

PRIVACY IN CYBERSPACE



CSH6 Chapter 69

“Privacy in Cyberspace:
U.S. and European Perspectives”

Henry L. Judy, Scott L. David,
Benjamin S. Hayes, Jeffrey B. Ritter,
Marc Rotenberg, & M. E. Kabay

1

Copyright © 2015 M. E. Kabay. All rights reserved.

Topics

- Worldwide Trends
- European Approaches to Privacy
- United States
- Compliance Models



2

Copyright © 2015 M. E. Kabay. All rights reserved.

Worldwide Trends

- Technology brings increased opportunities for data collection & commercial use
- Growing concern over privacy protection
- Cutting-edge developing technologies
 - ❑ DNA databases
 - ❑ RFID
 - ❑ Electronic health records
- Recent cyberprivacy issues



3

Copyright © 2015 M. E. Kabay. All rights reserved.

Recent Cyberprivacy Issues



- NSA Domestic Spying
- NSA PRISM in USA
- Phone Hacking in UK



4

NSA Domestic Spying



- October 2001 – President Bush orders NSA to begin surveillance within USA
- No law authorizing capture of telephone & Internet communications
- No court order satisfying 4th Amendment requirements
- Bush administration concedes that order violates even FISA (Foreign Intelligence Surveillance Act)
- Obama administration continued illegal surveillance



For cartoons lampooning this surveillance, see <http://tinyurl.com/oagvwp4>

5

Copyright © 2015 M. E. Kabay. All rights reserved.



FAQ How It Works Key Officials NSA Primary Sources State Secrets Privilege Timeline

Word Games

<https://www.eff.org/nsa-spying/timeline>

Timeline of NSA Domestic Spying

The information found in this timeline is based on the [Summary of Evidence](#) we submitted to the court in *Jewel v. National Security Agency (NSA)*. It is intended to recall all the credible accounts and information of the NSA's domestic spying program found in the media, official government statements and reports, and court actions. The timeline includes leaked documents, first published by the *Guardian* in June 2013, that confirmed the domestic spying by the NSA, as well as accounts based on unnamed government officials. The documents that form the basis for this timeline range from a Top Secret Court Order by the secret court overseeing the spying, the Foreign Intelligence Surveillance Court (FISA Court), to a working draft of an NSA Inspector General report detailing the history of the program. The "NSA Inspectors General Reports" tab consists of information taken from an internal working draft of an NSA Inspector General report that was published by the *Guardian* on June 27, 2013. It also includes a July 10, 2009 report written by Inspectors General of the Department of Justice (DOJ), NSA, Department of Defense (DOD), Central Intelligence Agency (CIA), and the Office of the Director of National Intelligence and a June 25, 2009 "End to End Review" of the Section 215 program conducted by the NSA for the FISA Court. For a short description of the people involved in the spying you can look at our [Profiles](#) page, which includes many of the key characters from the NSA Domestic Spying program. The documents published by various media outlets are gathered [here](#).

6

NSA PRISM in USA



- NSA collecting metadata about all phone calls in USA
- FISC (Foreign Intelligence Surveillance Court) ordered Verizon phone company to turn over all records
- Violated USAPATRIOT Act compelling disclosure only of *relevant* data



7

Copyright © 2015 M. E. Kabay. All rights reserved.

Phone Hacking in UK



- *News of the World* UK newspaper accessed voice mail of investigative targets from 2003 through 2007
- Management systematically opposed and undermined investigations by legal authorities
- Major failure to comply with journalistic and legal requirements



8

Copyright © 2015 M. E. Kabay. All rights reserved.

Laws, Regulations & Agreements



- General patterns emerging across countries
- Personally identifiable information (PII)
 - ❑ Anything tied to individual
 - ❑ Potentially subject to regulation
- Principle: data subject should control PII
- Privacy laws: obligations to respect data subject's expectations
- Fair information practices
 - ❑ Control by data subject
 - ❑ Prohibition of specific practices/applications concerning PII
- Challenge: integrate business, law & technology



9

Copyright © 2015 M. E. Kabay. All rights reserved.

Sources of Privacy Law



- Governments & public-sector entities
 - ❑ Restrained from undue intrusion
 - ❑ Constitutional mechanisms
 - ❑ Access to government-held PII in democracies
- Restraints on private-sector usage by laws
- European Charter of Fundamental Rights
 - ❑ Nation states must consider protection of PII as fundamental human right
 - ❑ Applies also to future members of EU
- Privacy being integrated into national constitutions & supranational law



10

Copyright © 2015 M. E. Kabay. All rights reserved.

European Approaches to Privacy



- History & OECD
- EU Data Protection Directive
- Harmonization of Non-EU European Countries
- EU Telecommunications Directive
- European Data Protection Supervisor



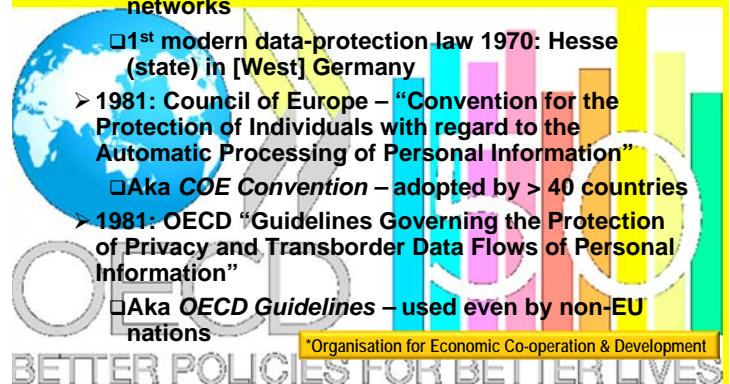
11

Copyright © 2015 M. E. Kabay. All rights reserved.

History & OECD*



- Privacy increasingly important in 1960s & 1970s
 - ❑ Surveillance potential of computers and networks
 - ❑ 1st modern data-protection law 1970: Hesse (state) in [West] Germany
- 1981: Council of Europe – “Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Information”
 - ❑ Aka *COE Convention* – adopted by > 40 countries
- 1981: OECD “Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Information”
 - ❑ Aka *OECD Guidelines* – used even by non-EU nations



*Organisation for Economic Co-operation & Development

EU Data Protection Directive



- Directive 95/46/EC passed in 1995
- Became effective 1998
- Requires EU member states to pass national laws implementing its terms
- National laws not identical
- Not enough for businesses with EU interests to use only DPD – must examine local laws
- Details:
 - ❑ EU Directive Requirements
 - ❑ International Data Transfer Restrictions
 - ❑ State of implementation

GDPR EU DPD
EU Data Protection Directive

EU Directive Requirements



- **Notice:** who, why, how, where, to whom
- **Consent:** right to block, opt out, require permission
- **Consistency:** follow terms of notice
- **Access:** see own info, make corrections
- **Security:** prevent unauthorized access
- **Onward Transfer:** contractual obligations to follow same rules and agreements
- **Enforcement:** private right of action, Data Protection Authority in every country
 - ❑ Investigate complaints
 - ❑ Levy fines
 - ❑ Initiate criminal actions
 - ❑ Demand changes



14

Copyright © 2015 M. E. Kabay. All rights reserved.

International Data Transfer Restrictions



- Regulation of interjurisdictional information exchanges
- Transfer from EU to non-EU countries
 - ❑ PROHIBITED *unless*
 - ❑ Destination has “adequate” legal protections
 - ❑ USA not considered to have adequate protection
- US/EU *Safe Harbor* arrangements discussed later in chapter



15

Copyright © 2015 M. E. Kabay. All rights reserved.

State of Implementation



“All 27 member countries of the European Union, including the new members states, have passed legislation fully implementing the directive.”



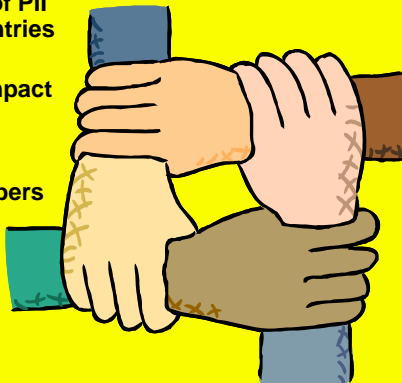
16

Copyright © 2015 M. E. Kabay. All rights reserved.

Harmonization of Non-EU European Countries



- Prohibition on transfer of PII has moved non-EU countries to pass consistent laws
 - ❑ Adverse economic impact
- Two categories
 - ❑ EU trading partners
 - ❑ Potential future members of EU



17

Copyright © 2015 M. E. Kabay. All rights reserved.

EU Telecommunications Directive

- Specific to telecommunications companies & agencies
- Ensure technological assurance of privacy for communications
- Restricts access to billing information
- Limits marketing strategies
- Allows per-line blocking of caller ID
- Forces deletion of call-specific information at end of communication
- New proposal goes further: affect *all* electronic communications



European Data Protection Supervisor



<http://www.edps.europa.eu/EDPSWEB/edps/EDPS>

- Independent supervisory body
- Monitor application of regulations affecting data gathering, transmission, and use of PII

19

Copyright © 2015 M. E. Kabay. All rights reserved.

United States



- History, Common Law Torts
- Public Sector
- Private Sector
- State Legislation



20

Copyright © 2015 M. E. Kabay. All rights reserved.

History, Common Law Torts



- Privacy as cause for tort: 20th century development
 - ❑ Constitution did not recognize privacy explicitly
 - ❑ Growing urbanization forced growing awareness of need for privacy law
 - ❑ "Right to be left alone" posited in 1890
 - ✓ Charles Warren & Louis Brandeis
 - ✓ Harvard Law Review article
 - ❑ State laws evolved without overarching federal law



21

Copyright © 2015 M. E. Kabay. All rights reserved.

Evolution of US Privacy Theory



- 1960 Restatement of Torts defined 4 subtypes related to privacy:
 - ❑ *Intrusion*: unreasonable breach of seclusion if offensive to reasonable person
 - ❑ *Revelation* of private facts: unauthorized & unreasonable publicity of facts not of legitimate concern to public – when given to wide audience
 - ❑ *False light*: conveying false impression
 - ❑ *Misappropriation*: unauthorized use of name or likeness for benefit or gain (often used by celebrities)



22

Copyright © 2015 M. E. Kabay. All rights reserved.

Public Sector in USA



- History
- Privacy Act of 1974 & FOIA
- ECPA of 1986
- Right to Financial Privacy Act of 1978
- Driver's Privacy Protection Act
- Law Enforcement & National Security Surveillance



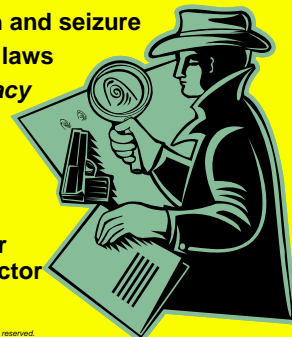
23

Copyright © 2015 M. E. Kabay. All rights reserved.

History of US Public Sector Privacy Laws



- Long-standing restrictions on government intrusions into private lives of citizens
- US Constitution
 - ❑ 4th Amendment governs search and seizure
 - ❑ 14th Amendment governs state laws
 - ❑ But no explicit mention of *privacy*
- Case law and statutes have defined privacy rights
- State constitutions usually also include restrictions
- Governments usually have stricter privacy protection than private sector



24

Copyright © 2015 M. E. Kabay. All rights reserved.

Privacy Act of 1974 & FOIA



- Privacy Act of 1974
 - ❑ Limits on federal government can use & transfer PII
 - ❑ Individual rights to know PII held by federal government
- Freedom of Information Act (FOIA) part of Privacy Act
 - ❑ Determine
 - ❑ Forbid
 - ❑ Access
 - ❑ Correct
 - ❑ Current, relevant, not excessive
 - ❑ Private right of legal action



25

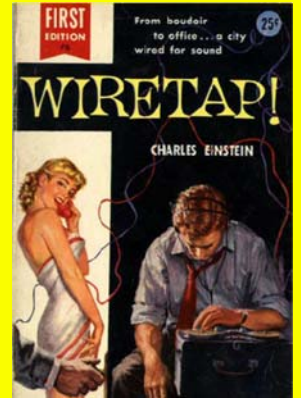
Copyright © 2015 M. E. Kabay. All rights reserved.

ECPA of 1986



➤ Electronic Communications Privacy Act of 1986

- ❑ Amended Wiretap Law of 1968
- ❑ Prohibits unauthorized, intentional
 - ✓ Interception of
 - ✓ Access to
- ❑ Wire, oral, electronic communications
- Require court orders to install devices
 - ❑ Pen registers (outbound phone numbers)
 - ❑ Trap and trace (incoming phone numbers)
- ❑ Not probable cause – only certification from LEO



26

Copyright © 2015 M. E. Kabay. All rights reserved.

Right to Financial Privacy Act of 1978



- Federal government cannot
 - ❑ Obtain financial records for individual
 - ❑ Without informing subject of investigation
- Subpoena: 90 day limit for informing subject
- Other methods for authorizing disclosure
 - ❑ Must inform subject
 - ✓ Before
 - ✓ Simultaneously with
 - ❑ Investigation



27

Copyright © 2015 M. E. Kabay. All rights reserved.

Driver's Privacy Protection Act



- 1st time Congress passed law limiting state government access to PII
- Prohibits disclosure of PII associated with motor vehicle ownership / driver's license
- Exceptions
 - ❑ Legitimate government activities
 - ❑ Facilitate (safety) recalls

28

Copyright © 2015 M. E. Kabay. All rights reserved.

Law Enforcement & National Security Surveillance

- Criminal activity aided by technological advances
- Law enforcement & national security information gathering also enhanced
- Monitoring – search data for signs of crime
 - ❑ Packet sniffers: capture & scan packets for keywords using signatures or heuristics
 - ❑ Black boxes: log communications traffic
- Surveillance – eavesdrop on communications / behavior of specific subjects of investigation
 - ❑ ECHELON – USA, UK, NZ, Australia, Canada
 - ❑ CALEA (Communications Assistance for Law Enforcement Act of 1994) requires technical standards for ISPs
 - ❑ Council of Europe Convention on Cyber-Crime (2004)
 - ✓ 22 countries ratified
 - ✓ Criticism from privacy advocates



29

Copyright © 2015 M. E. Kabay. All rights reserved.

Private Sector



- Overview of US Private Sector Regulations
- Gramm-Leach-Bliley Act
- Children's Online Privacy Protection Act
- Health Insurance Portability and Accountability Act
- Cable and Video Acts
- US/EU Safe Harbor
- Workplace Privacy
- Anonymous Cybersmearing
- Online Monitoring Technology
- Location Privacy
- Genetic Discrimination
- Social Network Sites & Privacy

30

Copyright © 2015 M. E. Kabay. All rights reserved.

Overview of US Private Sector Regulations



- US relatively limited in regulating private sector
 - ❑ Preference for self-regulation
- Most privacy-related laws are sector-specific
 - ❑ Financial services
 - ❑ Healthcare services
- Evolving issues
 - ❑ Workplace privacy
 - ❑ Defamation
 - ❑ Location
 - ❑ Genetics
 - ❑ Social networks



31

Copyright © 2015 M. E. Kabay. All rights reserved.

Gramm-Leach-Bliley Act

- GLB – 1999 law named for its architects
 - ❑ Took effect July 1, 2001
- Applies to all *financial institutions*
 - ❑ Protect data subjects' PII
 - ❑ Disclose policies to data subjects
 - ❑ Provide options for sharing info (or not)
 - ❑ FTC in particular has extended definition of *financial institutions*



Phil Gramm



Jim Leach

- Widespread effects in many industries
- ❑ Capture & maintain opt-out requests
 - ❑ Send notices to affected customers
 - ❑ Limits on selling customer lists
 - ❑ Be sure arrangements meet multiple regulators' requirements



Tom Bliley

32

Copyright © 2015 M. E. Kabay. All rights reserved.

Children's Online Privacy Protection Act



- COPPA passed 1998
- Prohibits
 - ❑ Collection
 - ❑ Use
 - ❑ Disclosure
- Children's PII without verifiable parental consent
- FTC rules violations "unfair or deceptive trade practices"



33

Copyright © 2015 M. E. Kabay. All rights reserved.

Health Insurance Portability and Accountability Act



- HIPAA (not HIPPA) passed 1996
 - ❑ Last compliance deadline was 2004
- Providers & health plans must
 - ❑ Give patients clear written explanations of how organizations handle PII
 - ❑ Minimize use of PII to essentials
 - ❑ Disclosure logs
 - ❑ Cannot condition services on waiver of rights
- Criminal penalties for fraudulent obtention
- States not preempted from more restrictive laws
- Substantial fines for violations



34

Copyright © 2015 M. E. Kabay. All rights reserved.

Cable and Video Acts

- Cable Communications Policy Act of 1984 §551
 - ❑ Protection of subscriber privacy
 - ❑ Annual notice of data collection/use practices
 - ❑ Mandatory prior consent
 - ❑ Law enforcement require court order for info
 - ❑ Private right of action (punitive damages, fees)
- Video Privacy Protection Act of 1988
 - ❑ Prohibits transfer of video rental records
 - ❑ Exceptions require customer approval
 - ❑ LEOs require warrant
 - ❑ Sometimes described as result of *borking* (now a recognized verb) Robert Bork in 1987 over (inoffensive) video rentals

US/EU Safe Harbor



- EU Privacy Directive (1998) restricts transfer of PII to nations with *adequate* privacy protection
- April 1998 – July 2000: negotiations on Safe Harbor provisions allow data transfers to *companies* willing to
 - ❑ Comply with EU Directive principles
 - ❑ Self-certify adherence by public report to US Dept of Commerce
 - ❑ Provide for independent audit or membership in suitable organization
 - ✓ TRUSTe, BBBOnline
 - ❑ Be subject to FTC regulation
 - ✓ Violation of SH actionable as fraud by FTC

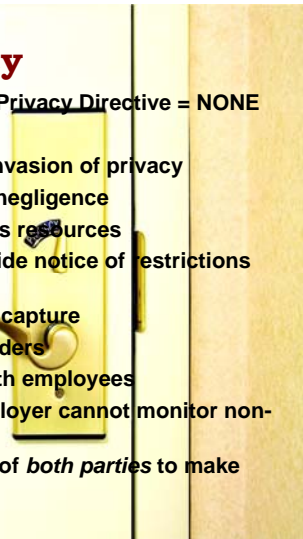


36

Copyright © 2015 M. E. Kabay. All rights reserved.

Workplace Privacy

- EU: simply restricted by EU Privacy Directive = NONE
- Difficult balance in US
 - ❑ Excessive monitoring = invasion of privacy
 - ❑ Inadequate monitoring = negligence
- Common law: employer owns resources
 - ❑ Therefore need only provide notice of restrictions and monitoring
- ECPA governs wiretapping / capture
 - ❑ But exempts system providers
 - ❑ And consent: contract with employees
 - ❑ Live telephone calls: employer cannot monitor non-work-related phone calls
 - ❑ FL & MD require consent of *both parties* to make wiretap legal



Anonymous Cybersmearing



- Organizations can be *claqued* or *smeared* by anonymous posters on the 'Net': options include
 - ❑ Do nothing (don't feed the trolls)
 - ❑ Identify the poster – contact or sue
 - ❑ Contact law enforcement
 - ✓ Threats to individuals or property
 - ✓ Attempts to manipulate stock prices
 - ❑ File suit against “John Doe” and subpoena ISP to discover identity of poster
 - ✓ May not work



38

Copyright © 2015 M. E. Kabay. All rights reserved.

Online Monitoring Technology



- Unauthorized monitoring of Web activity
- Cookies
 - ❑ Text files on hard drive
 - ❑ Recognize user (e.g., GOOGLE)
- Web beacons / bugs / single-pixel GIFs
 - ❑ Used in email messages to tell if recipient has opened the message
 - ❑ Report user identity and history to Web server



39

Copyright © 2015 M. E. Kabay. All rights reserved.

Location Privacy



- Wireless devices often include GPS capabilities
- Direct localized advertising to user
- Concerns over use by criminals (e.g., automatic “not at home now” beacon)
- Regulations limited



40

Copyright © 2015 M. E. Kabay. All rights reserved.

Genetic Discrimination



- Collection and distribution of genetic information an issue
- Can be used to predict differential *susceptibility* to specific diseases
- Could be used to discriminate against victims
 - ❑ Insurance companies could refuse to cover
 - ❑ Employers could refuse to hire or promote



[MK adds personal opinions:
 – Exactly what happens today with XX chromosomes (join NOW to fight this)
 – People with genes for high melanin skin pigment production (join the NAACP to fight this)]

41

Copyright © 2015 M. E. Kabay. All rights reserved.

Social Network Sites & Privacy



- Facebook, MySpace...
- Explosion of publication of formerly private PII
 - ❑ Marketing groups salivating
 - ❑ Stalkers too
- 2007 ENISA report (European Network and Information Security Agency)
 - ❑ Clear benefit
 - ❑ False sense of intimacy
 - ❑ Encourage social-networking education in schools
 - ❑ Encourage openness, notification of breaches
 - ❑ Privacy-friendly defaults



42

Copyright © 2015 M. E. Kabay. All rights reserved.

State Legislation

- US federal laws/regulations provide minimum terms
- States may be more stringent
- Many state laws
 - ❑ Organized by industry or sector
 - ❑ May affect anyone doing business in the state
- Notable examples
 - ❑ CA SB 1386 (2003) requires notification of breaches
 - ❑ California Financial Information Privacy Act (2003)
 - ❑ Most states have genetic-information protection laws
 - ❑ Several states regulate interception of RFID (radio-frequency identification devices)

Compliance Models

- US Legislation
- US FTC §5 Authority
- Self-Regulatory Regimes & Codes of Conduct
- Contract Infrastructure
- Synthesis of Contracts, Technology & Law
- Getting Started: A Practical Checklist



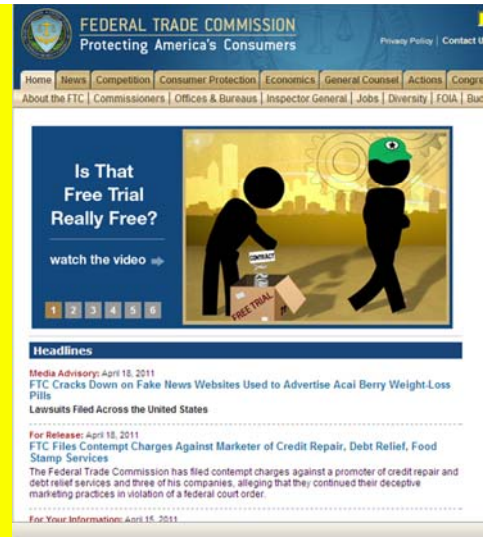
US Legislation

- Pass specific law
- Apply to any organization gathering/using PII
- Define rights of data subjects
- Various enforcement mechanisms
 - ❑ Private right of action (lawsuits & class action)
 - ❑ Actions by state attorneys general
 - ❑ Action by FTC re unfair/deceptive trade practices



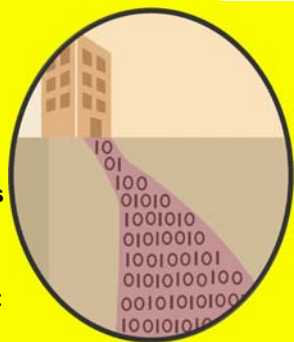
FTC

- Investigate unfair / deceptive trade practices
- Has applied to many privacy cases
- Mostly cases of negligent security



Self-Regulatory Regimes & Codes of Conduct

- Benefits
 - ❑ Minimizes need for government resources
 - ❑ Allows greatest flexibility for businesses
- Criticisms
 - ❑ Insufficient standards
 - ❑ Inadequate enforcement

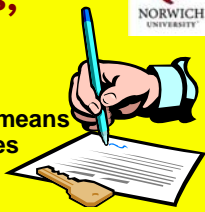


Contract Infrastructure

- Contracts can support or damage privacy
- Govern entire life cycle of PII
 - ❑ Collection
 - ❑ Storage
 - ❑ Use
 - ❑ Transfer
- Develop *chain of contracts*

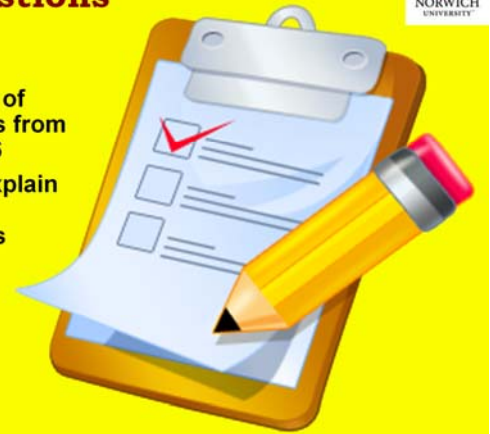


Synthesis of Contracts, Technology & Law



- Problems
 - ❑ Policing contracts may be beyond means or inclination of many businesses
 - ❑ Businesses unlikely to sue trading partners
 - ❑ Consumers unlikely to launch individual lawsuits
 - ❑ Class-action lawsuits possible
 - ❑ Once compromised, PII cannot realistically be re-protected
 - ❑ Extent of problem may exceed practical resources for enforcement
- Therefore may have to rely on technology

Review Questions



- Use the checklist of recommendations from authors in §69.4.6
- Be prepared to explain every one of the recommendations

A Practical Checklist (1)



- Achieve buy-in, at the highest level of the organization, to the idea that personal information management must be part of an organization's critical infrastructure.
- Perform due diligence to identify *all* types of personal information collected and the routes by which the data travel in and out of the organization.
- Identify all of the uses to which the information is put during its life cycle through collection, processing, use, transfer, storage, and destruction.

A Practical Checklist (2)



- Identify each law affecting the collection, use, and transfer of personal information to which the company is subject.
- Create an institutional privacy policy that accurately considers both a commitment to abide by various legal requirements and the legitimate business activities of the organization.
- Create supporting materials that educate employees and instruct on policy implementation.

A Practical Checklist (3)



- Implement consistent data transfer agreements with all data-trading partners, vendors, service providers, and others with whom personal information is acquired or transferred.
- Build privacy management into the organization's strategic planning, providing sufficient resources for personnel, training, technology, and compliance auditing.
- Hold employees accountable for implementation and compliance with the privacy policy and contract requirements.

A Practical Checklist (4)



- Consider innovative approaches to privacy protection and business development that limit or eliminate the collection of personally identifiable information.
- Periodically audit compliance.