



IAPP Privacy Certification

Certified Information Privacy Professional (CIPP)

Privacy Law and Compliance

Christie Grymes

Associate

Collier Shannon Scott

agenda

- **the US legal system**
- **privacy concepts**
- **privacy laws**
- **compliance basics**
- **theories of liability**



**the US
legal
system**

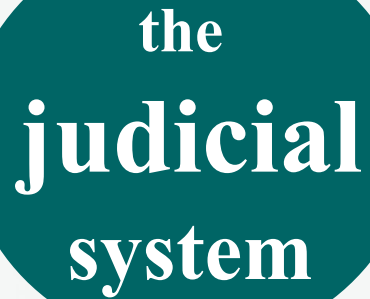
trial

**three
branches
of gov't**

	Executive Branch	Legislative Branch	Judicial Branch
purpose	enforces laws	makes laws	interprets laws
who	President, VP, Cabinet, Federal agencies (such as FTC)	Congress (House & Senate)	Federal courts
checks & balances	President appoints Federal judges, President can veto laws passed by Congress	Congress confirms presidential appointees, can override vetoes	determines whether the laws are constitutional

sources of law

- **enacted laws – local, state, federal, international**
- **regulations promulgated pursuant to a law by a regulatory agency, such as the Federal Trade Commission (FTC)**
- **court decisions that interpret the obligations under a law (sometimes known as “case law”)**
- **“common law” – law based on custom and general principles, embodied in court decisions, that serves as precedent or is applied to situations not covered by statute**



the
judicial
system

- **Federal courts**
 - **judges appointed by President**
 - **US Supreme Court**
 - **Circuit Courts of Appeal**
 - **District Courts**
 - **specialty courts**
- **state courts**
 - **judges elected or appointed**
 - **state supreme courts**
 - **state appeals courts**
 - **trial courts**
- **the US Supreme Court can hear appeals from state supreme courts, if it wants to**

some key definitions

- **person**
any entity with legal rights, such as an individual (a “natural person”) or a corporation (a “legal person”)
- **jurisdiction**
the authority of a court to hear a particular case
a court must have jurisdiction over both the type of dispute (subject matter jurisdiction) and the parties (personal jurisdiction)
- **preemption**
a conflicts of law doctrine: when a superior government’s laws supersede those of an inferior government for a particular subject

2 types of litigation

- **criminal litigation**
occurs when the executive branch sues a person claiming the person has violated a criminal law
- **civil litigation**
occurs when a person sues another person to redress some wrong
- **2 main types of civil litigation**
 - **contract disputes**
 - **tort (personal injury) claims**

**regulatory
regime**

Dept. of
Commerce

unsolicited fax rules
Federal Communications
Commission

safe harbor

TCPA, Can Spam

**Federal Trade
Commission**

**State Attorneys
General**

enforcement

FCRA, FACTA, GLBA

Bank Regulators
(Fed, OCC)

self- regulation

don't forget self-regulatory regimes

- **Direct Marketing Association
privacy promise**
- **BBBOnline & TRUSTe**
- **Children's Advertising Review Unit
(CARU)**
- **other trade associations, industry
best practices or codes of conduct**

analyze a law

- **Who is covered?**
- **What is covered?**
- **What is required or prohibited?**
- **Who enforces?**
- **What happens if I don't comply?**
- *Why does this law exist?*

sb 1386

- **Who is covered?**
 - ✓ entities that do business in California
- **What is covered?**
 - ✓ computerized PI of California residents – PI is name *plus* SSN, DL or financial data
- **What is required or prohibited?**
 - ✓ if unencrypted PI was (or may have been) accessed inappropriately, you must provide prompt notice to the affected individuals
- **Who enforces?**
 - ✓ CA AG, there is a private right of action
- **What happens if I don't comply?**
 - ✓ you can be sued for damages
- *Why does this law exist?*
 - ✓ *fear that security breaches cause ID theft*

privacy
concepts

ai

what is privacy

“privacy” is not well-defined

- **control of personal events – the right to birth control, abortion**
- **freedom from intrusion – the right to be left alone**
- **control of information – the right to keep personal information private**
- *privacy is the appropriate use of information given the circumstances*

privacy vs. security

privacy and security are different

- **security is the protection of information**
 - **who has access**
 - **what is most sensitive**
 - **who can manipulate the data**
- **privacy is the appropriate use of information as defined by:**
 - **law**
 - **public sensitivity**
 - **context**

types of
**personal
information**

- **public records**
information maintained by a government entity and available to the general public (e.g., real property records)
- **publicly-available information**
information that is generally available without restriction (e.g., information in news papers, telephone books)
- **non-public information**
information that is not generally available due to law or custom (e.g., financial data, medical records)

some key definitions

notice

a description of an organization's information management practices

- **the typical notice tells the individual:**
 - **what data is collected**
 - **how it is used**
 - **to whom it is disclosed**
 - **how to exercise any choices that may exist with respect to such use & disclosures**
 - **whether the individual can access or update the information**
- **but many laws have additional requirements**
- **notices have 2 purposes**
 - **consumer education**
 - **corporate accountability**

some key definitions

access

the ability to view personal information held by an organization – this ability may be complemented by an ability to update or correct the information

the ability to access and correct data is especially important when the data is used for any type of substantive decision-making

some key definitions

choice

the ability to specify whether personal information will be collected and/or how it will be used

- **“opt-in” means an affirmative indication of choice based on an express act of the individual authorizing the use**
- **“opt-out” means choice implied by the failure of the individual to object to the use or disclosure**
- **choice isn’t always appropriate, but if it is, it should be meaningful – based on a real understands the implications of the decision**

**privacy
laws**

ai

**two
approaches
to US law**

- **fair information practices approach**
 - provide notice and choice
 - process-oriented
 - **Gramm-Leach-Bliley is a prime example**
- **permissible purpose approach**
 - use limited to permissible purposes
 - context-oriented
 - **Fair Credit Reporting Act is a prime example**
- **HIPAA gives you the “best” of both worlds**
- **corporate accountability is always constant**

fair credit reporting act

Why does this law exist?

- ✓ 1940s merchants shared data to facilitate credit for consumer durables... by 1960s consumer credit was critical but individuals were harmed by inaccurate information that they could not see nor correct
- the FCRA was enacted to mandate accuracy, access and correction; and to limit use of consumer reports to permissible purposes
- amended in 1996 with provisions for non-consumer initiated transactions, standards for consumer assistance
- amended in 2003 with provisions related to identity theft (FACT Act)

fair credit reporting act

Who is covered?

- ✓ entities that compile consumer reports
- ✓ persons who use consumer reports
- **circular definitions...**
 - a consumer reporting agency is an organization that communicates consumer reports; while consumer reports are provided by CRAs*

fair credit reporting act

What is covered?

✓ a consumer report is any information that pertains to:

- credit worthiness;
- credit standing;
- credit capacity;
- character;
- general reputation;
- personal characteristics; or
- mode of living

and that is used in whole or in part for the purpose of serving as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other business purpose

fair credit reporting act

What is required or prohibited?

- ✓ 3rd party data used for substantive decision-making must be appropriately accurate, current and complete
- ✓ consumers must receive notice when 3rd party data is used to make adverse decisions about them
- ✓ consumer reports may only be used for permissible purposes
- ✓ consumers must have access to their consumer reports and an opportunity to dispute/correct errors
- ✓ comply with all other requirements on users and furnishers of consumer data

fair credit reporting act

Who enforces the FCRA?

- ✓ Federal Trade Commission
- ✓ state attorneys general
- ✓ private right of action

What happens if I don't comply?

- ✓ civil and criminal penalties
- ✓ in addition to actual damages, violators are subject to statutory damages
 - *\$1,000 per violation*
 - *\$2,500 for willful violations*

gramm- leach-bliley act

Why does this law exist?

- ✓ modernization statute revamping banking and insurance industries
- ✓ banks were in the news for sleazy data-sharing
- ✓ substantial privacy concerns due to consolidation of financial data

Who is covered?

- ✓ domestic financial institutions (FI)-- *any company “significantly engaged” in financial activities*

**gramm-
leach-bliley
act**

What is covered?

- ✓ **“non-public personal financial information” – but this includes any info:**
 - **provided by a consumer to a FI to obtain a financial product or service,**
 - **resulting from a transaction involving a financial product or service between a FI and a consumer, or**
 - **that the FI otherwise obtains in connection with providing a financial product or service to a**

**gramm-
leach-bliley
act**

What does GLBA require?

- ✓ **FIs must provide consumer customers with notices about privacy & security practices**
- ✓ **FI may share virtually any information with “affiliated” companies**
- ✓ **other than for defined exceptions, FI may share with “non-affiliated” companies only if consumer customers have not opted out**
- ✓ **FTC and FI regulators must promulgate privacy and safeguards rules**
- ✓ **GLBA does not preempt state laws**

**glba
privacy
rule**

the GLBA Privacy Rule

- ✓ **FTC and federal FI regulators established standards for the privacy notices**
 - **must give initial & annual privacy notices to consumer customers**
 - **9 categories of information**
 - **process opt-outs within 30 days**
- ✓ **share with other 3rd parties only if an exception exists**
- ✓ **ensure that service providers will not use the data for other purposes**

glba safeguards rule

the GLBA Safeguards Rule

- ✓ **administrative security**
 - program definition & administration
 - manage workforce risks, employee training
 - vendor oversight
- ✓ **technical security**
 - computer systems, networks, applications
 - access controls
 - encryption
- ✓ **physical security**
 - facilities
 - environmental safeguards
 - disaster recovery

gramm- leach-bliley act

Who enforces GLBA?

- ✓ **FTC and financial institution regulators**
- ✓ **state attorneys general**
- ✓ **no private right of action – *but failure to comply with a notice is a deceptive trade practice, actionable by state & federal authorities & some states have private rights of action for UDTP violations***

What happens if I don't comply?

- ✓ **enforcement actions**
- ✓ **possible private lawsuits**



HIPAA

Health Insurance Portability & Accountability Act of 1996

- **Who is covered?**
 - ✓ **health care providers, health plans and health care clearinghouses are covered directly – “business associates” and others who use or disclose PHI are covered indirectly**
- **What is covered?**
 - ✓ **“protected health information” (PHI) transmitted or maintained in “any form”**
- **What is required or prohibited?**
 - ✓ **covered entities may not use or disclose PHI except as permitted or required by the privacy & security regulations**



HIPAA

- **Who enforces HIPAA?**
 - ✓ **Department of Health & Human Services (HHS), state AGs**
- **What happens if I don't comply?**
 - ✓ **Civil and criminal penalties – fines of up to \$250,000 and/or 10 years imprisonment**

HIPAA does not preempt stronger state laws, and many states have stronger health care privacy statutes. *HIPAA sets the floor for medical privacy.*

Children's Data

- **Who is covered?**
 - ✓ **The Children's Online Privacy Protection Act applies to commercial website operators**
- **What is covered?**
 - ✓ **Collection and use of information on children under 13 years old via a commercial website**
- **What is required or prohibited?**
 - ✓ **With a few exceptions, website operators must obtain verifiable parental consent before they can collect PI from children**
- **Who enforces?**
 - ✓ **Federal Trade Commission and state AGs**
- **What happens if I don't comply?**
 - ✓ **you can be sued for damages, reputational risk**
- *Why does this law exist?*
 - ✓ *Response to websites collecting lots of personal data from little kids*

data protection laws

Why do these laws exist?

- ✓ government abuses sparked concerns in both Europe and the US
- ✓ data protection was about protecting individuals from government surveillance
- ✓ private data collections were part of the concern, because of ability of governments to compel production

European law is based on the protection of privacy as a fundamental human rights

US-EU contrast

- **US system: government use of data is restricted, private use is okay unless harmful or covered by sector specific law**
- **European system: no one can collect or use data unless permitted by law**



**the EU
framework**

- **EU Data Protection Directive 95/46/EC**
- **other EU directives, such as the Electronic Communications and e-Privacy Directive**
- **specific national laws on data protection, employment and general civil law**
- **guidance from the Article 29 Working Party**
- **guidance from national data protection authorities**



**the EU
directive**

- **enacted in 1995, effective 1998**
- **each country has its own national data protection law – Directive sets the floor**
- **prohibits transfer of personal data to non-E.U. jurisdictions unless “adequate level of protection” is guaranteed or another exception applies**
- **US is not adequate, but enforcement was limited prior to the safe harbor regime**
- **enforcement remains spotty, but recent high profile cases have changed the compliance landscape**



the **EU**
directive

- **“Personal Data”** – any and all data that relates to an identifiable individual
- **“Special Categories of Data”**– any and all data revealing race, ethnic origin, political opinions, religion or beliefs, trade union membership, sexual orientation or sex life, or criminal offenses... as well as biometric, health or disability data, national id numbers
- **“Processing”** – any and all operations on personal data (including collection, storage, handling, use, disclosure and deletion) – regardless of form or format (manual or automatic processing)

Yes, the definitions really are that broad

comply
with **EU**
laws

- **understand applicable national law requirements and company processes**
- **comply with all applicable laws for local data processing:**
 - **notification of DPAs, works councils**
 - **data collection (*e.g.*, notices)**
 - **purpose & use limitations**
 - **security**
 - **individual access & correction**
 - **limits on 3rd party processors**
 - **limited retention periods**
- **export data to other countries only if authorization for the transfer exists**

**data
transfers
are ok**

- **to a country that has been declared adequate (*e.g.*, Switzerland, Canada)**
- **within the safe harbor framework (from EU to US only)**
- **to any country, if a contract ensures adequate protection (*e.g.*, using model clauses)**
- **with “unambiguous consent” from the data subject**
- **upon authorization of EU Member State from which data is transferred**
- **if another exception applies (*e.g.*, if strictly necessary for performance of a contract with the data subject)**

safe harbor

- **US Department of Commerce created a series of documents that describe privacy principles similar to those in the Directive**
- **EU agreed that companies that self-certify that they are following the principles are in an adequate safe harbor**
- **FTC agreed that not following a self-certified standard is unfair/deceptive and subject to enforcement**
- **companies implement a privacy program, then certify annually to DOC that they are compliant**
- **not available to financial institutions and others who are not regulated by the FTC or Dept of Transportation**

model contracts

- **companies can provide for adequate protection by executing contracts which mandate certain safeguards – model clauses have been approved by the EU Commission, industry clauses may follow**
- **data exporters and importers provide notice, access, *etc.* – as defined by local law**
- **both exporter and importer are liable to the data subject for illegal data flows**
- **in most countries, you must notify DPA of the contract (but approval is generally automatic if model form is used)**
- **model form can be modified as long as basic provisions remain intact (*e.g.*, clauses can be added to other contract terms)**

consent

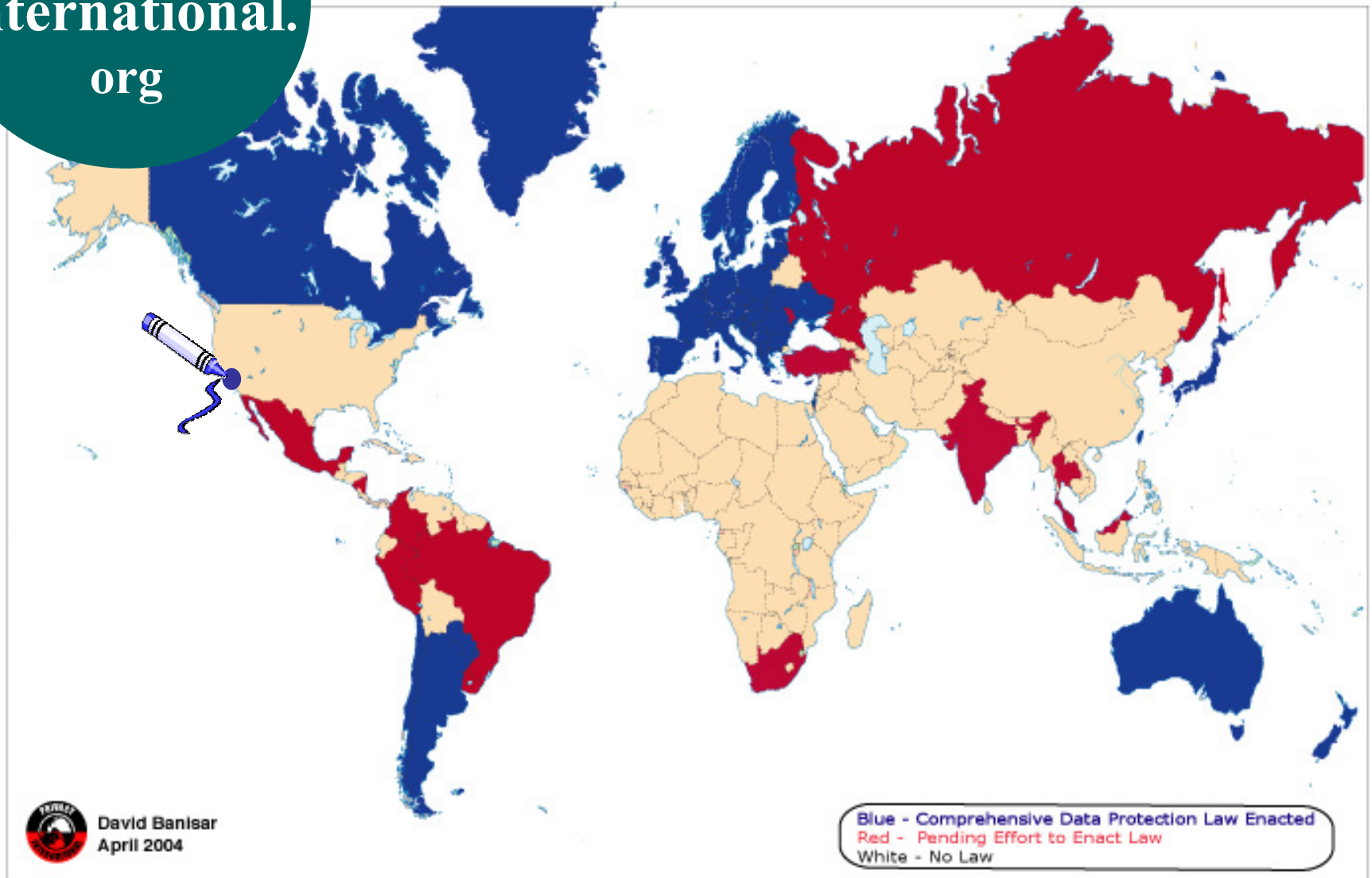
- **data transfers can generally be authorized by consent – and for sensitive data, consent is likely required regardless of your transfer mechanism**
- **for consent to be real, it must be “freely-given” and “unambiguous” – but the standards vary in each country**
- **EU authorities don’t always recognize consent for human resources data because of the “subordinate nature” of the employment relationship**
- **individuals must also be able to withhold (or revoke) consent, with no adverse consequences**

outside of Europe

- **many countries have enacted comprehensive data protection laws: Paraguay, Argentina, Peru, Hong Kong, Australia, New Zealand, Japan, South Africa, Tunisia...**
- **most reflect EU influences, but not all EU-style laws are “adequate” to the EU authorities**
- **Canada’s law (PIPEDA) is adequate, as is the law in Argentina – but Australia’s law is not**

www.privacyinternational.org

Data Protection Laws Around the World



**laws
regulating
marketing**

- **marketing communications are regulated globally**
- **US rules *generally* provide for opt-out choice**
 - **do not call**
 - **CAN SPAM**
 - **but do not fax is opt-in**
- **EU laws *generally* require opt-in choice**
 - **Electronic Communications and the e-Privacy Directives**
 - **but opt-out in certain circumstances**

**US laws
regulating
marketing**



**NATIONAL
DO NOT CALL
REGISTRY**

WWW.DONOTCALL.GOV

- **Federal Do Not Call registry**
 - **70 million names and growing**
 - **Scrub names every month**
 - **FTC & state AGs are enforcing...
plus private right of action (at least
in Massachusetts)**
 - **tip of the Telemarketing Sales
Rule iceberg**

**TSR &
telemarketing
rules**

the Telemarketing Sales Rules requires

- ✓ **screen names against DNC**
- ✓ **display caller ID information**
- ✓ **special rules for automated dialers**
- ✓ **call only between 8 am and 9 pm**
- ✓ **identify self & what you're selling**
- ✓ **disclose ALL material terms**
- ✓ **special rules for prizes & promotions**
- ✓ **respect requests to not be called back**
- ✓ **retain records for 24 months**
- ✓ ***be nice***

TSR & telemarketing rules

when the TSR does not apply

- ✓ non-profits calling on own behalf
- ✓ calls to existing customers, within the past 18 months
- ✓ calls to prospects, within 90 days of an inquiry
- ✓ inbound calls, if you don't up-sell
- ✓ most business-to-business calls

additionally, the TSR applies only to companies who are subject to FTC jurisdiction... but the FCC and state AGs have jurisdiction over everyone else

**state
telemarketing
rules**

the TSR does not preempt state telemarketing laws

- **42 states have telemarketing rules**
- **must register and often post bond**
- **process rules may differ from TSR**
 - **AR, CT, IN, KY, LA, MA, MN, MS, NM, RI, SD, TX, UT have more limited calling times**
- **must respect state DNC lists or DMA TPS**
 - **AK, CO, CT, FL, ID, IN, KY, LA, MA, MN, MS, MO, OK, PA, TN, TX, VT, WI, WY**
- **no exception for existing business relationship in Indiana**
- **private rights of action, statutory damages**

can spam act

Who is covered?

- ✓ anyone who advertises products or services by e-mail to or from the US

What is covered?

- ✓ transmission of “commercial electronic mail messages” – email messages whose primary purpose is advertising or promoting a product or service

What is required or prohibited?

- ✓ no false or deceptive messages, headers
- ✓ include working return email address
- ✓ include physical address
- ✓ identify messages as commercial
- ✓ offer clear and conspicuous opt-out
- ✓ process opt-outs within 10 days
- ✓ follow FTC (and FCC) regulations

do not fax

- **FCC regs prohibit unsolicited commercial faxes – since 1991**
- **new regulations require specific written authorization**
- **no exception for existing business relationship**
- **private right of action, statutory damages up to \$500 per fax**
- **Fax.com hit with \$5.3 million fine – on top of \$2.3 million judgment**
- **Hooters, Carnett – class actions and multimillion dollar liability**

no rules
yet

- **Direct mail**
- **Subservientchicken.com**




laws
compel
disclosure

- **Bank Secrecy Act**
- **USA PATRIOT Act**
- **Communications Assistance to Law Enforcement Act (CALEA)**
- **regulatory reporting requirements**
(e.g., FDA)
- **civil & criminal subpoenas**



the
privacy
act of '74

- **Who is covered?**
 - ✓ **Federal government entities and contractors**
- **What is covered?**
 - ✓ **personal info of US citizens and residents**
- **What is required or prohibited?**
 - ✓ **agencies can only compile data that is “relevant and necessary”; they must provide notice of new systems of record, access to data, and disclosures of data are limited**
- **Who enforces?**
 - ✓ **private right of action, with civil and criminal penalties for agencies and gov’t employees**
- *Why does this law exist?*
 - ✓ *concerns over government misuse of citizen data in computerized databases*



**compliance
basics**

compliance

privacy leaders

- **help define the corporate information policy values**
- **provide traditional legal compliance advice as well as business advice regarding best practices, risks and benefits**
- **craft enterprise-wide solutions that meet consumer expectations while providing appropriate data flow opportunities**
- **find the right balance for the company, given the company's culture and corporate goals**

four risks

four risks to manage

- **legal compliance** – *with laws, regulations, self-regulatory regimes & contracts*
- **reputation** – *not going beyond what people think is appropriate, even if it's legally ok*
- **investment** – *getting the proper return on information and technology*
- **reticence** – *doing what you need to do to grow your business*

privacy & security concerns permeate each of these

holistic programs

think about compliance holistically

- **consider your corporate culture and values**
- **understand your organization's data collection and sharing practices**
- **brainstorm about long term data & technology plans; anticipate outsourcing relationships, new products, channels, markets**
- **analyze public concerns, industry practices, the regulatory climate**
- *and then evaluate all of the legal and business risks*

**key
program
components**

- **values-oriented, permits flexible, enterprise-wide planning**
- **deep understanding of all data flows**
- **policies & procedures are designed around company needs and industry best practices**
- **formal implementation controls, testing, documentation, training**
- ***consumer-oriented* privacy statements**
- **“affirmation-education cycle” used to monitor and adjust**
- **supports compliance, advocacy, marketing, sales, customer service, product development, public relations...**

four basic
steps

Discover

*Issue Identification & Self-Assessment
Determination of Best Practices*

Build

*Procedure Development & Verification
Full Implementation*

Communicate

*Documentation
Education*

Evolve

*Affirmation and Monitoring
Adaptation*

managing vendors

- **you are always responsible for the actions of those who process data for you**
- **start with due diligence – establish a formal vendor qualification program**
 - **established security program?**
 - **employee management & training?**
 - **ability to segregate your data?**
 - **ability to meet your standards?**
 - **audited when & by whom?**
- **then understand the deal – what data? going where? how? how do the vendor's security protocols match up with your protocols?**

vendor contracts

- **standard confidentiality provision is a good *start*...**
- **add specific standards, appropriate given the relationship**
 - **employee screening, training**
 - **data transmission standards**
 - **access controls**
 - **computer security standards**
 - **incident response & reporting**
 - **insurance, indemnification**
 - **audit rights**
 - **remedies**
- **and have a plan for disaster ready, just in case**



**theories
of legal
liability**

Legal

private litigation

- **contract disputes**
occur when one person claims that another person breached an agreement that the two people had
- **tort (personal injury) claims**
occurs when a person sues another person to redress some wrong

breach of contract

contract

- *agreement between two or more parties that creates in each party a duty to do or not do something and a right to performance of the other's duty or a remedy for the breach of the other's duty*
- **a privacy notice is a contract if consumer provides data to company based on the company's promise to use the data in accordance with the terms of the notice**

tort of
negligence

negligence

- *an organization is negligent if:*
 1. *it has a duty*
 2. *it breaches that duty*
 3. *someone is harmed by that breach*
 4. *the harm includes actual damages*
- **a company will be liable for damages if it breaches a legal duty to protect personal information and an individual is harmed by that breach**
- **damages can be economic or non-economic**

**unfair &
deceptive
trade
practices**

regulatory agencies and enforcement authorities protect consumers against unfair, deceptive or fraudulent practices

- **deceptive trade practices:**
commercial conduct that includes false or misleading claims, or claims that omit material facts
- **unfair trade practices**
commercial conduct that (1) causes substantial injury, (2) without offsetting benefits, and (3) that consumers cannot reasonably avoid

**unfair &
deceptive
trade
practices**

“It's simple – if you collect information and promise not to share, you can't share unless the consumer agrees,” said Howard Beales, Director of the FTC’s Bureau of Consumer Protection. “You can change the rules but not after the game has been played.”

“Gateway Learning Settles FTC Privacy Charges” FTC Press Release, July 7, 2004

enforcement actions

- **your company's practices are "featured" in the newspaper**
- **you get a fax from the FTC, a "voluntary request" for documents and information**
- **the FTC already thinks (and may have evidence) that you broke the law**
- **you need a prompt, formal response telling them why they shouldn't sue you**
- **but things are probably going to get worse before they get better**
- **settlement agreements can be costly**
- **state AGs will probably contact you too**

settlement terms

e.g., for a security breach

- no further misrepresentations
- establish and maintain a security program
 - employee training and oversight
 - identify and manage reasonably foreseeable risks
 - implement appropriate safeguards
 - evaluate the program regularly
- annual independent review
- provide documents to FTC on ongoing basis, notify FTC of changes to your program
- for at least 20 years
- the state AGs will want money

it's
never
forgotten

- **the Fourth Estate ensure that no misstep is ever forgotten**
- **you can survive the first oops, but trust plummets if you have more than one**
- **lost opportunity costs going forward will be even greater than your actual out-of-pocket expenses for the breach**

an ounce of prevention is worth a pound of cure.

final thoughts

- **privacy regulation is only going to get more complex**
- **building trust is the key –**
 - **trust = value * security * privacy**
 - **trust makes your stakeholders more receptive to your messages and use of information**
 - **trust also makes your stakeholders less likely to complain**
- **but managing real risks is vital too**
 - **legal compliance**
 - **security breaches**



**build
trust**

- **manage all four risks:**
 - legal compliance
 - reputation
 - investment
 - reticence
- **assess your own practices regularly**
- **choose vendors carefully**
- **proactively monitor the legal climate**
- **be sensitive to people's needs and expectations – and have a value proposition that you can articulate for every audience**



IAPP Certification: *Promoting Privacy*