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.

Public/Private Interrelation

510 - Data Security and Privacy: Legal, Policy, and Enterprise Issues
University of Michigan School of Information
Week 4

Interrelation

- Cooperation
  - NCFTA
  - CERT
- Private Standards Accepted
  - Safe Harbor
- Private Standards Adopted
  - PCI-DSS statutes

Substantive Areas

- National Security
  - Critical infrastructure attack
  - Espionage
- Private Security
  - Enterprise/Personal attack
  - Theft
- Privacy

National Security

- Homeland Security Act
  - Title II - Information analysis and infrastructure protection
  - Title VII – Coordination with other entities

HSA Title II

- Receive and analyze information
- Assess vulnerabilities
- Integrate to identify priorities
- Develop national plan based on priorities
- Take steps to protect
- Administer advisory system
- Review policies and procedures for information sharing

HSA Title II Scope

- Focuses on
  - "Critical infrastructure"
  - "Internet events"
- Information sharing involves only government entities

HSA Title VIII

- Public and private
- Information Sharing and Analysis Centers
  - Proven very valuable
  - Originally sector specific but broadened
  - Potential problems with
    - FOIA
    - Antitrust
    - Federal Advisory Committee Act
    - Disclosures affecting privacy and civil liberties

HSA Domestic Issues

- FOIA exemption for voluntary submission if CII
- Secrecy may lead to adverse public consequence
- ECPA exemptions
  - Imminent danger, good faith, all government levels
- Legitimate data mining can raise privacy concerns

HSA International Issues

- "Transnational terrorism" broadens definition of national security
- Share with foreign governments
- Similar steps in other countries
  - EU members can compel ISPs to log use
  - Swiss – record email date, time, sender, recipient
  - Spain – one year ISP data retention

Sharing Issues

- Government secrets
- Industry secrets
- Business concerns
- Antitrust laws

Government Secrets

- Disclose systems
  - Details
  - Existence
- Disclose data
  - Details
  - Types

Industry Secrets

- Disclose trade secrets
- Disclose data
  - Details
  - Types

Business Concerns

- Financial effects
- Shareholder reaction
- Law enforcement reaction
  - Civil – GLBA
  - Criminal – impute insider activity
- Private lawsuits
- Customer reaction
- Congressional reaction

Antitrust Laws

- More to private-private interaction
  - Potential competitors discussing common approach to problem
- Can arise with in government context
  - Meeting that involved competitors convened by FTC Commissioner to discuss spam issues had to be vetted by FTC antitrust counsel

Sharing Approaches

- Mandatory
  - Breach notification
- Voluntary – government initiative
  - CERT - CERT/CC
  - NCFTA
  - Infragard
- Voluntary – private initiative
  - CastleCops – phishing investigations
    - Gone after operator tired of DDOS attacks
  - Internet Storm Center
  - Private corporate spam traps

International Approaches

- National Security Statutes
  - EU members can compel ISPs to log use
  - Swiss – record email date, time, sender, recipient
  - Spain – one year ISP data retention
- APEC adoption of UN resolution on criminal misuse of IT
- EC jawbone approach to improving security practices
- ENISA – collect, analyze, and share data
- G8 High Tech Subgroup

NGOs

- Non Governmental Organizations
- ITU World e-Trust
- ICC Global Action Plan for Electronic Business
- BIAC security assurance guide
- GBDe
  - Upstream and downstream sharing
  - Global definitions of “appropriate level of security”

Statutory Adoption of Private Standards

- Safe Harbor
  - COPPA
  - EU
- Reference to PCI-DSS

COPPA

- Children's Online Privacy Protection Act
- Components
  - Substantially similar requirements to FTC's
  - Effective mandatory compliance assessment
  - Financial or public reporting penalties
- Certification
  - Document how program meets standards
  - How assessment and compliance incentives meet requirements
- 4 approved

EU Safe Harbor

- Developed through negotiation between EU and US Department of Commerce
  - Approved 2000
- Annual self-certification to Commerce that it agrees to adhere to the safe harbor's requirements”
- 1345 companies registered (12/24/2007)
  - (was 997 on 7/31/2006)
  - Many not current with self-certification

Safe Harbor Red Tape

- Much more extensive than COPPA
- Enforced under False Statements Act
  - Certify falsely or fail to notify that a relevant self-regulatory or government enforcement body has found a persistent failure to comply
  - Government: FTC or DoT
  - Self regulatory: *e.g.,* TRUSTe, BBBOnline
- List of companies at www.export.gov/safeharbor/

PCI-DSS Principles

- Payment Card Industry Digital Security Standards
  - Build and maintain a secure network
  - Protect cardholder data
  - Maintain a vulnerability management program
  - Implement strong access control measures
  - Regularly monitor and test networks
  - Maintain an information security policy

PCI-DSS Implementation

- 12 Sections
- Audit guidelines and specific security standards
  - Encryption
  - Storage
  - Retention

State Legislation

- Adopt language clearly from PCI-DSS vs specific incorporation of PCI-DSS
- Examples from
  - Minnesota - adoption of language that can be traced to PCI-DSS
  - Texas - specific reference to PCI-DSS

Minnesota

- HF 1758
  - Forbids storing data longer than 48 hours
  - No shadow of PCI-DSS provision for "compensating controls" that allow company to demonstrate alternatives to formal PCI standards
- Enacted

Texas

- HB 3222
- Businesses that acquire credit card data in the regular course of business “must comply with payment card industry security standards”
- Passed TX House but not Senate

Industry Standards in Law Advantages

- Theoretically prepared by subject matter experts
- Revisions to keep up with technology may be faster

Industry Standards in Law Problems

- May entrench standard in law with delay if change necessary
- May not be general enough to address broad range of industries or allow risk management approach
- Even industry standards can be dated
  - WEP wifi security allowed by PCI-DSS in some instances as recently as last year