SIDLEY AUSTIN LLP

SIDLEY

BEIJING BRUSSELS CHICAGO DALLAS FRANKFURT GENEVA HONG KONG LONDON LOS ANGELES NEW YORK SAN FRANCISCO SHANGHAI SINGAPORE SYDNEY TOKYO WASHINGTON, D.C.

The Privacy Symposium – Cambridge, MA

Alan Charles Raul
August 23, 2007

Overview

- Where are we on privacy?
- What is privacy?
- Is privacy enough?
- Why worry about it?
- Where do we go next?
- Some observations on law and enforcement
- What litigation standards apply?
- Lack of privacy injury?
- Rationalization of legal regimes?
- Building an effective privacy and information management culture

Where are we on privacy?

- US Federal Government (1973 HEW principles, Privacy Act)
- EU (1995 Data Protection Directive)
- Industry regulators (Telecom/CPNI, GLB, HIPAA)
- FTC (Do Not Call, deceptive and unfair practice enforcement)
- Doubleclick
- California (Constitution, data breach notification law, myriad requirements)
- Data breach epidemic
- Government surveillance
- Amazon, Google (knowing users' interests)
- ChoicePoint, TJX
- The public?
  - Credit monitoring?
  - eHealth records
  - Personalization (targeted marketing?)
  - System reliability

What is privacy?

- Preventing personal information from being used or abused to impose:
  - Dollar losses
  - Dignity losses
    - Embarrassment and reputation
    - Loss of control over decisions, solitude, image
  - Disruption and disturbance
    - Inundation with marketing
    - Bothersome telephone calls
    - Physical searches
  - Denial of jobs, insurance, medical coverage
  - Government intrusions on liberty, autonomy, tranquility
  - Are there illusory privacy interests to be eschewed?

Is privacy enough?

- Do current privacy regimes focus on the harms or are they too abstract and bureaucratic?
- Is “privacy” too narrow a concept
- Going forward, will new angles take equal prominence?
  - Information security
  - Data retention: how long and who can retrieve?
  - Cybersecurity (network and infrastructure protection)
  - Data ownership among various stakeholders even beyond the data subjects
  - Litigation and “white collar” privacy

Where do we go next?

- Federal legislation?
- International "restatement" of core principles of privacy, data protection, and information around the world?
  - What is "restatement" of law: "clarification and simplification . . . better adapt[ed] to social needs"
  - Don't wait for governments . . . industry/academics/advocates will/should/may develop and help implement "restated" privacy law and let regulators catch up
- EU to refocus on preventing real privacy harms?
- International Internet dispute and consumer redress?
  - OECD already working on
- Privacy enhancing technologies
- Responsibility to defend against cybercrime
- Get public to adopt pro-privacy culture?

Categories of Data

Individuals
- Employees
- Job applicants
  - Background checks
  - Immigration status
- Customers
- Students
- Employees of clients
- Vendors
- Competitors

Online/websites

Health/medical

Financial information

Client data

Marketing

Credit/payment card data

Litigation/investigation data

IP

Trade secrets

Others

Sample Universe of Data Issues

- EU and global data protection
- Information security
- Consumer data
- Business data
- Employee/HR data
- Online/internet issues
- International data transfers
- HIPAA (medical/health/pharmacy)
- Data ownership
- Assuring convenient access to personal data
- Inter-company agreements allocating rights and responsibilities
- Workplace privacy
- CAN SPAM
- Telephone and fax
- Online marketing
- Behavioral targeting
- Outsourcing information processing
- Cybercrime exposure
- eDiscovery/investigations
- Records retention
- Expunging data/persistence of data
- Network security
- Legacy system issues
- Response to government requests

Domestic Privacy

- United States
  - Sector-specific, multi-faceted approach; no one overarching privacy law
  - Financial institution regulation under Gramm-Leach-Bliley Act
  - Regulation of personally identifiable health information under HIPAA
  - Duty to assess internal controls under Sarbanes-Oxley §404
  - Information security obligations imposed by various laws, regulators, liability decisions and business imperatives
  - FTC unfair or deceptive trade practices enforcement – failure to employ reasonable and appropriate security measures; violations of company privacy promises
  - Numerous state statutory requirements – data breach notification, security requirements, disposal requirements
  - State Attorneys General
  - Workplace monitoring/employee privacy
  - Negligence and invasion of privacy tort claims

International Privacy

- European Union
  - EU Data Protection Directive provides principles for privacy, security, access, onward transfer of personally identifiable information in the EU
  - Limits collection, processing, and retention of personal data
  - Allows onward transfer of personal information only to countries that provide “adequate” protection – this does not include the U.S.
  - Any corporation operating in the EU is automatically subject to the EU Data Protection Directive
  - EU Electronic Communications and Privacy Directive also contains relevant restrictions, most importantly on requirements for marketing
  - EU Directive is only a baseline; Member state laws must be considered
  - Employee/workplace privacy governed by labor relations requirements in various countries (works council involvement)

More international

Canada

- Personal Information Protection and Electronic Documents Act (PIPEDA)
  - Requires individual consent to the collection, use, and disclosure of personal information
  - mandates consumers' right to access, challenge, and seek corrections of information
  - requires physical safeguards on information such as
- ***Canada's PIPEDA has been deemed by the EU to provide an adequate level of protection***

More International

- Japan
  - Adopts elements of both the EU and U.S. approaches
  - Omnibus privacy law, enforced by various Ministries, who are free to issue their own, differing regulations
  - Five general requirements – specify purpose for data collection and limit use to that purpose, only gather personal data by lawful and appropriate means, transparency in the collection and use of personal data, maintain accuracy of data, protect data's security
  - Requires notification of security breaches to affected individuals and appropriate government bodies
  - Law provides for private causes of action
  - No bar on U.S.-Japan data transfers
  - Japan's law has not been deemed by the EU to provide an adequate level of protection

More International

- APEC
  - More self-regulatory, practical approach to privacy that weighs the benefits of privacy against its costs
  - Nine information privacy principles – preventing harm, notice, collection limitation, use of personal information, choice, integrity of personal information, security safeguards, access and correction, accountability
  - Allows for differing implementation of the principles among APEC countries, including adoption of exceptions

Privacy conflicts

- U.S. subsidiaries of foreign parent companies could be compelled to produce records held in the U.S. or in foreign offices.
- Foreign Governments have expressed concern that the Patriot Act will compromise the non-U.S. citizens' data.
  - Law enforcement access to personal information is inevitable, but does subpoena compliance team consult the privacy team?
- Litigation and internal investigation data transfers

What can go wrong?

- ChoicePoint – FTC obtained record $10 million fine and $5 million restitution, plus substantial injunctive requirements; $500,000 settlement with 43 state AGs; $12 million spent on security upgrades since 2005
- TJX: computer intrusion and stolen customer transaction data leads to government investigations and scores of putative class actions around US and Canada (46 million customers)
- Monster.com: 1.6 million job searches compromised by Trojan horse and phishing attacks
- HP "pretexting" investigation of Board members and journalists
- Telefonica Espana – fined €840,000 by the Spanish Data Protection Authority for sharing an individual's data with one of its subsidiaries for marketing purposes
- Tyco Healthcare – fined €30,000 ($40,972) by the French Data Protection Authority (CNIL) for improper storage and cross-border transfer of employee data (April 2007)

$50 Million Damages

- Florida bank recently ordered by a federal court to pay more than $50 million in damages for violations of federal Driver Privacy Protection Act
- Bought 650,000 names and addresses from the Florida DMV
- Bank paid only $5,656
- Used the names for car loan solicitations
- Federal appellate court already held that these Plaintiffs need not prove any actual damages

Kehoe v. Fidelity Federal Bank and Trust (S.D. Fla.)

FTC Standard for Security

- "In our investigations, we look at the overall security system that the firm has implemented and its ***reasonableness*** in light of the size and nature of the business, the nature of the information it maintains, the security tools that are available, and the security risks it faces. I emphasize that the standard is 'reasonableness,' not perfection.... [T]his is not a game of ***'cybersecurity gotcha'*** – we are not trying to catch companies with their digital pants down; rather, we are trying to encourage companies to put their data security defenses up."

– FTC Chairman Deborah Platt Majoras May 10, 2006

FTC "Deception" Cases

- *Eli Lilly & Co.*, FTC Docket No. C-4047 (May 8, 2002)
  - Individuals taking Prozac registered at an Eli Lilly web site for automated e-mail reminders to take their dose; e-mail sent to subscribers contained e-mail addresses of all subscribers
- *Microsoft Corp.*, FTC Docket No. C-4069 (Dec. 20, 2002)
  - Misrepresentations of the privacy and security of the company's Passport Internet sign-on service; service did not provide the required security to store sensitive user information and collected more personal information than stated in Microsoft's privacy policy

FTC "Deception" Cases

- *Guess?, Inc.*, FTC Docket No. C-4091 (July 30, 2003)
  - Personal information on company's website was not stored in an unreadable, encrypted format in violation of company's privacy policy and making information vulnerable to hackers
- *MTS Inc., d/b/a Tower Records/Books/Video*, FTC Docket No. C-4110 (May 28, 2004)
  - Security flaw in company's website allowed users to access order history records and view personal information about other Tower customers
- *Petco Animal Supplies, Inc.*, FTC Docket No. C-4133 (Mar. 4, 2005)
  - Violated company privacy promises because of website security flaws that rendered customer information vulnerable to hackers

FTC Attention To Information Security

- More recently, FTC has used its authority under the **"unfairness"** standard to bring cases in the area of data security
  - "Unfair" practices are those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably outweighed by countervailing benefits to consumers or competition and cause injury that consumers could not have reasonably avoided"
  - unfairness standard can be violated without any affirmative statement or promise of security; turns on reasonable industry practices that consumer can rely on

FTC "Unfairness" Cases

BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (June 16, 2005)

- company failed to employ reasonable and appropriate security measures to prevent unauthorized access to credit and debit card information collected from customers at its stores
- creates a general duty on everyone to protect personal information with reasonable security practices

FTC Attention To Information Security

The *BJ's Wholesale decision* "should provide clear notice to the business community that failure to maintain reasonable and appropriate security measures in light of the sensitivity of the information can cause substantial consumer injury and violate the FTC Act."

– FTC Chairman Deborah Platt Majoras (August 6, 2005)

FTC "Unfairness" Cases

- *United States v. ChoicePoint, Inc.*, No. 106-CV0198 (N.D. Ga. Feb. 15, 2006)
  - No reasonable procedures to screen prospective subscribers; failure to tighten application approval procedures or monitor subscribers after receiving subpoenas from law enforcement

Consequences of ChoicePoint FTC Case

- FTC obtained record $10 million fine and $5 million restitution, plus substantial injunctive requirements
- ChoicePoint now must establish, implement and maintain a "comprehensive information security program that is reasonably designed to protect the security, confidentiality, and integrity of personal information collected from or about consumers"
- ChoicePoint must submit to biennial assessments from an independent third party of its security program, with reports submitted to the FTC, through the year 2026
- Unwanted media, regulatory, prosecutorial and plaintiffs' lawyer attention

Other FTC "Unfairness" Cases

- *CardSystems Solutions, Inc.*, FTC Docket No. 052-3148 (Feb. 23, 2006)
  - Failure to take appropriate security measures in "authorization processing" (obtaining approval for credit and debit card purchases from the banks that issued the cards) resulted in millions of dollars in fraudulent purchases and was an unfair practice
- *DSW, Inc.*, FTC Docket No. C-4157 (Mar. 7, 2006)
  - Data security failure allowed hackers to gain access to the sensitive credit card, debit card, and checking account information of more than 1.4 million customers

And the FTC's newest case…

Guidance Software, Inc., FTC File No. 062-3057 (Nov. 11, 2006)

FTC said that the company "engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive personal information stored on its corporate network."

(1) stored information in clear readable text;

(2) did not adequately assess the vulnerability of its web application and network to certain commonly known or reasonably foreseeable attacks;

(3) did not implement simple, low-cost, and readily available defenses to such attacks;

(4) stored in clear readable text network user credentials that facilitate access to sensitive personal information on the network;

(5) did not use readily available security measures to monitor and control connections from the network to the internet; and

(6) failed to employ sufficient measures to detect unauthorized access to sensitive personal information.

California leads the way…

First state to have an agency dedicated to promoting and protecting the privacy rights of consumers

California Privacy Laws

OFFICE OF
Privacy
Protection

- California Constitution, Article 1, section 1
- Office of Privacy Protection - California Business and Professions Code sections 350-352
- Automobile "Black Boxes" Vehicle Code section 9951
- Birth and Death Certificate Access - Health and Safety Code sections 103525, 103525.5, 103526, 103526.5, 103527, and 103528
- Birth and Death Record Indices - Health and Safety Code sections102230, 102231 and 102232
- Cellular Telephone Number Directory – Public Utilities Code section 2891.1
- Computer Spyware – Business and Professions Code section 22947 et seq.
- Consolidation of Identity Theft Cases - Penal Code section 786
- Consumer Credit Reporting Agencies Act Civil Code section 1785.1-1785.36
- Court Records: Protection of Victim and Witness Information – Penal Code section 964
- Credit Card Address Change - Civil Code section 1747.06
- Credit Card/Telephone Service Address Change, Civil Code section 1799.1b
- Credit Card or Check Payment- Civil Code sections 1725 and 1747.8
- Credit Card Full Disclosure Act, Civil Code sections 1748.10 - 1748.12
- Credit Card Number Truncation - California Civil Code section 1747.9
- Credit Card “Skimmers” - Penal Code section 502.6.
- Credit Cards, Substitutes - Civil Code section 1747.05.
- Debt Collection: Identity Theft Victim Rights - Civil Code section 1788.18.
- Destruction of Customer Records - California Civil Code sections 1798.80 and 1798.84
- Driver’s License Information Confidentiality - Vehicle Code sections 1808-1821
- Driver’s License Information, Scanning or "Swiping" - Civil Code section 1798.90.1
- Electronic Eavesdropping - Penal Code sections 630-637.9
- Electronic Surveillance in Rental Cars – Civil Code section 1936
- Employment of Offenders - Penal Code sections 4017.1 and 5071 and Welfare and Institutions Code section 219.5.
- Fair Debt Collection Practices Act, Civil Code sections 1788-1788.33
- Financial Information Privacy Act, California - Financial Code sections 4050 - 4060
- Identity Theft: Victim Access to Records on Fraudulent Transactions or Accounts - California Civil Code section 1748.95, California Financial Code sections 4002 and 22470
- Identity Theft - California Penal Code sections 530.5-530.8

SIDLEY AUSTIN LLP
SIDLEY

California Privacy Laws

OFFICE OF
Privacy
Protection

- Identity Theft Victim's Rights Against Claimants - Civil Code section 1798.92-1798.97
- Information Practices Act of 1977- California Civil Code section 1798 et seq.
- Information-Sharing Disclosure, "Shine the Light" – Civil Code sections 1798.82-1798.84
- Insurance Information and Privacy Protection Act, Insurance Code section 791 et seq.
- Investigative Consumer Reporting Agencies Act, California Civil Code sections 1786-1786.60
- Legal and Civil Rights of Persons Involuntarily Detained - Welfare & Institutions Code section 5328
- Library Records, Confidentiality - Government Code sections 6254, 6267 and 6276.28
- Mandated Blood Testing and Confidentiality to Protect Public Health - California Health & Safety Code sections 120975-121020
- Medical Information, Collection for Direct Marketing Purposes – Civil Code section 1798.91
- Medical Information Confidentiality - California Civil Code sections 56-56.37
- Online Privacy Protection Act of 2003 - Business & Professions Code section 22575-22579
- Patient Access to Health Records - California Health & Safety Code section 123110 et seq.
- Personal Information Collected on Internet - California Government Code section 11015.5
- Public Records Act - California Government Code sections 6250-6268
- Search Warrant, Penal Code section 1524
- Security Breach Notice - Civil Code sections 1798.29 and 1798.82 - 1798.84
- Security of Personal Information – Civil Code section 1798.81.5
- Social Security Number Confidentiality - California Civil Code sections 1798.85-1798.86, 1785.11.1, 1785.11.6 and 1786.60
- Social Security Number Confidentiality in Family Court Records - California Family Code section 2024.5.
- Social Security Number Truncation on Pay Stubs – Labor Code section 226
- Spam Laws - Business and Professions Code sections 17529 and following and 17538.45
- State Agency Privacy Policies, Government Code section 11019.9
- Statute of Limitations, Penal Code section 803
- Supermarket Club Card Act - Civil Code section 1749.60 and following
- Telecommunications Customer Privacy - Public Utilities Code sections 2891-2894.10
- Telemarketing: State do-not-call list - Business and Professions Code sections 17590-17594
- Unsolicited Cell Phone/Pager Text Ads - Business and Professions Code section 17538.41
- Veterans' Discharge Papers, Notice of Public Record Status - California Government Code section 27377
- Warranty cards - Civil Code section 1793.1

SIDLEY AUSTIN LLP
SIDLEY

California leads the way…

- Online Privacy Protection Act

  Cal. Bus. & Prof. Code 22575-22579

  - requires conspicuous posting of a privacy policy, and compliance with that policy
  - applies to an operator of a commercial web site or online service that "collects and maintains personally identifiable information from a consumer residing in California who uses or visits" such web site or online service
  - enforcement through state unfair competition statute

California leads the way…

- Online Privacy Protection Act – national implications
  - companies with an online presence have their privacy policies available from a link on the homepage of their web site
  - privacy policies are developed with the criteria of OPPA in mind:
    - list of categories of personally identifiable information collected
    - list of categories of third-parties with whom operator may share such personally identifiable information
    - description of process by which consumer can review and request changes to personally identifiable information
    - description of process by which operator notifies consumers of material changes to the operator's privacy policy
    - effective date of privacy policy

California leads the way…

- "Shine the Light" Law

  Ca. Civ. Code 1798.83-1798.84

  – requires certain businesses, upon request, to disclose to customers the entities with whom they have shared personal information for marketing purposes within the last 12 months

  – must provide instructions about how to make disclosure request

  – companies that have a privacy policy that allows for opt-in or opt-out of the sharing of personal information need not provide the disclosure

  – penalties for non-compliance

State Affirmative Security Obligations

- California AB 1950
  - requires specified businesses to use safeguards to ensure the security of Californians' personal information
  - includes name plus SSN, driver's license/state ID, or financial account number
  - vendors and other third parties must be contractually required to do the same
  - does not apply to businesses that are subject to other information security laws, such as the federal financial and medical information security rules
- Arkansas, Nevada, Rhode Island, others following…

State Attorneys General

- Andrew Cuomo, New York
  - settled a claim against CS STARS LLC under New York's data breach notification law for the company's failure to provide required notifications of a breach involving approximately 540,000 New York consumers for **seven weeks** after the breach was discovered (April 2007)
- Bill Lockyer/Edmund Brown, California
  - *Optin Global* joint California/FTC effort resulted in a $2.4 million settlement of allegations that company directed individuals and businesses to unlawful email ads that pitched mortgage services, car warranties, travel deals, prescription drugs and college degrees
  - *Hewlett Packard* pretexting investigation, indictments

State Attorneys General

- Marc Dann, Ohio
  - first state to sue DSW over data breach resulting in the access of personal information on DSW's computer system
    - led company to establish reserve of between $6.5 and $9.5 million, in part to address Ohio AG complaint that company failed to notify 700,000 Ohio consumers that personal information was compromised
  - Identity Theft Verification Passport Program to assist in the rehabilitation efforts of Ohio citizens who had been victims of identity theft

U.S. Private Litigation

- Causes of action
  - State data breach notification statutes
  - Electronic Communications Privacy Act (unauthorized interception or stored communications)
  - Computer Fraud and Abuse Act (unauthorized access to computers)
  - State unfair and deceptive acts/practices (UDAP) statutes
  - Sate common law, privacy torts and negligence
- Unresolved issues
  - Preemption
  - Contract or Tort
  - Strict Liability or Negligence
  - Standard of Care
  - Injury/Standing?

Lack of Privacy Injury?

- *Barber v. Overton* (6th Cir. 8/2/07): Government disclosure of SSN does not rise to level of constitutional injury
- *Randolph v. ING Life Insurance & Annuity Co.* (D.C. June 13, 2007)
  - ING employee took computer home with personal and financial information of DC government employees; ING employee's home was burglarized, computer stolen
  - Plaintiffs' claimed injury as a result of their "heightened risk of identity theft" caused by ING's negligence in allowing their personal information to be stored on an employee's computer and removed from otherwise secure facilities
  - Court: "Fear of future harm, even if reasonable, is simply not the kind of concrete and particularized injury, or imminent future injury, courts will recognize as a basis on which to bring an action"

Injury?

- *Kahle v. Litton Loan Servicing LP* (S.D. Ohio May 16, 2007)
  - computer equipment stolen from Litton's facility containing personal information of 229,501 individuals
  - Plaintiff claimed Defendant was negligent
  - Court agreed that Defendant owed Plaintiff a duty and that duty was breached, but no injury resulted
  - Court: time and money spent monitoring Plaintiff's credit was not the result of any present injury, but was in anticipation of potential future injury that had not materialized

Injury?

- *Guin* v. *Brazos Higher Education Service Corporation, Inc.* (D. Minn. February 7, 2006)
  - laptop that contained unencrypted information was stolen during a burglary of an employee's home
  - Court found no evidence that Brazos violated its duties under GLB or its commitments made in its privacy policy
  - No evidence of any actual identity theft or other injury, or even that burglars targeted the personal information on the laptop, as opposed to the laptop itself
  - Laptop theft was not reasonably foreseeable and thus proximate cause is not established

Injury?

- *Stollenwerk* v. *TriWest Healthcare Alliance* (D.Ariz. 2005)
  - no harm from the mere presence of personal information on stolen computer hard drives
- *Smith* v. *Chase Manhattan Bank* (N.Y. App. 2002)
  - no harm from unwanted solicitations
- *Conboy* v. *AT&T Corp*. (2d Cir. 2001)
  - no presumption of emotional distress, and other similar damages cannot be presumed from disclosure of personally identifiable information, absent some concrete evidence of demonstrable harm

Calls for comprehensive federal legislation

Consumer Privacy Legislative Forum – organized to "to support a process to consider comprehensive consumer privacy legislation in the United States"

Eastman Kodak Co.	Intel Corp.
eBay Inc.	Microsoft
Eli Lilly and Co.	Oracle Corp.
Google, Inc.	Procter & Gamble Co.
Hewitt and Associates	Sun Microsystems, Inc.
Hewlett-Packard Co.	Symantec Corp.

Common standards for privacy in the US

"The growing focus on privacy at both state and federal levels has resulted in an increasingly rapid adoption of well-intended privacy laws that are at times overlapping, inconsistent and often incomplete. This is not only confusing for businesses, but it also leaves consumers unprotected. A single federal approach will create a common standard for protection that consumers and businesses can understand and count on."

Brad Smith, Senior Vice President & General Counsel, Microsoft

Restatement of international privacy and information law

- Why not?

Building an effective culture of privacy and information management

- Regularly require honest assessment of risks to corporate operations and identify threats and vulnerabilities
- Establish corporate policies governing information usage and employee conduct
- Incorporate best practices and standards, and monitor legal and technological developments
- Ensure sufficient funding is allocated to develop and maintain an enterprise-wide program
- Reinforce the culture through education, training and measuring compliance with meaningful metrics
- Watch over your business partners
- Conduct regular reviews and audits

Contact Information

Alan Charles Raul
Sidley Austin LLP
1501 K Street NW
Washington, DC 20005
202.736.8477
araul@sidley.com

SIDLEY AUSTIN LLP
SIDLEY