110 Pitfalls & Landmines in Privacy & the Collection, Use, & Security of Personal Information

Jeffrey D. Adelman
Vice President and General Counsel
j2 Global Communications

Paula Barrett
Partner
Eversheds LLP

Brent V. Bidjou
*Corporate Legal Counse*l
Fair Isaac Corporation

Faculty Biographies

Jeffrey D. Adelman

Jeffrey D. Adelman is vice president and general counsel of j2 Global Communications, Inc. in Los Angeles. j2 provides outsourced, value-added, messaging services, including its flagship eFax service, to individuals and businesses throughout the world. Mr. Adelman's responsibilities include overseeing the in-house legal team and providing legal counsel to the company and its board of directors on a variety of matters.

Prior to joining j2, Mr. Adelman practiced general corporate, securities, and mergers and acquisitions law with Miller, Canfield, Paddock & Stone, Detroit's largest and oldest law firm.

Mr. Adelman attended the University of Michigan for both undergraduate and law school.

Paula Barrett
Partner
Eversheds LLP

Brent V. Bidjou
Corporate Legal Counsel
Fair Isaac Corporation

ACC Association of Corporate Counsel

110 Pitfalls & Landmines in Privacy & the Collection, Use & Security of Personal Information

Jeffrey D. Adelman – j2 Global Communications, Inc.
Brent Bidjou – Fair Isaac Corporation
Paula Barrett – Eversheds LLP

ACC's 2005 Annual Meeting: Legal Underdog to Corporate Superhero—Using Compliance for a Competitive Advantage

October 17-19, Marriott Wardman Park Hotel

North America Overview

Jeffrey D. Adelman
Vice President and General Counsel
j2 Global Communications, Inc.

This presentation is for informational purposes only and does not constitute as legal advice. You should seek counsel to assess the implications of the legislation discussed in this presentation on your company's specific operations.

Overview of Privacy and Security Issues

- No single U.S. or international law regulates Internet privacy and security.
- Many laws *might* apply depending on the circumstances.
- The regulatory environment is changing rapidly.
- General approach: Say what you do; do what you say; obtain consent to collection, use and disclosure of personal information.

Establishing a Compliance Program

- Identify personal information handled by the organization and from which jurisdictions the information originates in order to determine which regulations apply.
- Identify organization's current level of compliance with applicable privacy and security regulations. This includes evaluation of the organization's technical infrastructure.
- Design policies, procedures, and processes that are compliant with the applicable regulations and disseminate to appropriate personnel and provide adequate training.
- Perform regular audits and training, and modify policies and practices as necessary to ensure continued compliance.
- Keep abreast of changes in regulatory environment, including disclosure requirements for security breaches.

Making Privacy and Security a Priority

- Assign privacy, security and compliance officer roles to specific individuals in the organization. In doing so, consider the organization's size, the complexity of privacy and security implementation and oversight, and the nature of the information.
- Privacy and security must be a corporate priority with oversight by senior management and the board of directors as part of good corporate governance.

Information Collected and its Source

- Applicable regulations vary based on type of information collected and jurisdiction where disclosure is initiated
  - Personal Information (e.g., name, address, telephone, email, credit card)
  - Personal Health Information (e.g., medical records and insurance information)
  - Personal Financial Information (e.g., financial records, credit report)
  - Personal information from children
  - Source of information is in the U.S. vs. International

Gramm-Leach-Bliley (Privacy/Safeguard: 15 U.S.C. § 6801-6809)

- Subtitle A of Title V restricts disclosure by financial institutions of individual consumers' nonpublic personal information (NPI) to nonaffiliated third parties.
- FTC has issued Privacy and Security Rules
- "Financial institution": banks, securities firms, insurance companies, and companies "significantly engaged" in providing other financial services to consumers.
- *General Scheme*: Notice and Opportunity to Opt Out.

Gramm-Leach-Bliley (NPI)

- NPI: Includes (a) nonpublic personally identifiable financial information; and (b) any list, description, or other grouping of consumers derived using any personally identifiable financial information that is not publicly available.
- "Personally Identifiable Financial Information" is any information:
  - A consumer provides to obtain a financial product or service;
  - About a consumer resulting from any transaction involving a financial product or service; or
  - Otherwise obtained about a consumer in connection with providing a financial product or service.

Gramm-Leach-Bliley (Privacy)

- *Customers* (as opposed to *consumers*) must receive a privacy notice when they first become a customer and once a year thereafter for as long as the customer relationship lasts.
- *Consumers* are entitled to privacy notice only if the financial institution shares the consumers' information with companies not affiliated with it, with exceptions.
- "Consumer": an individual who obtains or has obtained a financial product or service from a financial institution for personal, family or household reasons.
- "Customer" is a consumer who has a continuing relationship with a financial institution.
- Privacy notice: clear, conspicuous, accurate statement of policies on disclosing NPI to affiliates and nonaffiliated third parties, disclosing NPI after the customer relationship is terminated, and protecting NPI.
- *Opt Out*: Consumers and customers have the right to opt out of having their information shared with nonaffiliated third parties, with exceptions.
- Prohibits disclosure of customer account numbers to non-affiliated companies for marketing purposes, even if the customer does not opt out.

Gramm-Leach-Bliley (Security)

- Requires financial institutions to develop a written information security plan that describes their program to protect customer information. Plan must be appropriate to size and complexity, nature and scope of activities, and sensitivity of customer information handled.
- As part of its plan, each financial institution must:
  - designate one or more employees to coordinate the safeguards;
  - identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
  - design and implement a safeguards program, and regularly monitor and test it;
  - select appropriate service providers and contract with them to implement safeguards; and
  - evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business arrangements or operations, or the results of testing and monitoring of safeguards.

Health Insurance Portability and Accountability Act (HIPAA) (42 U.S.C. 201 et seq.)

- Privacy and security provisions and underlying Department of Health and Human Services rules apply to "Covered Entities" (CEs) with respect to "Protected Health Information" (PHI)
- CEs include Health Plans, Health Care Clearinghouses and Health Care Providers
  - Covers employers based on their roles as health plan sponsors
- PHI: personally identifiable health information maintained by a CE (name, city, zip code, ph, fax, etc)
- Security Standard: CE must:
  - Ensure confidentiality, integrity, availability of electronic PHI created, received, maintained or transmitted by CE.
  - Protect against reasonably anticipated threats or hazards to security or integrity of PHI.
  - Protect against reasonably anticipated unauthorized uses or disclosures of PHI.

HIPAA Business Associates

- CEs must enter into Business Associate Agreements (BAAs) with Business Associates (BAs)
- BA: Any person or entity performing or helping perform a function or activity involving the use or disclosure of PHI on behalf of a Covered Entity.
- Required assurances of BA in BAA:
  - Not to use or disclose PHI except as allowed by the BAA or required by law;
  - Use appropriate safeguards to protect confidentiality of PHI;
  - Report BAA violations to the CE;
  - Ensure that its agents/subcontractors agree to same requirements;
  - Provide CE information necessary for it to comply with patient disclosure requirements;
  - Provide HHS the BA's internal practices and records relating to use and disclosure of PHI;
  - Return or destroy PHI once the contract is terminated, if feasible and legal.

Fair Credit Reporting Act (15 U.S.C. 1681 et seq.)

- Designed to protect the privacy of credit report information and to guarantee that information supplied by consumer reporting agencies (CRAs) is accurate.
- Companies reporting information about consumers to a CRA are considered "furnishers" of information.
- CRAs include many types of databases -- credit bureaus, tenant screening companies, check verification services, and medical information services -- that collect information to help businesses evaluate consumers.
- Prohibition on furnishing information known to be inaccurate or where the furnisher consciously avoids knowing whether it is inaccurate.
- Must correct information discovered to be inaccurate and resubmit to each CRA.
- Specific requirements regarding disclosure of consumer delinquent accounts.

Children's Online Privacy Protection Act **15 U.S.C. 6501-6506**

- Applies to:
  - Operators of commercial Web sites and online services directed to children under 13 that collect personal information from them.
  - Operators of general audience sites that knowingly collect personal information from children under 13
  - Operators of general audience sites that have a separate children's area and that collect personal information from children under 13.
- Requires operators to:
  - Post privacy policy on homepage of Web site and link to it on every page where personal information is collected.
  - Provide parents notice about site's information collection practices and obtain verifiable parental consent before collecting personal information from children.
  - Give parents choice as to disclosure of child's personal information to third parties.
  - Provide parents access to child's personal information, opportunity to delete it and opt-out of future collection or use of the information.
  - Maintain confidentiality, security, integrity of personal information provided by children.
- Safe harbor: FTC may approval self-regulatory guidelines and FTC has approved several.

Electronic Communications Privacy Act

(18 U.S.C. 2510-22, 2701-2711)

- Prohibits wire or electronic service providers from releasing information regarding customers' communications, unless the release is specifically authorized by a court order, subpoena, warrant, or other exception.
- Safe harbor for service providers that improperly release information in good faith reliance on a court order, subpoena or warrant.

Confidentiality of Social Security Numbers – California Civil Code § 1798.85

- Individuals, businesses and certain gov't entities may not (unless required by state or fed'l law):
  - Publicly display SS#s, print SS#s on ID cards or badges, require people to transmit SS#s over the Internet unless secure or encrypted, require people to use SS# to logon to the Internet without a password, print SS#s on mailed documents, or embed or encode a SS# on a card or document where printing it would be prohibited.

Destruction of Personal Information

- **Fair and Accurate Transactions Act (FACTA):** Employers must destroy personal information about their employees before they throw it out if they got the information from a credit report. That means "shredding or burning" paper documents or "smashing or wiping" computer disks.
- **California Civil Code 1798.80-1798.84:** any business that deals with "personal information" "shall take all reasonable steps to destroy" a customer's records that are no longer of value by "shredding, erasing or otherwise modifying" the information to render it unreadable. Private right of action established.
- **Wisconsin 895.505** - certain businesses, particularly financial, medical and tax preparation institutions, must properly dispose of all confidential client records and information.
- **Georgia SB475**: crime for a business to discard personal information unless it first "shreds, erases, modifies" and makes "reasonably" sure no one will have access to it before it is destroyed. Up to $10,000 fine per violation.

Canada: The Personal Information Protection and Electronic Documents Act (PIPEDA)

- Covers collection, storage and use of personal information by organizations in the public and private sectors.
- Pre-empts provincial legislation unless it is "substantially similar".
- General Rule: Businesses must inform consumers of who is collecting the information, why the information is being gathered, and for what purposes it will be used.

PIPEDA - Requirements for Collection of Personal Information

- Gathered with the knowledge and consent of the consumer;
- Collected for a reasonable purpose;
- Used only for the reasons for which it was gathered;
- Accurate and up to date;
- Open for inspection and correction by the consumer;
- Stored securely

PIPEDA (continued)

- Enforced by the Privacy Commissioner of Canada
- Canadian entities required to designate individual to handle privacy issues and complaints
- Individuals can file complaint with the Privacy Commissioner, who has authority to investigate and publish results.
- Individual can then file action in Federal Court, which can require compliance and award damages.

Legislative Update on Security Breach Consumer Notification and Practical Measures to Mitigate Risk

Brent Bidjou, Fair Isaac Corporate Legal Counsel

This presentation is for informational purposes only and does not constitute as legal advice. You should seek counsel to assess the implications of the legislation discussed in this presentation on your company's specific operations.

Economic Impact of Identity Theft

- According to the Federal Trade Commission (FTC), 10,000,000 Americans were affected by identity theft in 2004.
- The problem is getting increasingly worse and is the most common fraud perpetrated on individuals.
- In 2004, identity theft accounted for 39 percent of consumer fraud complaints filed with the FTC.
- An FTC survey indicated that identity theft has cost the United States approximately $52,600,000,000 in 2004 with individuals and businesses bearing this heavy financial burden.

Facts of Choicepoint Security Breach

- Choicepoint is a GA based data firm which maintains databases containing aggregated personal information on US consumers.
- Choicepoint gave the information including addresses, phone numbers and social security numbers to criminals which posed as legitimate small businesses to obtain access to this personal data.
- Choicepoint initially chose to notify between 30,000 to 35,000 California residents that their information may have been accessed by unauthorized parties.
- Choicepoint's notification efforts extended beyond California to a pool of 145,000 impacted consumers across the nation and gained the attention of national media.

Facts of Choicepoint Security Breach-Cont'd

- Since this incident, Choicepoint became subject to an FTC inquiry on its compliance with federal information security laws, an SEC investigation for insider trading violations, lawsuits alleging violations of the Fair Credit Reporting Act, a shareholder class action lawsuit alleging inadequate security measures, action by GA regulators to place Choicepoint on probation and require immediate consumer notification of future security breaches. Choicepoint saw a decline of its share price by over 20% within the first month of news releases.
- Choicepoint is not alone and in recent months, other companies including Seisint (Lexis-Nexis) and Bank of America, have provided consumer notifications for security breach incidents. Bank of America alone provided notifications to over 1.2 million credit card holders after backup tapes with their account numbers and personal information were lost.

Facts of CardSystems Security Breach Incident

- Unauthorized research opened door to MasterCard breach.
- The head of the card processing firm blamed for a security breach affecting up to 40m credit card numbers has admitted it wasn't supposed to hold the compromised data. John M. Perry, chief exec of CardSystems Solutions, told the *New York Times* that the data was being kept for "research purposes".
- MasterCard said that the [unencrypted] data - which included customers names, card numbers and cvv (security) codes but not customer addresses - had been "inappropriately retained" by CardSystems, the paper reports.

Security Breach Notification in 2005

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
15-Feb-05	ChoicePoint	ID thieves accessed	145,000
25-Feb-05	Bank of America	Lost backup tape	1,200,000
25-Feb-05	PayMaxx	Exposed online	25,000
8-Mar-05	DSW/Retail Ventures	Hacking	100,000
10-Mar-05	LexisNexis	Passwords compromised	32,000
11-Mar-05	Univ. of CA, Berkeley	Stolen laptop	98,400
11-Mar-05	Boston College	Hacking	120,000
12-Mar-05	NV Dept. of Motor Vehicle	Stolen computer	8,900
20-Mar-05	Northwestern Univ.	Hacking	21,000
20-Mar-05	Univ. of NV., Las Vegas	Hacking	5,000
22-Mar-05	Calif. State Univ., Chico	Hacking	59,000
23-Mar-05	Univ. of CA, San Francisco	Hacking	"hundreds of thousands"
28-Ma-05	Univ. of Chicago	Dishonest	59,000
April ?, 2005	Georgia DMV	Dishonest insider	"hundreds of thousands"
05-Apr-05	MCI	Stolen laptop	16,500
08-Apr-05	Eastern National	Hacker	15,000
08-Apr-05	San Jose Med. Group	Stolen computer	185,000
11-Apr-05	Tufts University	Hacking	106,000
12-Apr-05	LexisNexis	Passwords compromised	Additional 280,000
14-Apr-05	Polo Ralph Lauren/HSBC	Hacking	180,000
14-Apr-05	Calif. FasTrack	Dishonest Insider	4,500

Security Breach Notification in 2005

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
15-Apr-05	CA Dept. of Health Services	Stolen laptop	21,600
18-Apr-05	DSW/ Retail Ventures	Hacking	Additional 1,300,000
20-Apr-05	Ameritrade	Lost backup tape	200,000
21-Apr-05	Carnegie Mellon Univ.	Hacking	19,000
26-Apr-05	Mich. State Univ's Wharton Center	Hacking	40,000
26-Apr-05	Christus St. Joseph's Hospital	Stolen computer	19,000
28-Apr-05	Georgia Southern Univ.	Hacking	"tens of thousands"
28-Apr-05	Wachovia,	Dishonest insiders	676,000
	Bank of America,		
	PNC Financial Services Group and		
	Commerce Bancorp		
29-Apr-05	Oklahoma State Univ.	Missing laptop	37,000
02-May-05	Time Warner	Lost backup tapes	600,000
04-May-05	CO. Health Dept.	Stolen laptop	1,600 (families)
05-May-05	Purdue Univ.	Hacker	11,360
07-May-05	Dept. of Justice	Stolen laptop	80,000
11-May-05	Stanford Univ.	Hacker	9,900
12-May-05	Hinsdale Central High School	Hacker	2,400
16-May-05	Westborough Bank	Dishonest insider	750
18-May-05	Univ. of Ohio	Hacking	30,000

ACC's 2005 Annual Meeting: Legal Underdog to Corporate Superhero—Using Compliance for a Competitive Advantage October 17-19, Marriott Wardman Park Hotel

Security Breach Notification in 2005

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
18-May-05	Jackson Comm. College, Michigan	Hacker	8,000
19-May-05	Valdosta State Univ., GA	Hacker	40,000
20-May-05	Purdue Univ.	Hacker	11,000
26-May-05	Duke Univ.	Hacker	5,500
27-May-05	Cleveland State Univ.	Stolen laptop	44,420
28-May-05	Merlin Data Services	Bogus acct. set up	9,000
30-May-05	Motorola	Computers stolen	unknown
31-May-05	Omega World Travel	Stolen Laptop	80,000
06-Jun-05	CitiFinancial	Lost backup tapes	3,900,000
10-Jun-05	Fed. Deposit Insurance Corp. (FDIC)	Not disclosed	6,000
16-Jun-05	CardSystems	Hacker	40,000,000
17-Jun-05	Kent State Univ.	Stolen Laptop	1,400.00
18-Jun-05	Univ. of Hawaii	Dishonest Insider	150,000
22-Jun-05	Eastman Kodak	Stolen Lapton	5,800
22-Jun-05	East Caraolina Univ.	Hacking	72,000
25-Jun-05	Univ. of CT (UCONN)	Hacker	72,000
28-Jun-05	Lucas Cty. Children Services (OH)	Exposed by email	900
29-Jun-05	Bank of America	Stolen Lapton	18,000
30-Jun-05	Ohio State Univ.	Stolen Laptop	15,000

Security Breach Notification in 2005

DATE MADE PUBLIC	NAME	TYPE OF BREACH	NUMBER
30-Jun-05	Ohio State Univ.	Stolen Laptop	15,000
01-Jul-05	Univ of Ca, SanDiego	Hacking	3,300
06-Jul-05	City National Bank	Lost backup tapes	Unknown
07-Jul-05	Mich. State Univ.	Hacking	27,000
07-Jul-05	Univ. of Southern Calif. (USC)	Hacking	270,000
21-Jul-05	Univ. of Colorado	Hacking	42,000
30-Jul-05	San Diego Co. Emp. Retirement Assoc	Hacking	33,000
30-Jul-05	Calif. State Univ., Dominguez Hills	Hacking	9,613
31-Jul-05	Cal Poly-Pomona	Hacking	31,007
02-Aug-05	Univ. of Colorado	Hacking	36,000
09-Aug-05	Sonoma State Univ.	Hacking	61,709
10-Aug-05	Univ. of North TX	Hacking	39,000

ACC's 2005 Annual Meeting: Legal Underdog to Corporate Superhero—Using Compliance for a Competitive Advantage October 17-19, Marriott Wardman Park Hotel

California Security Breach Notification Standard – CA Civil Code 1798

- Primary State Legislation that addresses Data Security Breach Notification.
- Specifically indicates when organizations must disclose security breaches of CA resident data.
- Compliance with this statute was the impetus for the consumer notifications that occurred in Choicepoint and notifications made since.
- Choicepoint and LexisNexis representatives testified before the US Senate that those companies suffered security breaches of consumer data before this law was passed in 2003 and chose not to alert the public in those cases.

Data Governed Under CA Civil Code 1798

- "Personal information" means individual name and a combination of one or more of the following unencrypted data elements: Social Security Number, Drivers License Number or CA ID card number, account number, credit or debit card number, in combination with the required security code, access code or password that would permit access to an individual's financial account.
- Personal information does not include publicly available information from lawful sources.
- Applies to persons or businesses that conduct business in CA, that own or license computerized data that contains personal information which was or reasonably believed to be acquired by an unauthorized person.
- In force since July 1, 2003.

Methods of Consumer Notification Under CA Civil Code 1798

- Notification must be provided in the most expedient time possible without delay, with pending law enforcement investigation being an exception to this requirement.
- Notification must occur through one of the following methods:

1) Written notice (i.e. letter)
2) Electronic Notice (requires consistency with ESign legislation)
3) Substitute notice via e-mail, website posting or announcement or notification via statewide media (used when cost of providing notice exceeds $250K, or whether the class of impacted consumers exceeds 500K, or where the agency does not have sufficient contact information)

Non Compliance Fines and Penalties Under CA Civil Code 1798

- Injured consumers can bring a civil legal action to recover damages.
- Injured consumer's rights and remedies are cumulative with other rights and remedies that are available under law.
- Businesses that violate, propose to violate or have violated this regulation can be subject to injunction.

Proposed Federal Security Breach Consumer Notification Bills

- **Notification of Risk to Personal Data Act (S751)** (Senator Feinstein Bill).
- Largely modeled after CA Civil Code 1798 with heavy bipartisan support.
- Burden of proof on the party required to notify and to demonstrate that the notifications were made in a timely manner.
- Notification must occur following the discovery of the breach of security of the system, or where corrective measures have been taken to prevent further disclosures and restore the integrity of the data system, or where written notice from law enforcement is provided indicating that notification will no longer seriously impede the investigation.
- Contains enforcement provisions for the FTC and State Attorney Generals.
- Excludes some good faith and at national security or law enforcement investigative activity from notification requirement.
- Has a preemptive effect on any inconsistent State or local laws.

Provisions of Proposed Notification of Risk to Personal Data Act

- "Personal information" includes: Social Security Number, drivers license or state identification number, account number or credit or debit card number, along with password, security code or access code to the individual's account.
- "Breach of security of the system" means the compromise of the security, confidentiality or integrity of data that results in, or if there is a reasonable basis to conclude has resulted in, the unauthorized acquisition of personal information maintained by a person or business and which does not include good faith acquisition.

Provisions of Proposed Notification of Risk to Personal Data Act – Cont'd

- Notification Methods can be written, via e-mail or through "Substitute Notice" which includes conspicuous Internet postings on public websites or notification to major print or broadcast media in area where the injured party resides.
- Notification must contain a description of the categories of information that was, or was reasonably believed to have been acquired by an unauthorized person and a toll free number where the injured consumer can determine whether their personal data was included in the security breach.
- Notification also includes the toll free numbers and contact information for the major credit reporting bureaus.

Provisions of Proposed Notification of Risk to Personal Data Notification Act – Cont'd

- Civil Money Penalty Provisions: Violators are subject to fines of up to $1,000 per individual and up to $50,000 per day while the failure to give the required notice occurred. These rights and remedies are in addition to others available under law.
- Designates the FTC as the appropriate regulator to enforce this Act and is empowered to assess applicable fines.
- Provides the State Attorney Generals with the enforcement power to bring actions on behalf of injured state residents in either state or federal district court.
- Proposes language to amend the Fair and Accurate Credit Transaction's act (FACTA) Section 605(A)(b)(1) to indicate the receipt of consumer notification under this act provides a basis to request a fraud alert on the injured party's credit bureau file.

Other Current Bills Related to Identity Theft on Capitol Hill

- **Information Protection and Security Act** (HR 1080 and S 500) – introduced to regulate information brokers and create individual rights with respect to personally identifiable information.
- **Social Security Number Misuse Prevention Act** (S 29) – introduced to limit the misuse of Social Security Numbers, to establish criminal and civil money penalties for such misuse and for other purposes including federal injunctive authority.
- **Privacy Act of 2005** (S 116) – Introduced by Senator Feinstein to require the consent of an individual prior to the sale and marketing of such individual's personally identifiable information, and for other purposes such as limits on providing protected health information and drivers license privacy.

Other Current Bills Related to Identity Theft on Capitol Hill – Cont'd

- **Comprehensive Identity Theft Prevention Act** (S 768)– Introduced to provide comprehensive identity theft prevention and creates a new category of "sensitive personal information which includes Social Security Number, medical condition or drug therapies, bank or investment account number information, credit or debit card information, individual payment history, state drivers license information or resident ID Number and other information deemed appropriate by the FTC. The bill also support the development of an Office of Identity Theft within the FTC.

Other Current Bills Related to Identity Theft on Capitol Hill – Cont'd

- **Personal Data Privacy and Security Act of 2005 (S1332)**
- Bipartisan bill promised by Senator Arlen Specter and Patrick Leahy which proposes a national version of the California notification law and requires US Businesses to make data security breaches public and **those that do not comply face criminal prosecution**. The bill also proposes limits on the trade in Social Security numbers by disallowing businesses from requiring consumers to reveal their Social Security number's in return for goods and services and Social Security number's cannot be sold without consumer permission.

What are the Risks Due to a Major Information Security Breach?

- Public notification to clients & consumers that could result in damage to brand and reputation
- Business contracts lost, delayed or not renewed
- Civil lawsuits, including class action suits
- FTC enforcement and sanctions
- Lost of shareholder value – shareholder lawsuits
- SEC sanctions

ACC's 2005 Annual Meeting: Legal Underdog to Corporate Superhero—Using Compliance for a Competitive Advantage

October 17-19, Marriott Wardman Park Hotel

What Actions are Companies Taking with Their Service Providers to Mitigate Risk of Information Security Breaches?

- More intrusive vendor audits
- Onsite inspections
- Onsite/remote testing
- More detailed questionnaires on information security procedures
- More audits/assessments
- More stringent requirements from partners/industry bodies
- Payment Card Industry Data Security Standards (PCI DSS) requirements annually

Additional Practical Measures to Mitigate the Risk of a Major Information Security Breach

- Encrypt data – local and server
- Keep sensitive data on servers, not on laptops
- Manage access to data and servers. Segregate productions systems from Corp network
- Depersonalize data whenever possible
- **Never** retain CCV data
- Never use or retain data for out of contract purposes
- Never transport, access or process data across borders without a legal review.

Conclusion

- Post Enron & WorldCom: Expedited enactment of Sarbanes-Oxley legislation to address corporate governance and accounting firm scandals.
- Post ChoicePoint, Lexis-Nexis & Bank of America: Expedited national legislation to require security breach consumer notification to help affected consumers better exercise current FACTA ID fraud alert to credit bureaus to mitigate harm and to allow for the Federal Trade Commission's regulation of the data broker industry.

European Data Privacy

Paula Barrett

Partner, Eversheds LLP

This presentation is for informational purposes only and does not constitute as legal advice. You should seek counsel to assess the implications of the legislation discussed in this presentation on your company's specific operations.

Why Should Your Board Care?

- Can apply to US Companies:
  - Where an individuals personal information is processed by or on behalf of that US Company using equipment located in the EEA
  - Where the US company has an office, branch or agency in the EEA or acquires a corporate entity within the EEA which is processing individuals personal information
- Impact of not complying:
  - Liability for loss (damage/distress)
  - Fines
  - Data may have to be destroyed, cleansed or cannot be used in evidence
  - Complaint to Commission or local regulatory authority
  - Bad publicity
  - Bad employee relations
  - Disruption to corporate transactions/company value damage
  - Lost Contracts – EEA Customers will demand compliance

Starting Compliance Programme

- Take “bites” from the “elephant” – don’t devour at once!
- Assemble team – Legal, HR, Marketing, IT
- Conduct audit/review – know what you do with personal information
- Build plan from ground upwards – policy should reflect reality
- Divide programme in to streams e.g. Employee Data, Marketing Data, Customer Data and Supplier Data
- Registration/Notification – failure to register can be criminal offence
- Training
  - how deep does it need to go
  - Maintain consistency and records

Some Basics

- The EU Directive applies to the processing of personal data
- In summary "personal" data means:
  - you can identify living person from it e.g.. contains their name, photo, voice; or
  - can identify living person from it + other data in employer's possession e.g.. contains a home address, an identity number, relates to incident involving the individual
- "Data" includes information …
  - being processed electronically/by computer
  - manual records in a structured filing system
- "sensitive" personal data
  - personal data which refers to racial/ethnic origin, religious or philosophical beliefs, political opinions, trade union membership, health or sexual life

Controller's Duties – Key Principles

- Personal Data must be:-
  - processed fairly and lawfully
  - collected for specified, explicit and legitimate purpose and not processed further in an incompatible way
  - adequate, relevant and not excessive
  - accurate and, where necessary, kept up to date
  - not kept for longer than necessary
  - processed in accordance with individuals rights
  - secured against accidental or unlawful loss, alteration or unauthorised disclosure, access or other processing.

Fair & Lawful Processing (Principle 1)

- To process personal data, must satisfy one of the specified legitimate criteria (Art. 7)
  - e.g. unambiguous consent of data subject, processing necessary for performance of contract with data subject, processing necessary to comply with legal obligation, processing is in legitimate interest of controller
- If sensitive personal data, must also satisfy criteria in Art. 8
  - e.g. have explicit consent (usually in writing), necessary for performance of legal right in employment context, protecting vital interests of data subject
  - N.B. in some countries e.g. Portugal also need approval of regulatory authority

Employee Data

- Documentation and Process Review to include:
  - Advertising and Applications Forms
  - Ad hoc job enquiries responses
  - Employee Contracts
  - Consent wording – where required
  - Staff handbooks
  - File Management
  - Monitoring Activity
  - Information Flows
  - Third Party Involvement
- Additional Policy creation:
  - Data Protection Policy re handling of staff data
  - Information Retention and Destruction Policy
  - IT Policy – sections on monitoring & security
  - Access Request Procedure

Vacancy Advertising and Applications

By way of example:

- Identify to whom the information will be provided:
  - name of employer (including any group companies)
  - any recruitment agency
- Identify how the information provided will be used (unless self evident)
- Consider whether appropriate to use the same application form for every job
- Only seek relevant personal data
- Only request information about criminal convictions if justified in terms of role offered
- Secure method of sending in applications
- Policy for applications sent 'on-spec'
- Vetting – wait until appropriate time and only if proportionate

Monitoring vs Data Privacy

- Complex Legal Framework – varies from Country to Country
  - Data Protection legislation
  - Labour law
  - Human Rights
  - "Spying" controls – particularly if interception of communication involved
- Common theme – information should be provided about potential monitoring

Security

- Take appropriate steps to secure against unauthorised loss, destruction or misuse
- Have regard to "state of art" – moving feast
- Sensitive information and financial information – likely to be higher threshold
- Italy – separate security policy has to be filed with authorities
- No express obligation flowing from Directive to inform individuals of security breach
- Argument that should disclose under fair and lawful processing principle

Marketing

- Understand what data you collect and what you do with it
- Common mistake to assume b2b communication not covered
- How do you communicate – emails and SMS more tightly controlled.
- Opt In/Opt Out – are you using the correct approach to collect consent
- Impact of Privacy and e-commerce Directive
  - Opt in consent for email and SMS unless satisfy exceptions
  - Check mailing and telephone contact lists against preference agency registers
- Check the scope of consents obtained are correct
- Think long term when drafting consents
- Sharing of databases – be careful – have you got consent?
- Buying databases – get assurances but YOUR responsibility
- Selling databases – consent is king
- Cleansing databases

Customers

- Do you handle personal data owned by customer
  - Remember accessing it incidentally also covered
- Do you simply use it to provide service back to customer
  - If yes probably acting as "processor"
  - If no probably a controller to controller transfer
- In most EU countries obligations fall on controller more than processor. Some exceptions e.g. Ireland.
- As minimum Customer will require security obligations in contract with you
- Many will ask you to sign EU Model Clause Processor Agreement

Transfer outside of EEA

- Transfer outside of EEA prohibited if recipient country doesn't have adequate protection.
- EEA? - EU and Iceland, Liechtenstein and Norway
- The EU Commission decides whether a country has adequate protection
- Currently (18/7/2005)
  - Hungary
  - Switzerland
  - US companies signed up to "Safe harbor"
  - Canada though not entirely (see http://www.europa.eu.int/comm/internal_market/privacy/adequacy/adequacy-faq_en.htm#1)
  - Argentina (as of 30 June 2003)

Transborder Transfer Mechanisms

- Does derogation apply?
  - Data subject consents (not all countries allow e.g. France)
  - Necessary to perform contract with data subject
  - Necessary for conclusion or performance of contract with third party concluded in interest of individual
  - Necessary for establishing, defending or exercising legal claims
  - Necessary to protect vital interests of the individual
- Consider other practical steps e.g. can data be anonymised before transfer
- If exemption doesn't apply need other means of ensuring adequacy:
  - Self Assessment of Adequacy
  - US Safe Harbor Registration
  - EC Model Clause Contract
  - EC Approved Binding Intra Group Rules

Safe Harbor

- US only
- Not all sectors covered
- Annual audit and certification
- Potential for class actions
- Investigation and Fines from FTC
- Low take up
- Does not cover "processor" transfers
- Consider applying where large amount of transfers
- Simplicity when dealing with third parties

EC Model Contracts

- Controller to Processor and Controller to Controller versions
- Simplicity of solution key advantage here but:
  - "Euro speak"
  - onerous e.g. enforceable by third parties
  - can't modify them
- New Versions released earlier this year – more business friendly
- Other models have been approved for use e.g. ICC
- Problems in volume of paper for large groups
- No processor to processor versions – headaches for service providers and their subcontractors

Binding Corporate Rules

- New Solution - only applicable for intra-group transfers
- The rules must
  - be binding internally & externally
  - be legally enforceable by data subjects & data protection authorities
  - contain a duty to inform the data protection authority if a member of the corporate group may be unable to fulfil its obligations, if this will have a substantial effect
- Problem - Individual Approval by Commission or Member State data protection authorities. "Home" authority to act as single point of contact.
- Selected Group co. in EU liable for rest of group's compliance
- Good idea but not yet implemented

Round Up

- Don’t ignore – Authorities building enforcement capability
- Obtain Board Buy-in
- Build Team – DP Champions
- Build Compliance Programme
- Try to do some sort of audit/review first
- Do get local law advice – Directive isn’t the full story
- Implement in Streams
- Decide on Transborder transfer mechanism
- Train Staff/Inform them of policies created
- Live the policies – culture of compliance