Citation Key

for more information see: http://open.umich.edu/wiki/CitationPolicy

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }

Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)

Public Domain – Expired: Works that are no longer protected due to an expired copyright term.

Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.

Creative Commons – Zero Waiver

Creative Commons – Attribution License

Creative Commons – Attribution Share Alike License

Creative Commons – Attribution Noncommercial License

Creative Commons – Attribution Noncommercial Share Alike License

GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }

Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }

Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

Approaches by Other Jurisdictions

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 3

US and States

- General consumer protection laws
  - Broad and varied application
- 48 states have breach notification laws; also DC, NYC, VI, and PR
  - All cover financial data; some cover medical
  - Vary in form of notification
  - Vary in verification of notification
  - Vary in required consumer recovery assistance programs
- Do Not Spam databases – UT, MI
- Conflicts – US law usually preempts

Some Common Elements

- Personally identifiable information
- Exemptions if data encrypted
  - Check encryption definition
  - No exemption if PIN included
- Delay notice at LE request
- Allowable forms of notice
- Most have some exemption if company covered by federal law such as GLBA or HIPAA

Coverage Issues to Check

- Triggers
  - Access; accessed and “used”
  - Disclosed
  - Likely/unlikely to have been used
  - Harm likely/unlikely
  - Who makes determination
- Whether applies outside jurisdiction
  - Outside companies
  - Outside consumers
- Provisions for third party data holders

RI ID Theft Protection Law

- "A business that owns or licenses computerized unencripted [*sic*] personal information about a Rhode Island resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information…."
- "whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person or a person…."

California as Pace Setter

- At least 79 privacy/security related laws between 1999 and the end of 2009
- Many laws affect all who interact with or have data about California residents
- Many laws blocking use, printing, or displaying of SSN
- Many laws helping identity theft victims

California Constitution

- *Article 1: Declaration of Rights*
  - *Section 1: All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and **privacy**.*

CA Law Examples

- SB 1386, 2002: must report any possible compromise of non-public financial information about a California resident
  - updated by AB 1950 2004 - must protect info
- SB 1298, 2008 extends to medical records
- AB 68, 2002: must publish privacy statements on web pages
- SB 27, 2004: companies must disclose with whom they share individuals' information and what info they share

More CA

- SB 1090, 2003: prohibits satellite providers from monitoring subscriber viewing habits
- AB 2840, 2004: limit use of electronic surveillance information by rental car companies
- SB 1436, 2004: prohibits unauthorized installation of spyware
- SB 355, 2005: prohibits phishing

MA Caught Up

- Insure the security and confidentiality of customer information in a manner fully consistent with industry standards
- Protect against anticipated threats or hazards to the security or integrity of such information
- Protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer

Major Provisions

- Paper and electronic
- Notify consumers and law enforcement
- Identity theft provisions extend beyond traditional PII and financial information
- Credit report security freeze
- Only state with GLBA-style security rule

MA Delays

- Regulations due to take effect 1/1/09
- Small business concerns and economy led to delay in enforcement and amendments
- Amendments due to become effective 3/1/10

Nevada

- Encrypt sensitive information during transmission

International

Background

US vs. US and US vs. World

- US
  - Patchwork of state and federal
  - Mostly by sector
  - Companies pushing for national standards
- Non-US
  - Mix of uniform/sector, local/national, none
  - Some push for global approach

International Considerations

- Culture
- Economy
- Socio-political context
- Language
- Control, management of personnel
- Laws
- Law enforcement
  - Extraterritorial jurisdiction
- Judicial system

Scope of Issues

- Website
- Foreign subsidiaries in US
- Foreign clients
  - Foreign clients
  - US clients with foreign subsidiaries
- Foreign distribution or foreign activities
  - Distributors; agents
  - Send US services offshore
- Services provided by third parties
  - Foreign service providers of the organization's US service providers

Convention on Human Rights (1950)

- European Convention on Human Rights
- Article 8
  - *"Everyone has the right to respect for his private and family life, his home and his correspondence"*

OECD Privacy Guidelines - 1980

- 8 principles
  - Collect data with individual's consent
    - Understand what data collected & can correct
  - Relevant to purpose and accurate
  - State purpose and limit use to purpose
  - No other use for data w/o individual's consent
  - Protect collected data
  - Disclose practices & policies of accessors data
  - Data holders held accountable for above

OECD Security Guidelines - 2002

- "Toward a Culture of Security"
  - Awareness
  - Responsibility
  - Response
  - Ethics
  - Democracy
  - Risk Assessment and reassessment
  - Security Design and implementation
  - Security Management

European Union

- 27 member states
  - 27 + legal systems
- Harmonized through directives, e.g.,
  - 1995 Data Protection Directive
  - 2002 E-communications Directive
  - 2006 Data Retention Directive
- Numerous important differences remain

EU Data Protection Directive – 1995

- Effective 1998
- Comprehensive approach to privacy
  - "*Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.*"
  - Passed at EU level, implemented by each country
- Wide latitude

Data Protection Directive Conditions

- Transparency - subject informed & gives consent or legally required, subject has access to data & can correct errors, data must be protected
- Legitimate purpose - processed only for specified, explicit and legitimate purposes
- Proportionality - processed only as much as needed for stated purpose
- Data only moved outside of EU to places that *'provide an adequate level of protection'*

US Safe Harbor

- US company self-certifies that they adhere to a set of 7 principles
  - Notice: inform individuals of data collected
  - Choice: must offer opt-out opportunity of some uses
  - Onward transfer: only to compliant organizations
  - Security: take “reasonable precautions” to protect
  - Data integrity: info must be relevant and accurate
  - Access: must have access to their own info
  - Enforcement: must have enforcement mechanisms

US Safe Harbor Adoption

- *"[a]n organization needs to self certify annually to the Department of Commerce in writing that it agrees to adhere to the safe harbor's requirements"*
  - (but only for their European customers)
- 1345 companies registered (12/24/2007)
  - (was 997 on 7/31/2006)
  - Many not current with self-certification

EU Directive on Privacy and Electronic Communications (2002)

- Ensure *"the right to privacy, with respect to the processing of personal data in the electronic communication sector"*
  - Protect the privacy of confidential data in transit and in storage
  - Users should be "offered the opportunity to refuse" a cookie
  - Data on subscribers can only be stored long enough to provide service
  - Prior consent for email marketing

APEC – Asia Pacific Economic Cooperation

- 21 member economies along Pacific Rim
  - 40% of world's population; 60% of world's domestic product. Includes US
- APEC Privacy Framework
  - Non-binding
  - 9 principles
    - Prevent harm
    - Notice
    - Choice
    - Uses of PII
    - Access and correction
    - Integrity
    - Security safeguards
    - Accountability
- Little progress in implementing

Cross-Border Law Enforcement

- Mutual Legal Assistance Treaty
  - Criminal only
  - Slow – 4-6 months
- Letters Rogatory
  - Diplomatic request to enforce US judicial order
  - No obligation
- Limited scope agreements
  - 24/7 Network Preservation Request
  - IAEAA
- US Safe-Web - 2006

SAFE-WEB Act - Cooperation

- Expressly confirms: 1) FTC authority to redress U.S. harm caused by foreign wrongdoers and harm abroad caused by U.S. wrongdoers; and 2) availability in cross-border cases of all remedies available to the FTC
- Permits the FTC to cooperate with DOJ in using additional staff and financial resources for foreign litigation of FTC matters
- Expressly authorizes the FTC criminal referrals when violations of FTC law also violate U.S. criminal laws
- Provides for foreign staff exchange arrangements and permits the FTC to accept reimbursement for its costs in these arrangements
- Authorizes the FTC to accept reimbursement for providing assistance to law enforcement agencies in the U.S. or abroad, and to accept gifts and voluntary services in aid of the agency's mission

SAFE-WEB Act – Data Protection

- Allows sharing of confidential information with foreign law enforcers, subject to appropriate confidentiality assurances
- Allows investigations and discovery in aid of foreign law enforcers
- Protects information provided by foreign enforcers from public disclosure if confidentiality is a condition of providing it

International

Emerging Issues

Data Protection Standards

- Private standards international in scope
  - ISO 27001 *et al* began as British standards
  - ISO, PCI-DSS
- Statutes could have extraterritorial effect
  - GLBA
  - OECD Security Guidelines

Security Breach

- International implications of data breach notifications
  - TJX has customers in US, UK, Canada
- Companies in UK and Greece have been fined for failure to disclose
- Many more countries examining such laws
  - None passed yet (AFAIK)

Data Retention

- US – minimum requirements
  - Varies with substantive areas; e.g., tax, telecommunications
- EU - maximum requirements
  - 2006 EU Retention Directive
  - Cannot keep personal data longer than needed

Data Retention/Disclosure

- US – retain and disclose
  - eDiscovery Amendments to Federal Rules of Civil Procedure require “good faith, reasonable approach” to retention and destruction
  - Data destruction could be problematic
- EU – limited retention and permission required for disclosure
  - Data protection laws

But….

- US – no legal requirement for ISPs to retain
- EU - considering minimums

Whistle Blowers

- SOX section 301 requires that companies establish anonymous hotlines
- Triggers non-US data privacy laws that don't allow anonymous data collection
  - EU – data subjects has right to know source of data collected about him/her

In the Real World

- Global cooperation
- Global privacy/security program with modifications to accommodate national and regional differences
- Use best practices and standards
- Seek common enforcement approach