Privacy Legislation

1. Federal Privacy Act (1974)

- governs collection, maintenance, use & dissemination of public records by federal agencies

… numerous amendments over the years

a. records on individuals by federal agencies must be for a lawful and necessary purpose

b. must provide adequate safeguards against misuse

c. any citizen can:

- find what information is being collected on them by each agency
- access, copy, and make corrections
- prevent use of the information for other purposes - no longer true! Government agency requirement is now one of informing the individual

2. Other Federal Legislation

Wiretap Act (1968)

– government needs probable cause and warrant to tap telephone and oral communications

Fair Credit Reporting Act (1970)

- protects consumers from willful and/or negligent inclusion of inaccurate information in credit reports
- specifies valid uses/users & permission typically required
- right to see and challenge the information held
- information in database expires and is expunged after reasonable period of time
- easy to identify and dispute inaccurate information (annualcreditreport.com)

Family Educational Rights and Privacy Act (1974)

- governs access to educational information and records
- applies to schools and institutions receiving funds from US Dept of Education
- gives parents access to child's education records, opportunity amend records, and some control over disclosure
- after 18, schools must have student's consent prior to disclosure
- written permission required by parent or by student over 18
- disclosures of directory information allowed

Right to Financial Privacy Act (1978)

- government must receive the consent of customer of bank or financial institution customer before it can access the financial information

1986: Congress amended RFPA to allow the government to compel disclosure of requested information.

2001: USA PATRIOT Act amended the RFPA

Privacy Protection Act (1980)

- protects journalists from being required to turn over to law enforcement their work product and documentary materials, including sources, before disseminated to the public

Electronic Fund Transfer Act (1980)

- Banks must notify you about third party access to account
- A customer can be liable for unauthorized withdrawals if card is lost or stolen and do not follow certain criteria:

Loss:

- limited to $50 if institution notified within two business days
- could be up to $500 if institution notified between 3 and 59 days
- not reported within 60 business days, customer risks unlimited loss on transfers made after the 60-day period (all money in account plus maximum over draft)

Electronic Communications Privacy Act (1986)
- expands wiretap act of 1968 to include electronic communications
- lists procedures govt must use when using electronic surveillance

Stored Communications Act (1986)
- addresses voluntary and compelled disclosures of "stored wire and electronic communications and transaction records held by ISPs
- only subpoena and prior notice required to force ISP to disclose contents of an email of files on a server … far less burden than probable cause

Video Privacy Protection Act (1988), **HIPPA** (1996), **Telecommunications Act** (1996), etc.

Homeland Security Act (2002)
- aftermath from twin tower attacks on 2/11/2001
- goal was to prepare for, prevent, and respond to domestic emergencies, particularly terrorism
- consolidated numerous U.S. executive branch organizations into a single agency

Incorporated staunch domestic privacy protections:
- federal government may NOT monitor private activities without warrant supported by probable cause
- major doubts that law is being followed (Edward Snowden leaks in 2013 of NSA documents)
- state-sponsored domestic surveillance likely with numerous legislative amendments suggested to address

3. Similar privacy acts in each State
- apply most often to state and local government agencies
- some consumer privacy legislation as well

Examples:
- mandatory disclosures in the event of personal information accessed by hackers
- websites must post privacy policies
- must comply with own published privacy policies
- must provide data collection opt out opportunities
- must identify personal data that app or site collects
- must comply with "Do Not Track" requests

… these are typically exceptions rather than the rule

4. Current U.S. Legislative Status

- no uniform or overarching legal structure for protecting online privacy at U.S. federal level
- Congress likely to continue to act only in ad hoc sectoral manner when confronted by crisis
- State laws stepping in
  … substantial efficacy if numerous states pass similar consumer protection laws but quite constrained by current U.S. Supreme Court
- Global Effect:
  e-commerce firms serving global audiences must meet EU's more stringent data privacy provisions – too constraining or insufficient?

5. European Union General Data Protection Regulation (2016)

Goals:

- give control to people over their personal data
- simplify commerce by unifying regulations across EU

Key Points:

• Applies to processing personal information about data subjects in European Economic Area (EEA) regardless of where the processing occurs

• Data controllers must design systems with privacy in mind (e.g. must use highest-possible privacy settings by default)

• No personal data may be processed unless processing is done under one of six lawful bases that are specified in detail by the regulation

- consent
- contract
- public task
- vital interest
- legitimate interest
- legal requirement

• When data processing is based on consent, data subject has the right to revoke it at any time.

.... extensive further notification, transparency, and responsiveness provisions with major sanctions for violations

Privately Owned Databases in the U.S.

Perhaps the greatest threat to individual privacy in the U.S. is the private commercial sector.