlines</i>
28	Appendix IV: <i>An Interview With Chris Carney, Bon Secours Health System</i>
30	Appendix V: <i>An Interview With Kirk Herath, Nationwide</i>
32	Endnotes

I N T R O D U C T I O N



In the Information Age, privacy has become an asset—and like any significant asset, it will become more valuable as it becomes more scarce. As a result, the protection of privacy is becoming an important competitive differentiator for leading organizations worldwide, in industries from financial services to health care, to consumer and technology markets, to government—a variety of which have installed chief privacy officers in the past 18 months to lead their efforts.

Faced with consumer demands for heightened privacy protection, as well as rapidly evolving regulatory efforts in the United States and around the world, leading

Privacy can be good for business, and information-sharing can be good for consumers.

organizations are increasingly viewing privacy protection as a way to enhance stakeholder trust as well as avoid costs, mitigate risks, improve customer satisfaction, and, potentially, generate new revenues. These leaders understand that the privacy, security,

and accessibility of organizational information (electronic and otherwise) enable all transactions, not just e-transactions. The ability to assure customers of the privacy, security, and accessibility of their information is fundamental to engendering their trust—which is, in turn, fundamental to the building of any brand. Thus, organizations that approach privacy as a strategic issue—and their customers and their information as strategic assets—are rallying around the evolving idea that “Privacy can be good for business, and information-sharing can be good for consumers.”²

Understanding the Extent of the Issue—and Its Risks

Apart from the strategic gains they can realize from protecting their stakeholders’ privacy, organizations that fail to do so face a variety of substantial risks—including reputation and brand damage; litigation and enforcement actions; disruption of operations; and even failure to achieve their strategic goals. Many organizations,

N
A
N
E
W
C
O
V
E
N
A
N
T
W
I
T
H
S
T
A
K
E
H
O
L
D
E
R
S

© 2001 KPMG LLP, the U.S. member firm of KPMG International, a Swiss association. All rights reserved. 22650atl

unfortunately, tend to underestimate the importance of this issue, and many of them do not yet realize the genuine risks they face and to what extent they are vulnerable.

At the heart of the problem is the extraordinary amount of information organizations have today—information about their customers, vendors, alliance partners, and employees. Until something happens to put them at risk, many organizations do not know how much or what kind of information they have, who has access to it, to what extent its use may be regulated, or what penalties they may face for its mishandling. Or, they may believe that adherence to information security practices will also take care of privacy protection (when, in fact, the two are connected but pose separate challenges; see box below).

These false impressions can have serious consequences. Moreover, they inhibit organizations from viewing privacy protection as a new way to differentiate themselves among their competitors and to better meet customers' needs. “‘What so many businesses don't get,’ [says] Ann Cavoukian, the information and privacy commissioner of Ontario, Canada,... ‘is that you shouldn't [have] an adversarial relationship with privacy. Privacy is good for business.... If you're in the information business today, you've *got* to lead with privacy.’”³

Understanding Privacy, and How It Differs from Security

Privacy is defined as the protection of the collection, storage, processing, dissemination, and destruction of personal information. “Personal information is defined as any information relating to an identified or identifiable individual [or institution, in some cases]. Such information includes, but is not limited to, the customer's name, address, telephone number, social security/insurance or other government identification numbers, employer, credit card numbers, personal or family financial information, personal or family medical information, employment history, history of purchases or other transactions, credit records, and similar information. Sensitive information is defined as personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, sexual preferences, or information related to offenses or criminal convictions.”⁴

Security, on the other hand, focuses on ensuring that information is conveyed where it is intended, as it is intended. An information systems security architecture enables information and transactions to stay private. An organization can have security without privacy, but privacy is impossible without security.

This white paper describes the complex array of privacy issues organizations worldwide now face. It builds a case for approaching privacy protection as a strategic business opportunity—one that is integrated with the organization's overall strategy and, thus, has the support of the board and top leaders. It addresses the challenges organizations face in balancing their customers' right to privacy with their own clear interest in using customer information to identify marketing opportunities that could help them better meet their customers' needs and expectations. It describes how organizations can enhance the trust their stakeholders have in them by communicating their efforts to protect privacy and by demonstrating compliance with relevant legislation and regulations. Finally, this document addresses how organizations can seek to develop a competitive advantage—as well as a new covenant with their stakeholders—through the design and implementation of a comprehensive privacy risk management program.

“The world of security is huge. But the world of privacy is bigger. If I were to be able to have on your telephone a little device that traced every phone call you made, they would put me in jail. If I were to do that with a personal computer, you'd say, ‘You're doing effective customer profiling.’”⁵

MICHAEL D. CAPPELLAS, CHAIRMAN AND CEO
COMPAQ

THE CURRENT ENVIRONMENT: ISSUES AND LEGISLATION DRIVING THE PRIVACY DEBATE

N

ew technologies, the proliferation of information, anecdotes about privacy breaches, and globalization are among the forces fueling concern about privacy among both organizations and their stakeholders. Increasingly, individuals want to choose who does and does not have access to their medical, financial, purchasing, and other personal information. And, if access is needed, individuals would like to be able to specify for what purposes and to what extent access will be granted. They also want specific assurances that the information they consider private is, in fact, kept private by the organizations with which they do business.

Increasingly, individuals want to choose who does and does not have access to their information.

Figure 1: Privacy Risk Management Process



In approaching privacy protection as a business strategy, organizations need to identify privacy risks (which include personal data-flows) and then construct a process whereby they can measure, monitor, and control privacy management to meet organizational and stakeholder needs.

5 MANAGING PRIVACY AS A COMPETITIVE ADVANTAGE

When asked by Forrester Research, for example, “How much of a violation of your privacy is it for businesses to collect and then supply data about you to other companies?” 72 percent of consumers participating in the study responded “extremely/very.”⁶ What’s more, “94 percent of Internet users want privacy violators to be disciplined. If an Internet company violated its stated privacy policy and used personal information in ways that it said it [would not], 11 percent of Internet users say the company’s owners should be sent to prison; 27 percent say the owners should be fined; 26 percent say the site should be shut down; and 30 percent say the site should be placed on a list of fraudulent Web sites.”⁷

Consumers are particularly concerned about the privacy of online transactions, especially about whether they can trust organizations to safeguard their credit card data and other key information. Although trust is not the only reason people buy from a company, without it, they will go elsewhere: while 35 million Americans spent about \$45 billion online in 2000, researchers have estimated that U.S. companies lost out on at least another \$12.4 billion because consumers were reluctant to share their personal information over the Internet.⁸

Opt In or Out?

Unlike privacy laws in the European Union, those in the United States have historically balanced consumer privacy against the benefits of information sharing; however, both U.S. and E.U. laws require mechanisms that enable individuals to stop the use of their information. How much individuals control the content of transactions and how much organizations themselves do has become the question for U.S. organizations, and, increasingly, U.S. lawmakers. The key debate is whether consumers should be given the option to “opt in” or “opt out” of having their information shared with, or sold to, third parties. (Online, they opt in or out simply by choosing whether to buy and otherwise share information.) Most of the online industry would prefer to tell Web site visitors that “personal information might be retained for internal purposes or even distributed to third parties”⁹ unless they exercise their right to opt out and thus prevent the information from being used for marketing purposes or by third parties. On the other hand, most consumer groups want Web sites to request that consumers explicitly “opt in” before they be allowed to retain or distribute information on a visitor.

At a Glance: Six Key Pieces of Privacy Legislation

As of mid-2001—in just the first six months of the 107th U.S. Congress—at least 100 privacy-related or privacy-referenced bills or amendments have been introduced and in some cases voted upon by either the Senate, the House, or both.¹⁰ Other regulations are being debated at the federal level and within the states, where organizations face additional requirements, and citizens support these efforts. A recent survey of U.S. voters by the Public Opinion Strategies firm indicates that strengthening privacy laws to assure that computerized medical, financial, or personal records are kept private is the highest-rated issue of concern to voters nationwide.¹¹ At least 73 of the Fortune 100 must already adhere to at least one of four sets of privacy regulations that recently became law¹² (described in the first four boxes below).

Gramm-Leach-Bliley Act (GLBA)
GLBA's main purpose was to eliminate many restrictions on affiliations among banks, insurance companies, and securities firms; it also provides standard rules to guide financial institutions on how they handle information pertaining to individuals. GLBA's Title V requires federal agencies to establish appropriate standards for financial institutions to protect certain non-public information. Customers and consumers must be provided with an annual privacy notice of their ability to opt out of non-exempt sharing of covered personal information with third parties. Those regulations went into effect in November 2000 with mandatory compliance scheduled for July 1, 2001.
The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
<p>HIPAA was driven by the need to enable a mobile society to contain medical costs, insure more Americans, and enhance the quality of health care. It also required Congress to establish an electronic privacy standard for medical information within three years or the Department of Health & Human Services (HHS) would do so. When Congress missed its deadline, HHS issued a proposed rule in November 1999. A final rule was issued in December 2000 and the regulations went into effect April 14, 2001, but these may be modified through guidelines at a later date. The HIPAA privacy compliance deadline is April 2003 (2004 for smaller health plans).</p> <p>The standards protect individually identifiable medical information, including demographic information, payment records, and other identifiable data. Protections apply to oral, written, audio-visual, and electronic information. Hospitals, medical centers, health plans, clearinghouses, and pharmacies are all affected. Indeed, "many of the nation's top hospitals have already begun to overhaul their IT infrastructures, training programs and filing systems in an effort to comply..."¹³ The U.S. Department of Health and Human Services estimates implementation of the final rule on privacy standards will cost \$17.6 billion¹⁴ over 10 years.</p>

MANAGING PRIVACY AS A COMPETITIVE ADVANTAGE

Safe Harbor Accord for the European Commission's Directive on Data Protection

The accord is designed to bridge different privacy approaches between the European Union and the United States and provide a streamlined means for U.S. organizations to comply with the 1995 European Union Directive (see Appendix I), which "requires that transfers of personal data take place only to non-E.U. countries that provide an 'adequate' level of privacy protection."¹⁵ Having negotiated the safe harbor with the U.S. Department of Commerce, the European Union approved it in July 2000, although its parameters continue to evolve. In the United States, private sector adoption of the agreement was slow to start, and some organizations continue to favor renewed negotiation with the European Union. Currently, the agreement does not cover financial services organizations.

The Children's Online Privacy Protection Act of 1998 (COPPA)

COPPA is designed to protect the privacy of children using the Internet. The Federal Trade Commission rule means that as of April 21, 2000, commercial Web sites or online services that are targeted to children need to obtain parental consent before collecting, using, or disclosing personal information from minors under age 13.

Privacy Act of 1974

Effective September 27, 1975, the Privacy Act is an omnibus code of fair information practices, which attempts to regulate the collection, maintenance, use, and dissemination of personal information by federal government agencies.

The Code of Fair Information Practices (1973)

Produced in 1973 by the U.S. Department of Health, Education & Welfare's Advisory Committee on Automated Data Systems, the Code contains five universal principles that pertain to organizations' use of information systems:

- ▶ Organizations may not maintain personal data record-keeping systems whose very existence is secret.
- ▶ An individual must be able to find out what personal information is in a record and how it is used.
- ▶ An individual must be able to prevent personal information that was obtained for one purpose from being used or made available for other purposes without their consent.
- ▶ An individual must be able to correct or amend a record of personally identifiable information.
- ▶ Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

The effects of these complex U.S. laws extend well beyond industry lines. A large manufacturer must comply with financial privacy laws when, for example, it issues credit cards in addition to selling heavy equipment. A large retailer is affected by medical privacy regulations because it has pharmacies in its stores. Another company that issues a private-label credit card is affected both by financial and health care laws if consumers use the card in pharmacies. In addition, Australia and countries in Europe, Asia, and others in the Americas also face complex, conflicting regulations and customs, some provisions of which affect multinational organizations. (See chart on page 10.)

The mishandling of private information can lead to expensive problems as well as damaging publicity. Indeed, “The cost of a privacy PR blowout can range from tens of thousands to millions of dollars based on the company’s size and the visibility of its brand, and this [impact] doesn’t include lost business and damage to the brand.”¹⁶ Recently, for example:

- ▶ A large U.S. bank paid millions to settle a complaint that it sold customer data, including account numbers and balances, Social Security numbers, and home phone numbers, to telemarketers.¹⁷
- ▶ An online ad agency was hit with charges that it would violate consumer privacy if it merged anonymous user names with data from a company it acquired. When the Federal Trade Commission launched a probe, the agency’s share price “tumbled more than 20 percent in a week.”¹⁸
- ▶ Employees of a major department of the U.S. government are accusing their employer of “breaching their privacy by giving fellow workers and some patients access to their Social Security numbers and dates of birth. The class action suit on behalf of the [department’s] 180,000 employees seeks \$1,000 for each one, the minimum amount under the 1974 Privacy Act.”¹⁹

To prevent such problems from occurring—and, more important, to benefit strategically from a privacy protection focus—leaders should consider how to adapt their business models to recognize investment in privacy protection as an asset rather than as a cost-of-business reaction to regulatory actions. The next section discusses the opportunity organizations now have to pursue privacy protection as a strategic business opportunity—one that can enable them to enhance customer retention and build customer trust.

Privacy Protection Gains Importance Worldwide

Canada: The federal Personal Information Protection and Electronic Documents Act, which went into effect January 1, 2001, prohibits organizations from collecting, using, or disclosing any individual's personal information without the consent of that individual. It applies to the shipping, railway, airline, banking, telecommunications, and broadcasting businesses and will impose major restrictions on the ability of organizations to deal with personal data.²⁰

European Union: Established in 1995, the European Community's Data Protection Directive "created a necessary framework for use of personal data while ensuring the protection of the fundamental rights of the individual to privacy." The Directive required all member states to enact legislation implementing the Directive by October 25, 1998, which most of them have done. The Directive sets out eight data protection principles that, with few exceptions, prohibit transfer of personal data to a country outside of the European Economic Area unless that country ensures an adequate level of protection of that data. The Safe Harbor Accord between the European Union and the United States, which took effect November 1, 2000, evolved in response.²¹

Australia: Passed by the federal parliament in December 2000, the Privacy Amendment (Private Sector) Act 2000 amends the Privacy Act 1988, which had mainly covered public-sector agencies. The Act sets out how private-sector organizations should collect, use, keep secure, and disclose personal information. The Act is based on ten National Privacy Principles, which give individuals a right to know what information organizations hold about them as well as a right to correct inaccurate information. The Act includes special provisions for sensitive and health information, as well as direct marketing. For many organizations, including health services, the new principles will commence on December 21, 2001.²²

Argentina: "The Argentine congress has adopted the stiffest data protection law in Latin America. It is modeled on the German version of the European Union's data protection directive...[which, although rigorous, is less so than] the Italian version, which [requires] strict consumer consent before any direct marketing activities are allowed."²³

*"Privacy isn't a technology issue; it's a social issue. And I believe that companies really want to help consumers protect information—not just because it's the right thing to do, but because it's also good business. If a company doesn't earn the respect of its customers by respecting their privacy, those customers won't come back."*²⁴

HARRIET PEARSON, CHIEF PRIVACY OFFICER
IBM CORPORATION

THE OPPORTUNITY: CREATING ORGANIZATIONAL VALUE
THROUGH PRIVACY PROTECTION



As the privacy revolution continues to evolve, an organization needs to assess the risks it faces across its entire operation—remembering that paper-based privacy problems may be just as prevalent as electronically based challenges. Leaders should ask, for example, “Am I honoring my commitments to my customers? Am I serving them in the ways they want to be served? What regulations will change my industry, and how can I prepare for their implementation?” A privacy risk management program—one that makes security a priority—can help organizations address these issues and ultimately help them create a new covenant of trust with their stakeholders.

Focusing first on security issues can ultimately help organizations create a new covenant of trust with their stakeholders.

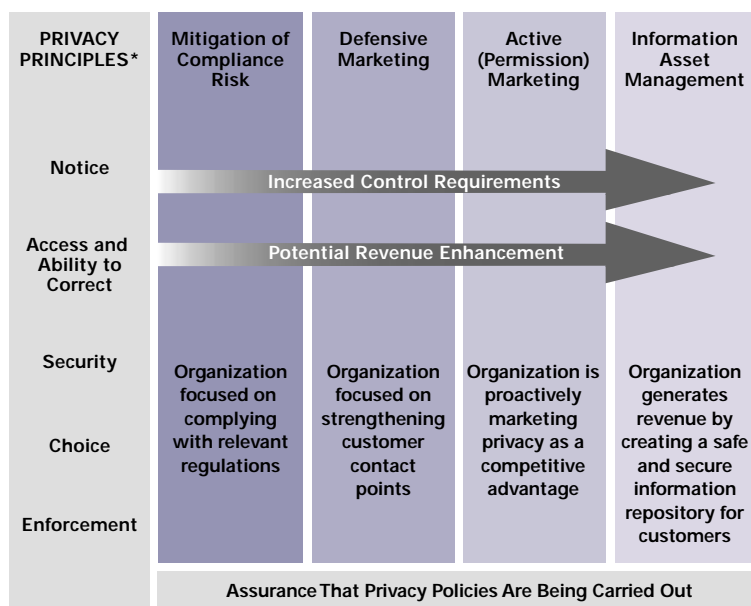
Such a program offers a number of key benefits:

- ▶ **Risk Mitigation:** In addition to protecting against the risks associated with privacy breaches, a privacy risk management program can help organizations reduce and prevent the substantial opportunity costs related to customers’ concerns about the organization’s trustworthiness and their perceptions of the value of its brand.
- ▶ **Asset Protection:** Organizations maintain so much information today that many of them are often unaware of what they have, where it is, or why they have it. A privacy risk management program can help organizations identify information assets and underscore the need for checks and balances so that the organization can address such issues.
- ▶ **Process and Cost Efficiency:** To protect customers’ privacy, organizations must manage information often in huge quantities and potentially warehoused in disparate databases in different business units. Analysis of associated personal data-flows can uncover duplicate or no-longer-relevant data, enabling organizations to update their mailing lists and better target their marketing efforts. In such cases, money spent to protect privacy can be offset with cost savings realized through efficiencies.

- Marketplace Differentiation:** Organizations have a rare chance now to build their perceived value with customers by communicating privacy policies to create a covenant of trust. And they can continue to build that trust by adhering to their privacy policies and communicating this compliance to their customers.

To be able to realize the benefits of privacy protection, leaders need to consider how to move from simply mitigating risks to strategically managing information assets—a transformation that has at its heart a renewed focus on the customer (see *Figure 2* below). The next section describes how organizations can approach this challenge and thereby develop an enterprisewide approach to privacy risk management.

Figure 2: Privacy Benefits: Continuum of Privacy Objectives



Organizations' privacy efforts can be depicted along a continuum. Some entities are focused on basic compliance with pertinent regulations as a means of controlling their privacy risks. Others deploy defensive marketing strategies to strengthen customer contacts, while still others actively market privacy to achieve a competitive advantage. Those that are managing their information assets most effectively are beginning to generate revenues by creating safe and secure information repositories for customers. Although such efforts often require considerable investment of financial and human resources, organizations that make these investments ultimately reap the benefits of being better able to identify, meet, and even exceed their customers' needs and expectations.

*Notice, Access, Choice, and Enforcement are explained on pages 22–23. These basic principles, along with efforts to ensure Security, are central to privacy protection.

A NEW COVENANT WITH STAKEHOLDERS

A N A P P R O A C H T O P R I V A C Y R I S K M A N A G E M E N T



An effective approach to privacy risk management begins with recognizing that it is not solely a technology-based or an e-business issue. Rather, it is a strategic issue that encompasses the protection of a variety of assets, many of which are not electronically based. (Indeed, although globalization and the Internet have increased the quantity of data and the speed and complexity of its flow, privacy issues affect paper records as well.) Records of customer preferences are, in fact, part of a covenant between a person and an organization, delineating how that entity will collect and use information about that person—and how it will safeguard his or her privacy.

Privacy issues affect paper records as well as electronic ones.

An effective privacy risk management program provides a mechanism for an organization to manage privacy risks in a manner consistent with its business needs, regulatory requirements, and marketplace expectations. Such a program:

- Discloses privacy principles;
- Addresses the collection, use, and retention of customer information;
- Ensures the accuracy, confidentiality, and security of the information maintained;
- Identifies how customer privacy is maintained in business relationships with affiliated and non-affiliated third parties (such as vendors and alliance partners);
- Periodically tests for compliance with organization policies and compliance requirements; and
- Monitors and evaluates the business implications of possible changes in laws and attitudes toward privacy.

Once Posted, A Privacy Policy Becomes Words to Live By

Once they have a management program and a privacy policy in place, organizations also need to recognize that posting such a policy and then failing to live up to it may create a legal liability. In a recent example, one online toy retailer, after consenting to an involuntary bankruptcy, "sought to auction personally identifying data it obtained from online customers. [It] had accumulated a database of some 250,000 consumers, but all under a privacy policy that explicitly promised it would 'never' disclose the information."²⁵ The Federal Trade Commission and nearly 48 attorneys general from various U.S. states and territories sought to prevent the sale, arguing that it constituted an unfair trade practice. The retailer ultimately reached a settlement that strictly controlled the terms of the proposed sale. "But by then the controversy had scared away buyers, and the court refused to approve the settlement without an actual sale. The case's conclusion does not bode well for future dot.com bankruptcies. For one thing, it casts doubts on the value of customer data—formerly considered a primary asset of dot.coms. At a minimum it will likely discourage future dot.coms from pursuing bankruptcy as an option."²⁶ Clearly, once developed and posted, a privacy policy must become part of the organizational culture.

Putting policies in place is a good first step, but it cannot be the only step. Organizations need to know where consumer and other information comes from, where it is circulated, where it goes, and how it is used. They need to know what they need; they need to avoid collecting information they do not need; and they need to make sure vendors, and other third parties, follow the same rules. Moreover, leaders need to recognize and communicate that such efforts must be ongoing.

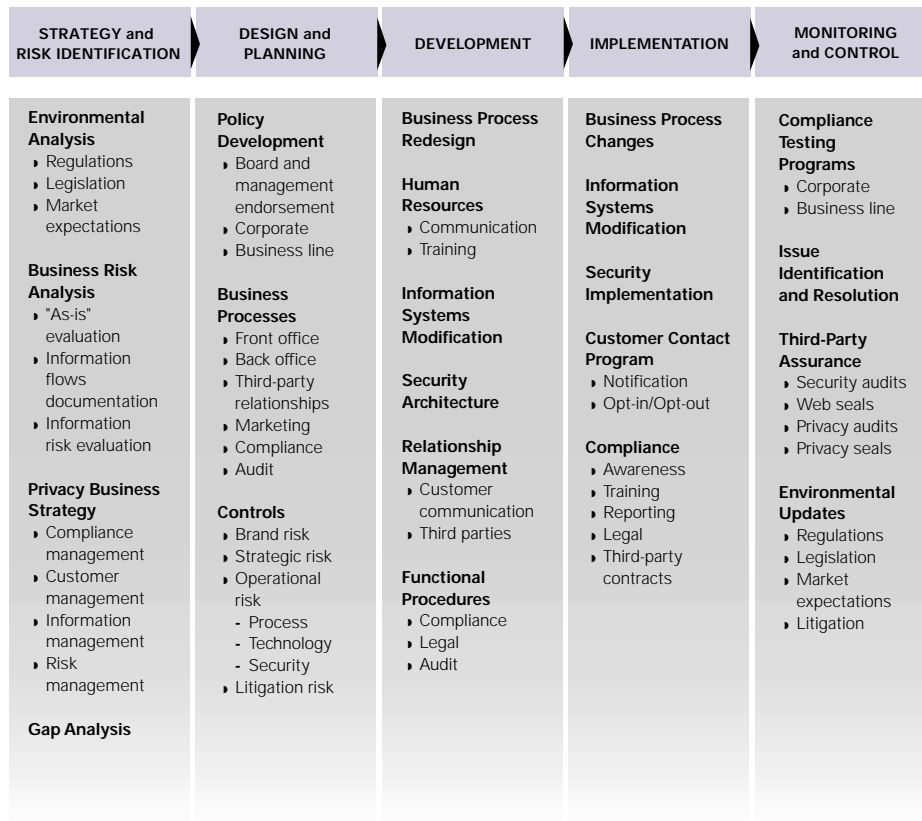
To accomplish these goals, organizations should begin to manage privacy holistically, with an individual (a chief privacy officer) or a team held accountable for the process. The appointment of a CPO "...is by no means just a Silicon Valley fad; rather it represents a certain maturing of businesses' approach to privacy. ...American Express, AT&T, and Microsoft already have them. So do companies as varied as Delta Air Lines, Mutual of Omaha, the Royal Bank of Canada, and Equifax."²⁷ Indeed, there are between 200 and 300 CPOs in the United States, according to Alan F. Westin, head of the Association of Corporate Privacy Officers, who believes that number may jump into the thousands in the next few years.²⁸

No one individual, however, can take sole responsibility for designing, developing, and implementing the effort. A program of privacy risk management requires the collective expertise of a variety of departments and specialists, including professionals with knowledge, insight, and

experience with information risk management and business process analysis and redesign as well as with privacy regulations, legislation, litigation, and the organization's own industry-specific needs. To varying degrees the team should also include business line managers, IT managers, and members of the organization's legal, marketing, and internal audit departments.

This overall process of privacy risk management may be depicted as a "life cycle," encompassing five phases. Those phases are shown in *Figure 3* and are delineated on the pages that follow.

Figure 3: Privacy Risk Management Life Cycle



MANAGING PRIVACY AS A COMPETITIVE ADVANTAGE

1. Strategy and Risk Identification

Managing privacy as a business strategy helps a company identify and mitigate its risks and leverage the substantial opportunities that such an effort may uncover. To start, a company needs to understand its environment fully, including the regulations and potential legislation that affect all of its markets as well as its customers' privacy needs. The analysis should encompass external

Critical Questions for Leaders

1. How can we best identify what information we have, who has access to it, to what extent its use is regulated, or what penalties we may face for its mishandling?
2. Who are our stakeholders, and what are their needs and expectations related to our protection of their privacy?
3. How do our customers perceive that their personal information will be used—and not used?

customers and their consumers as well as internal “customers,” including vendors, employees, and other stakeholders.

The organization then conducts a “business risk assessment,” identifying and documenting all the data flows within the organization—in all forms of media, electronic and otherwise. It needs to determine where the information originates, where it flows, how it is stored, and how it is disseminated. This process usually uncovers the most obvious areas of exposure and begins to reveal more subtle

risk and compliance issues. With this assessment of the “as is” state, the organization can develop a better informed, high-level privacy strategy, which encompasses its specific goals for management of compliance, customers, information, and risk.

Setting a reliable strategy requires that the organization determine how it can better comply with regulatory requirements and identify how best to manage information and its related risks. To meet these objectives, organizations can perform a gap analysis—comparing the “as is” state to the desired “to be” state set out in the privacy strategy—and then assess the risks and opportunities that arise. A gap analysis of the HR process, for example, would determine whether the company’s training program encompasses current privacy regulations and the company’s compliance policies.

2. Design and Planning

Once risks are identified and a strategy is set, leaders can focus on developing a privacy policy (and supporting procedures) that is both appropriate and workable for the organization and that

supports its strategy. Beyond the privacy policy, leaders should also create a plan that addresses privacy risk issues—and communication of those issues—at all levels of an organization, including front- and back-office operations, marketing, audit, HR, compliance, and third-party relationships. To do so, leaders should analyze the effects of the gaps identified in key processes and design the appropriate controls for the organization to mitigate associated risks. Controls are needed, for example, to ensure that access to certain information is limited to the people who have a defined need to know.

The organization can use the privacy business strategy and the privacy policy to determine how current processes can be improved. An effective privacy policy reduces the risk of litigation and regulatory noncompliance, and, at the same time, builds trust and loyalty among customers and other stakeholders.

Critical Questions for Leaders

1. How would we be affected—externally and internally—if a portion of private data became public?
2. How can we ensure, internally, that our customers' privacy preferences will be honored?
3. To what extent can a focus on privacy help us, for example, eliminate duplicate data or otherwise contain costs?

3. Development

During the development phase, the organization puts in place mechanisms for addressing the issues identified during design and planning. It establishes practices and controls to maximize compliance with the privacy policy, such as developing internal training programs in which employees learn about the importance of privacy and how to protect private information. Entities

Critical Questions for Leaders

1. What specific mechanisms must we establish to enable us to comply with our privacy policy?
2. What changes should we make in support systems, training, or business processes to help reinforce our privacy efforts?
3. Does our technical architecture ensure the privacy of our data as well as its security?

may also find that changes can, or should, be made to existing business processes and supporting systems. Some of these changes can generate tremendous additional value, for example, by integrating disparate customer databases residing in different divisions of the organization.

During this phase the organization should also review its technical architecture so that, for example, it can ensure that firewalls as well as authorization and encryption methodologies and mechanisms are

in place to limit data access to only the employees who need it to perform a specific business function. By communicating these efforts internally and externally, the organization can remind and assure its stakeholders of its commitment to privacy protection. Such efforts can inspire new confidence in external stakeholders, who, secure in the knowledge that their privacy is respected, may be more likely to choose the organization over its competitors.

Critical Questions for Leaders

1. Who will manage our implementation efforts day-to-day, and how will we communicate the importance of these efforts?
2. How should we inform our stakeholders of our efforts to ensure their privacy?
3. What are the regulations to which we are subject, and how do we ensure that we are in compliance?

4. Implementation

This phase entails implementing the changes in business processes, information systems, and security measures that the entity has designed, planned, and developed. Once leaders make these changes, they may also want to initiate a “customer contact” program to raise stakeholder awareness—and appreciation—of how the organization is addressing privacy issues and of changes they should expect in how it operates. In addition, the

organization should review and revise its management reporting, legal, and third-party contract practices to align them with its new privacy initiatives and guidelines.

5. Monitoring and Control

Monitoring and control of privacy-risk-related processes and initiatives begin during the implementation phase and remain ongoing. Although these measurement efforts are particularly important for organizations in regulated industries, which undergo heavy scrutiny of privacy-related processes and procedures, monitoring and control are essential for any organization that invests in a privacy risk management program and expects to derive meaningful results from it. Issues arising during implementation are addressed and resolved during this phase. The organization must take into account how its privacy policy and processes are affected by changes in the business environment, including regulatory and legislative developments, market expectations, and litigation.

To ensure that policy and processes are in place and working properly, organizations should consider conducting separate security and privacy audits. Internally, a privacy audit can provide

a useful self-assessment of organizational compliance with laws and regulations. Externally, a privacy audit can help demonstrate commitment to privacy management as well as compliance with regulations and internal policies. It encompasses both on- and off-line privacy management, including business processes, implementation of policies, and employee training. Data flows are examined to see if “gaps” in privacy have been effectively closed, and if new gaps have opened. When an organization communicates the results appropriately, a privacy audit can help build the covenant of trust with customers by providing a regular means of testing the enabling system and of verifying organizational compliance with its own privacy policies.

Critical Questions for Leaders

1. What performance measures should we initiate to monitor and manage our privacy efforts?
2. How could we benefit from a privacy and/or security audit?
3. Would a Web seal provide our stakeholders with an extra measure of assurance?

Some organizations use third-party professional services firms to perform these audits, which enable them to reassure their stakeholders of their strict compliance with privacy standards. The organization may also seek the additional benefit that derives from obtaining third-party assurance—such as a Web seal—to demonstrate that it fulfills defined criteria in various areas of business, information security, information privacy practices, and transaction integrity.

This five-phase approach can help enable organizations to manage privacy as a strategic issue subject to ongoing changes in technology and regulation. It can help them consider privacy from a holistic perspective, starting with a clear understanding of their own environment and the unique issues and opportunities created by the markets in which they participate. Finally, it can help organizations brand themselves as privacy-focused, possibly through third-party verification, and thereby begin to differentiate themselves as market leaders.

IMPLICATIONS AND OPPORTUNITIES



At the heart of privacy legislation, regulations, and guidance is the challenge of balancing a customer's right to privacy with the organization's clear interest in using customer information to identify potential business opportunities, both inside and outside an organization. When organizations have their customers' trust, they benefit from those customers' increasing willingness to

Leaders cannot determine how to treat customer information without knowing customer needs.

share increasingly specific information about their preferences as well as their satisfaction levels. Such information can enable organizations to understand, meet, and, eventually, anticipate customer needs and desires more effectively.

Thus, to design and implement an effective privacy management program, organizations must first invest in understanding what their customers want and expect. Leaders cannot determine how to treat customer information without knowing their customers' needs. In the short term, however, most organizations will focus on compliance with privacy regulations. During those efforts they need to remember that long-term market differentiation will ultimately evolve from a concerted effort to brand the organization as privacy-conscious in keeping with identified customer expectations. Moreover, leaders must acknowledge that waiting to address the issue until after a privacy breach has occurred will almost certainly be an expensive approach with potentially serious consequences for the organization's reputation and bottom line.

A NEW COVENANT WITH STAKEHOLDERS

C O N C L U S I O N

P

rivacy risk management affords organizations a rare opportunity to build their perceived value with customers and other stakeholders by communicating their privacy policies in such a way as to create a covenant of trust. This covenant is a transparent, mutual understanding of who owns the information, who controls it, and how it will be used. It can be a genuine competitive advantage, but it

requires organizations to look beyond the demands and requirements of evolving regulations.

Thus, while compliance with legislation and regulations may compel companies to revisit their privacy practices, if that is all they do, they will not be doing enough. In fact, they will

likely be overlooking the full extent of the risks they could confront. They may be collecting and archiving much more information than they

will ever use—and spending more money than they should. Moreover, they may be neglecting an opportunity to use their privacy practices as a tool for building customer relationships and, ultimately, brand value in the global marketplace. A privacy risk management endeavor can help organizations address these challenges, and, in the bargain, help them create an important new covenant with stakeholders.

Companies may be neglecting an opportunity to build customer relationships and, ultimately, brand value.



M A N A G I N G P R I V A C Y A S A C O M P E T I T I V E A D V A N T A G E

APPENDIX I: UNDERSTANDING THE
SAFE HARBOR PROVISION OF THE
EUROPEAN UNION'S DIRECTIVE ON DATA PROTECTION

By prohibiting the transfer of personal data to nations that do not meet European standards for privacy protection, the European Commission's Directive on Data Protection (ECDDP), adopted in 1995 and supposed to be implemented by October 25, 1998, threatened to impede the flow of information between E.U. and U.S. organizations, which the European Union believes do not provide an "adequate" level of privacy protection.

To help U.S. companies to avoid interruptions in their E.U. business dealings—or, worse, prosecution under European privacy laws—the U.S. Department of Commerce, in consultation with the European Commission, has developed a "safe harbor" system that will "allow continuing data flows between the U.S. and the E.U. and ensure privacy protection for E.U. citizens' personal information."²⁹ Although the lack of formal implementation of the Safe Harbor provisions by U.S. companies is under some scrutiny by the European Union, the principles that form the foundation of the Safe Harbor will continue to be a significant factor in the privacy debate.

Approved by the European Commission in July 2000, the Safe Harbor principles essentially enable U.S. companies to do business in the European Union³⁰ by establishing what is deemed to be an "adequate" level of privacy protection. These provisions continue to evolve. For example, because of recent changes in U.S. financial privacy laws under the Gramm-Leach-Bliley Act (GLBA), the European Union and United States did not include the financial services sector in the Safe Harbor accord.³¹ Now that GLBA is being implemented, both sides are now revisiting issues related to financial privacy. Until they reach a compromise, financial institutions are not covered by the Safe Harbor.

U.S. organizations can comply with the Safe Harbor by (1) joining a self-regulatory privacy program that adheres to the Safe Harbor principles; (2) developing their own self-regulatory approach (consistent with the principles); or (3) being subject to a body of law that protects privacy. However, U.S. firms can also comply with the Directive in other ways (than the Safe Harbor). Alternative ways to comply include: (1) consent of each individual whose data is transferred; (2) exemptions; (3) inter-firm agreements (via the so-called Standard Clauses); or (4) adhering to the Safe Harbor principles without actually registering under the Safe Harbor. Each approach has benefits and risks:

"U.S. companies that fail to enter the Safe Harbor face the possibility that E.U. companies will, as required under E.U. law, halt transfers of personal information to the United States. In addition, E.U. subsidiaries of U.S. companies that fail to enter the Safe Harbor, or take other steps to comply with the Directive, could be prosecuted by European authorities for transferring data to parent companies that do not have adequate protections. At the same time, U.S. companies that fail to live up to their obligations after entering the Safe Harbor face enforcement actions by the Federal Trade Commission (FTC), state Attorneys General, and in some states, private rights of action for deceptive trade practices."³²

Depending on how the Safe Harbor agreement continues to evolve, organizations that want to do business with E.U. countries will need to establish and demonstrate compliance with privacy policies in keeping with the Safe Harbor principles—whether they choose formally to enter the Safe Harbor, join a Department of Commerce–approved self-regulatory program (seal program), or develop their own program that meets Safe Harbor standards. "Regardless of which method a company chooses, to receive the protective benefit the Safe Harbor confers (presumption of adequate protections) it must self-certify annually to the Department of Commerce that it is adhering to the Principles by applying them to all data transferred after entering the Safe Harbor."³³

The Safe Harbor encompasses basic privacy principles:

- ▶ **Notice:** Organizations must provide individuals with clear notice of “the purposes for which it collects and uses information about them, the types of third parties to which it discloses the information, and how to contact the company with inquiries or complaints.”³⁴
- ▶ **Choice:** Before any data is collected, an organization must give its customers the opportunity to opt out of any disclosure of their information to third parties or of a use of that information that is incompatible with the purpose for which it was originally collected. Also before any data is collected, organizations must allow their customers to choose whether to opt in to the sharing of their sensitive information (e.g., data related to such factors as health, race, or religion).
- ▶ **Onward Transfer:** Unless they have the individual’s permission to do otherwise, organizations may share information only with those third parties that belong to the Safe Harbor or follow its principles.
- ▶ **Security and Data Integrity:** Organizations need to ensure that the data they maintain is accurate, complete, and current—and thus reliable for use. They must also ensure the security of the information by protecting it against loss, misuse, unauthorized access, disclosure, alteration, and destruction.
- ▶ **Access:** Unless they would be unduly burdened or violate the rights of others, organizations must give individuals “access to personal data about them and provide an opportunity to correct, amend, or delete such data.”³⁵
- ▶ **Enforcement:** Organizations must “enforce compliance, provide recourse for individuals who believe their privacy rights have been violated, and impose sanctions on their employees and agents for non-compliance.”³⁶

Joining the Safe Harbor will be expensive, but the alternatives may be equally so, especially if one puts policies in place and fails to comply with them. (One alternative is signing a standard contract with the data commissioners in the source country. The draft contract as of June 2001 is actually more strict than the Safe Harbor.)

The E.U. member states have agreed to give U.S. companies time to consider the impact of the ECDDP and whether Safe Harbor implementation is appropriate for them. The European Commission will review the appropriateness of the grace period in mid-2001. It will thoroughly review the Safe Harbor program in 2003. In the meantime, organizations can consult two Web-based resources for more information:

- ▶ Official home page for the U.S. Safe Harbor Accord – <http://www.export.gov/safeharbor/>
- ▶ Safe Harbor Workbook – <http://www.export.gov/safeharbor/SafeHarborWorkbook.htm>

Organizations eligible for safe harbor protection include:

- ▶ U.S. organizations subject to the jurisdiction of the Federal Trade Commission (FTC).
- ▶ U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DOT).

In addition, other organizations, such as financial institutions, may be eligible if the appropriate enforcement agencies or regulators formally announce that they will take enforcement action against organizations that claim Safe Harbor compliance but fail to live up to their statements.

APPENDIX II: AN INTERVIEW WITH
KAREN ALNES, WELLS FARGO

Karen Alnes is vice president of corporate marketing—privacy policies at San Francisco-based Wells Fargo, a diversified financial services company providing banking, insurance, wealth management and estate planning, investments, mortgage and consumer finance from more than 5,400 stores, its Internet banking site (www.wellsfargo.com) and other distribution channels across North America and elsewhere internationally. Alnes talks here about the challenges and conflicts she perceives in recent privacy legislation.³⁷

How does Wells Fargo view the privacy issue?

Any privacy effort should focus on the customer, so that organizations can identify what customers want and then provide desired products. We seek to make sure that our customers have choices, that they understand what their choices are, and that we are managing their information so that we can systematically honor those choices.

We have found that a privacy focus involves much more than the legislation—certainly more than the Gramm-Leach-Bliley Act and all of the laws that are out there. Some of those laws have become burdensome and costly without addressing consumers' greatest concerns. I think the two things the American public cares about most are dinner-time telemarketing and identity theft. The GLBA and the Fair Credit Reporting Act have focused on commercial information-sharing, but I believe people are far more concerned about controlling unsolicited sales communications.

What about the opt-in/opt-out debate?

I think people are confused about what opt-in and opt-out really mean. They also don't understand the difference between commercial information-sharing and solicitation preferences—opt-out versus “do not solicit.” There are those who believe that the only customer-friendly outcome would be an “opt in” environment, in which the customer would give permission each and every time his information might be used for marketing purposes. Unfortunately, the real result would be 10 times more direct marketing, because companies wouldn't have the information necessary to target the offers.

The use of information allows us to provide better and more specific service to our customers. Stores know that you shop in certain departments, favoring certain designers or sizes, for example, and they tailor their mailings to you based on those preferences and how those preferences might change over time. Similarly, a health care provider might send information based on someone's age and health record. If a department store or an HMO can use information that way—to serve its interests and its customers—why is it wrong for a bank to do it? An opt-in environment imposed only on financial institutions would restrict our ability to provide personalized service and offers to our customers.

Should customers be asked to opt-in to those opportunities?

Opt-in has an emotional appeal. In practice, it does not work very well, because it has to be too categorical. What's more, it will increase marketing costs, and it will cause people to receive even more unsolicited mail or telephone calls from companies with which they do not have relationships. It doubles the complexity of the process. If you have to ask somebody every time, “Are you interested in this product?” then soon, simply asking the question becomes a solicitation. Or if you just ask once in a lifetime, “Are you ever interested in hearing from us

about new products and services,” or, “Do you want to be solicited?” People will simply say, “No.” It’s a difficult question, and neither banks nor their customers come out ahead.

The problem we face is that most people don’t know what products are available unless we tell them. They don’t always know what they need, or their needs may change. What if one bank decided to tell every one of its customers that they have to opt-in to find out about what they offered, but competing organizations did not? For example, if we made people opt-in if they wanted to hear about brokerage, but a competitor chose to market brokerage services to anyone, we wouldn’t be serving our customers, and we may lose some of them as a result.

For you, then, this focus on privacy is prompting new concerns about how you can and should market your products.

That’s right. Privacy is not about financial information. Privacy is not about medical information. The use and sharing of information should be a concern to every business that does direct marketing, because this is really about the regulation of direct marketing. And that is something that is going to take a long time to sort out.

We need to keep in mind that direct marketing exists because it works. Telemarketing exists because it works. And even if only three percent of the people you contact with an offer say, “Yes, I want to buy that,” it still works, and it’s still profitable. We have to figure out how we can offer people products and services—when, where, and how they want them.

Where do you see the privacy issue going, and where would you like to see it go? You’re clearly concerned about the costs, and the benefits.

There are certainly costs involved, but we want to be sure we are investing in things and processes that truly benefit our customers. A business should be able to tailor its product offerings to customers and be able to anticipate what they are going to want, based on the information it has about them. If a business can’t send its customers information describing a new product, then it won’t be serving its customers.

APPENDIX III: AN INTERVIEW WITH
KLM ROYAL DUTCH AIRLINES

The interviewee is an information security project manager at KLM Royal Dutch Airlines, which will celebrate its 82nd anniversary in 2001. He discusses the consequences for KLM of the privacy provisions of the forthcoming European Union's Directive on Data Protection.³⁸

How will the implementation of the E.U. Directive affect your business?

The Netherlands' current privacy law is very strict, but it only affects organizations' registration of personal data—credit card numbers, for example, and, in our business, information such as meal choices, traveling companions, seating preferences, passenger disabilities, and frequent flyer status. The new law affects not just the recording of such data but also the handling of it. We have to be able to document what information we collect as well as when and why we collected it. And, before we request information, we have to be able to tell the customer why we need it and what we are going to do with it. To do that, we need to identify all the departments and processes in which our client data is handled. Once the law goes into effect on September 1, 2001, we will have one year to bring all our activities, registrations, and databases into compliance. That effort is now well underway, as are all our efforts in relation to the current privacy law. Information security is also part of the new E.U. directive: The company or organization processing data needs to secure the confidentiality, integrity, and availability of personal data.

How will the Directive affect your handling of information?

You need certain basic information just to do business. For example, we need to have a person's name and destination to be able to fulfill the transportation contract, which is what a ticket represents. Other information might be nice to have to help you know your customers better and therefore serve them better. The new law applies to what we do with that information, beyond the operation of the flight. So, for example, if I want to send a brochure to a customer about a city he or she may be visiting, I need to ask first if that person wants to receive that information from me; I cannot simply assume they do. Or, if a passenger ordered a vegetarian meal, we cannot use that information for purposes other than operating the flight. Under the law, we're not allowed to send that passenger a mailing, for example, notifying him or her of a source for vegetarian recipes unless we first obtain the individual's consent. We can draw conclusions from information, but we cannot act on those conclusions other than for purposes of operating our flights.

Do you expect the Directive to be cumbersome or ultimately good for organizations?

I think the new law will ultimately be good for the company. For one thing, it will help us make our use of personal information transparent for our customers. When people here in the Netherlands receive marketing mailings, typically their first question is, Who supplied my address? Companies here don't want to be known as organizations that release personal information too easily. That kind of behavior can create an image problem. KLM is considered a reliable airline, not only in its operations but also in its handling of data. We want absolutely to maintain that image.

Will the Directive affect communication among departments at KLM?

Yes. We must be more careful about transferring data that are not directly necessary to perform the contract of carriage among companies within the KLM group. Most of them are European, but the U.S. carrier Northwest Airlines is also a partner. And, on Sept. 1, 2001, we are not even allowed to send client data other than for the performance of the contract of carriage to U.S. companies unless those companies are in compliance with the European Union's Safe Harbor Principles. By signing a contract agreeing to comply with those principles, Northwest will be agreeing to treat private data exactly as KLM does.

Do the people and companies in the Netherlands embrace the E.U. Directive and support compliance?

It depends who you ask. For example, I've read that in the United States, people get a lot of "junk mail." That's also starting here, and a lot of people are asking, Who supplied my address? Therefore the new law is good; it solves part of that problem. If you ask companies, however, many will say that it will restrict their marketing efforts. At KLM, we are very conservative in that respect. We send mailings only to our registered frequent flyers or people who have requested regular mailings or specific information (with the consent of these clients).

Where do you see this issue going? And how are your preparations evolving?

At KLM, we won't have many changes. For us, the biggest effort will not be simply complying with the law, but documenting and monitoring the flow of data. Customers will be able to contact us and ask, What personal information did you record, when did you do that, and why did you do it? Because they will be able to ask those questions, we must be sure we have documented that process and are able to answer their questions—immediately. What do we have, when did we get it, and why do we have it? We have until Sept 2002 to document the whole flow of the private information we maintain.

To this end, our efforts in this department are focusing on enhancing awareness of procedures ensuring data security and privacy. This includes coordination of efforts with our legal department. Making these efforts now will make the second phase, beginning after September 2002, easier and much more efficient. Customers will be asking us a lot of questions. We're making sure we can answer them.

Relations with our partners are also an issue. If they're within the European Union, it's not much of a problem. But although the E.U. Directive applies to all European countries equally, there will still be variations in its interpretation. The Directive is the common denominator, so to speak, and we can impose our own more strict interpretations. Our image as a reliable airline is one of our most valuable assets, and we want to be sure we do all we can to protect that reputation.

APPENDIX IV: AN INTERVIEW WITH
CHRIS CARNEY, BON SECOURS HEALTH SYSTEM

Chris Carney is CEO of the Baltimore-based Bon Secours Health System, which includes hospitals, nursing homes, assisted and independent living facilities, residential treatment centers, and other providers within 14 systems in nine eastern states. He describes his views on health care privacy and how his thinking has evolved in response to the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA).³⁹

How does Bon Secours view the privacy issue?

Privacy, or what we have traditionally called patient confidentiality, has been embodied in health care policies, procedures, and codes of conduct for many years. Bon Secours recognized it as a System in 1998, when we adopted a corporate responsibility program that mandates respect for privacy across the organization and within each facility. We regard privacy as having a moral dimension, in that respecting privacy is equivalent to respecting individual dignity. In our organization, respect for individual dignity is a core principle, so privacy, or confidentiality, naturally flows from our values.

We see privacy driving a lot of debate, largely over how it's defined and what degree of privacy people expect when they receive health care. And now with the onset of HIPAA, we have begun to see new privacy regulations that attempt to change certain aspects of organizational or individual behaviors that frankly may or may not benefit patient privacy and confidentiality.

I'm in favor of anything that removes complexity from health care billing, so the HIPAA regulations that seek to simplify transactions and data sets, for example, could be good for us as providers as well as for patients and their families, physicians, and insurance companies. But certain parts of HIPAA appear to be a solution in search of a problem. In addressing privacy, HIPAA reaches well beyond administrative issues and into patient care. I don't believe that the security and privacy aspects of HIPAA were based upon publicly available data or derived from citizens' requests of their representatives in Congress. If you believe that the vast majority of health care providers in the United States are already concerned about privacy, then HIPAA should be something that refines and improves their inclination to protect privacy as opposed to drastically reforming it—which is what it seeks to do.

How do you expect that HIPAA's privacy aspects will affect your organization and your patients?

One of our obligations under HIPAA is that during the admissions process, we must communicate to patients and their families our approach to privacy protection. In my years of experience—as a leader of hospitals, as a patient, and as a family member—most people do not come into the hospital with privacy as a major concern. They are primarily interested in their health and receiving quality health care in a caring environment.

I'm not saying that privacy isn't important. It's just not clear to me how HIPAA's privacy provisions are going to measurably improve our ability to provide the high-quality, compassionate, responsive care that people come to us expecting to receive. Currently, insurers can amend policies with pre-existing condition modifications, but state insurance commission regulations do not give unrestricted ability to health insurers to refuse to sell someone a policy based upon knowledge of their health record. So how these new health care privacy provisions actually help people receive better care is not apparent.

Is HIPAA currently affecting how your employees go about their work every day?

Not yet, because we have two years before the regulations go into effect. At this point we are actively studying the regulations, and we continue to be part of national advocacy campaigns to modify them. The risk we face is that certain parts of the HIPAA privacy and security regulations are just about impossible to implement. So we continue to recommend to HHS that certain regulations be modified and simplified so that they can be implemented. I have to say I was more optimistic about our prospects before the Administration announced in April 2001 that they're going to proceed with implementation according to the schedule and then modify the regulations before the actual effective date.

To be prepared, we're creating a structure for allocating funds to implement HIPAA, because there are millions of dollars of capital and operating expenditures associated with it, none of which are funded. We're also staying in close touch with our partners—vendors, insurance companies, and computer companies—all of whom will be affected by the regulations.

Where do you see this issue going? Where would you like to see it go?

This issue is part of a national concern about privacy that has become far bigger than I had anticipated. I think it reflects the huge conflict between Americans' desire to have instant access to anything, wherever they are, and at the same time to expect some degree of confidentiality or security associated with that access. Every time you get on your cell phone you really don't know who's listening in. That doesn't stop you from using your cell phone, or giving your credit card number over that phone, or using an ATM machine. Technology has advanced farther and faster than our thinking, as a country or as a people, and certainly faster than the ability of the legislative and judicial processes to keep up. Convenience has become a huge part of contemporary life, and with convenience there goes certain risks. We have yet to say which of those risks are acceptable to us and which are not. The HIPAA legislation emerged without any clear measurement of what risks we needed to guard against.

If you can see no measurable benefit, can you imagine any way the HIPAA privacy regulations will help you or your customers?

The primary benefit is that as a result of all the work that providers and payors will go through to implement these regulations, the importance of privacy will be continually reinforced. These efforts will reinforce our practice to continue to talk with our employees and our physicians about what privacy is and why it's important. Whether that's a top concern of our patients, however, is the question. If you were to ask the thousands of patients for whom Bon Secours is responsible today if they were concerned about their privacy in the health care setting, I'd guess that few would describe it as what keeps them up at night. They're much more concerned about health care costs, access, and quality—which is what they ought to be most concerned about.

APPENDIX V: AN INTERVIEW WITH
KIRK HERATH, NATIONWIDE

Kirk Herath is chief privacy officer at Nationwide, a Fortune 500 company and one of the largest diversified financial and insurance services providers in the United States. Headquartered in Columbus, Ohio, where it was founded in 1925, Nationwide has assets of \$117 billion and more than 35,000 employees and agents. Herath talks here about how he expects recent legislation and other privacy-related issues to affect his organization.⁴⁰

How does Nationwide view the privacy issue?

A focus on privacy is simply good business. But to be successful, privacy efforts must transcend mere compliance, because privacy is a risk management issue. It's evolving quickly, and gauging customer expectations while continuing to do business is difficult. As long as an industry is dependent on personal information as its raw material, problems will occur. For that reason some members of our industry may view a privacy effort as a nuisance; for us it's a business opportunity.

How did your role as CPO evolve?

I was appointed CPO in April 2000, with a mandate to implement the Gramm-Leach-Bliley Act (GLBA) and a privacy program. I'd been following the issue for several years, so when GLBA finally passed, in November 1999, we already had the foundation for a governance structure as well as a multidisciplinary, multifunctional team encompassing leaders from each of our business units and functional areas. Privacy and security go hand in hand, so we keep the departments separate but closely aligned. In fact, they are completely different disciplines. Security is technical while privacy has a legal focus. No single entity owns privacy, and there's not an area in the whole corporation that privacy doesn't touch. Even the maintenance people have to worry about trash disposal.

How does your perspective on privacy play out in day-to-day business?

My staff includes just a few people, with virtual teams that expand as needed. We serve at the center of a hub-and-spoke system of internal information-sharing with the business units and the functional areas. A reporter called the other day and asked what we had to do now that we've issued our privacy statements. I laughed, because the statements are the tip of the iceberg. They are a public communication of our information practices; there's still a lot to do day to day. For example, we're working on our privacy infrastructure project—establishing the policies and procedures as well as the physical and technological means by which privacy can be assured. I also reminded the reporter that HIPAA is coming, and it will be almost all-consuming for a couple of years. HIPAA has a fairly strict standard on access; files will have to be kept in locked cabinets or rooms, and unless someone's job gives them a need to know, they won't have access, electronically or physically, to that material. Planning the necessary internal education, and determining how we should enforce internal compliance, requires at least a third of our time now.

How will HIPAA's privacy aspects affect your organization?

For many companies, full compliance with HIPAA is an impossibility. It blows up their business models, or it becomes so expensive that it puts them out of business. The provision that seems particularly onerous is the one I call the "chain of custody," which requires organizations to maintain a ledger tracking every place certain information has ever resided, along with a record of who has handled it. Jane in accounting saw it, and she gave it to Phil the mail guy, who dropped it off with Ken the claims guy, who gave it to Ken the claims guy's boss, who then sent it over to.... It simply can't be done. Inevitably, organizations will indicate in letters to the files that they considered it, they tried to do it, they realized the cost would be in the millions, and they saw that complying would put them out of business.

It's interesting that the two issues that drove privacy were identity theft and those dinnertime telemarketing calls that we all detest. There were some abuses on the health care side, but if you look at the record, those instances were very few and terribly anecdotal. So what we have now is legislation by anecdote.

Do you expect your customers, or Nationwide itself, to benefit significantly from these efforts?

No, I think it's a necessity, more than a benefit; something you have to do to be in business. Some will do a better job than others—especially those that go to a customer choice model, an opt-in. European companies offer opt-in, it's very big among Internet companies, and a couple of banks do the same. Royal Bank of Canada (RBC), for example, has a wonderful opt-in. Their customers tell them if they want to receive any communications, period; or if they want to get information by mail, by phone, or electronically. Customers specify what information they desire. Insurance products? If so, which ones? As a result, RBC can start creating pools of people to whom they can market, and I do think this is where the market will drive us within five years.

Opt-in is actually easier to comply with than opt-out. I'm a lawyer, and from a pure compliance perspective, and from a legal risk perspective, opt-in is golden. Opt-out, on the other hand, is fraught with problems. Plus, a lot of people think it's a ruse. They're convinced you're trying to pull one over on them. For example, right now, outside certain exceptions, we do not share information, and that's what we say in our privacy statement. The statement also says that if we ever decide to share, we'll offer customers the chance to opt out. I've had people call and tell me they want to opt out now, but there's nothing for them to opt out of. We don't share information.

Where do you see the privacy issue going? Where would you like to see it go?

The marketers are starting to believe the surveys that show that the way companies have traditionally used information violates how average Americans want their information to be used. Many companies, in fact, are slowly realizing that offering customers a choice is actually a good idea. The market leaders will move in that direction, in part because the technology already exists to track people in "buckets" based on their interest in products and how they want to receive information. Instead of sending a million people a mailing, expecting only two percent to respond, why not contact the 10 percent who actually want the information? Of that 10 percent, you might get as many as half of them to respond because you're tailoring the message to those you know are interested. So, ultimately, I think the market is going to drive the privacy issue, simply because even the legislators that support the strictest privacy protections don't want to regulate people out of business.

E N D N O T E S

- ¹ Mary Pat McCarthy and Stuart Campbell with Rob Brownstein, *Security Transformation: Digital Defense Strategies to Protect Your Company's Reputation and Market Share*. New York: McGraw-Hill, 2001, pp. 162-3.
- ² Drew Clark. "House Lawmakers Treat Privacy Issue Cautiously," *National Journal's Technology Daily*, 3/1/01.
- ³ Toby Lester. "The Reinvention of Privacy," *The Atlantic Monthly*, 3/01, pp. 27-39.
- ⁴ As defined by the European Union (E.U.) directives and the United States Safe Harbor Privacy Principles, 7/21/00, and cited in the "AICPA/CICA WebTrust SM/TM Program for Online Privacy, November 30, 2000," p. 7.
- ⁵ Michael Cappellas, Chairman and CEO of Compaq, in a speech given at KPMG's Americas Lead Partner Forum, New York City, 4/01.
- ⁶ Jay Stanley with John C. McCarthy, Michael J. Tavilla, and Jeremy Sharrard. "Surviving the Privacy Revolution," *The Forrester Report*, Forrester Research, Inc., 2/01, p. 8.
- ⁷ Susannah Fox et. al. "Trust and Privacy Online: Why Americans Want to Rewrite the Rules," *The Pew Internet & American Life Project*, PR release 8/20/00.
- ⁸ Jay Stanley with John C. McCarthy. "Growing Privacy Labyrinth Hinders eBusiness," *The Forrester Brief*, 12/1/00, p. 2.
- ⁹ Patrick Ross. "Congress Responds to Concerns, But Conflict Could Delay Action," CNET News.com, 2/23/01.
- ¹⁰ KPMG's Government Affairs group.
- ¹¹ Public Opinion Strategies, 6/24/01. www.publicopinionstrategies.com
- ¹² Jay Stanley with John C. McCarthy, Michael J. Tavilla, and Jeremy Sharrard. "Surviving the Privacy Revolution," *The Forrester Report*, Forrester Research, Inc., 2/01, p. 7.
- ¹³ "Compliance With HIPAA Standards Will Require Massive Security Overhaul And Present a Tougher Challenge Than Y2K, According To Health Care Experts," *Business Wire*, 4/17/01.
- ¹⁴ Standards for Privacy of Individually Identifiable Health Information, Preamble, 45 CFR Parts 160 through 164, Section IV - Final Regulatory Impact Analysis, which may also be found at <http://aspe.hhs.gov/admsimp/final/PvcPre04.htm>
- ¹⁵ "U.S. and E.U. Reach Agreement on Safe Harbor Principles for Data Privacy," *The Computer Lawyer*, 5/00, Vol. 15, No. 5, p. 34.
- ¹⁶ Jay Stanley with John C. McCarthy, Michael J. Tavilla, and Jeremy Sharrard. "Surviving the Privacy Revolution," *The Forrester Report*, Forrester Research, Inc., 2/01, p. 9.
- ¹⁷ Peter H. Lewis and Ellen Florian. "The End of Privacy," *Fortune*, 3/19/01, p. 64.
- ¹⁸ David M. Katz. "Privacy Risks Threaten Bottom Lines," CFO.com, 2/22/01.
- ¹⁹ "Employees' Suit Alleges Invasion of Privacy," *The Bulletin's Frontrunner*, 11/3/00.
- ²⁰ Jeffrey A. Kaufman. "Canadian Privacy Laws: A Trap For The Unwary," *The Metropolitan Corporate Counsel*, 10/20, p. 21.
- ²¹ Jennifer O'Brien. "United Kingdom: Dataflow Between Europe And The U.S.," Mondaq Business Briefing, 4/6/01.
- ²² From "The Australian Privacy Commissioner's Website," <http://www.privacy.gov.au/>
- ²³ Thomas Weyr. "Argentina Adopts Tough Data Protection Law," *DM News*, 10/23/00.
- ²⁴ Christine Canabou, Pamela Kruger and Cathy Olofson. "What's on Your Agenda? Ten Senior Executives and Thinkers Explain the Most Crucial Item on Their Leadership Agenda," *FastCompany.com*, 6/01. <http://robin.fastcompany.com/cgi-bin/nph-t.pl?U=161&M=68303&MS=272>
- ²⁵ Luis Salzar. "Post-Mortem for Toysmart.com," *The Bankruptcy Strategist*, 2/01, Vol. 18; No.4, p 10.
- ²⁶ Ibid.
- ²⁷ Toby Lester. "The Reinvention of Privacy," *The Atlantic Monthly*, 3/01, pp. 27-39.
- ²⁸ Tamara Loomis. "Chief Privacy Officers; A New Executive Role Gains Wider Acceptance," *New York Law Journal*, 5/10/01.
- ²⁹ "U.S. and E.U. Reach Agreement of Safe Harbor Principles for Data Privacy," *The Computer Lawyer*, 5/00. Vol. 15, No. 5, p. 34.
- ³⁰ John T. Bentivoglio and Sarah Haden. "U.S. Companies Must Decide Whether to Enter U.S.-E.U. Safe Harbor for Data," *The Computer & Internet Lawyer*, 3/01, Vol. 18, No. 3, p. 1.
- ³¹ "Financial Services Regulatory Report, March/April 2000 - Mayer Brown & Platt," Mondaq Ltd., *International Briefing*, 11/24/00.
- ³² John T. Bentivoglio and Sarah Haden. "U.S. Companies Must Decide Whether to Enter U.S.-E.U. Safe Harbor for Data," *The Computer & Internet Lawyer*, 3/01, Vol. 18, No. 3, p. 1.
- ³³ Ibid.
- ³⁴ Ibid.
- ³⁵ Ibid.
- ³⁶ Ibid.
- ³⁷ Telephone conversation with Karen Alnes, 5/23/01.
- ³⁸ Telephone conversation with an information security project manager at KLM Royal Dutch Airlines, 6/05/01.
- ³⁹ Telephone conversation with Chris Carney, 5/07/01.
- ⁴⁰ Telephone conversation with Kirk Herath, 5/09/01.