Chapter 6 (Privacy and the Government): 6.1 Introduction

- Driver's Privacy Protection Act (1994) prohibits states to provide certain personal information provided by drivers, must share this information with federal government
- majority of Americans generally support surveillance for the greater good of society
- Daniel Solove's four groups of privacy-related activities:
    - **information collection**: gather
    - **information processing**: store, manipulate, use
    - **information dissemination**: spread
    - **invasion**: intrude a person's daily life, interrupt their solitude, or interfere with their decision making

Chapter 6 (Privacy and the Government): 6.2 USA Legislation Restricting Information Collection

- Employee Polygraph Protection Act (1988)
    - prohibits most private employers from using lie-detector tests
    - governments and some exceptional situations are fine
- Children's Online Privacy Protection Act (2000)
    - need parental consent to collect children's (0-12) information
- Genetic Information Nondiscrimination Act (2008)
    - prevent discrimination in medical benefits + employment based on genetic information
    - does not apply to life insurance, disability insurance, long-term care insurance, companies w/ 15 or fewer employees, and more

Chapter 6 (Privacy and the Government): 6.3-6.4 Information Collection by the Government + Covert Government Surveillance

- ways the American government has citizen information:
    - census records, can share this information in national emergencies
    - national income tax, originally just used to pay for Civil War expenses
    - FBI NCIC 2000, DBs that support law enforcement
        - eg used to store suspected terrorists
        - critics: can arrest innocent people w/ same name, people with access have sold information
    - CCTV + drones
        - critics: vast majority of people are truly innocent, not very police-like to violate this much privacy
    - **wiretapping (calls) + bugs (audio), both felonies but still used by authority figures**

        - most common critique: **people with access can use information for malicious purposes**
        - TALON database
- Fourth Amendment: protection against unreasonable searches and seizures by the government

Chapter 6 (Privacy and the Government): 6.5 USA Legislation Authorizing Wiretapping

- **government argues that in cases of national security, should be allowed to wiretap**
- Foreign Intelligence Surveillance Act (1978): does not allow targeting of any American citizen or anyone located within the USA
    - NSA can still gain access to servers of the largest corporations at will
- Electronic Communications Privacy Act (1986): can place pen register and trap-and-trace device on a suspected phone line
    - can legally use **roving wiretaps**: wiretaps that move from phone to phone if the suspect is suspected of avoiding surveillance via multiple phones
- Stored Communications Act: government does not need search warrant for emails from Internet service providers over 180 days old
    - many companies against, believe a warrant should always be required
- Communications Assistance for Law Enforcement Act (1994): networking equipment should be designed/modified to allow for wiretapping

Chapter 6 (Privacy and the Government): 6.6 USA PATRIOT Act

- Patriot Act: anti-terrorism via more rights infringement
    - higher figures can intercept communications if they suspect terrorism
    - FBI can issue a National Security Letter to obtain a search warrant on an individual given that the suspected activities being investigated does not infringe the First Amendment
    - critics: too much power to federal government, reduces rights of law-abiding American citizens
    - **very unpopular to many citizens, but even big corporations are in on it with the government**
- **has worked many times, but Brandon Mayfield incident shows that it can be abused to the extreme**

Chapter 6 (Privacy and the Government): 6.7 Regulation of Public and Private DBs

- Privacy Act of 1974: Richardson Committee established Code of Fair Information Practices
    - limitations:
        - only applies to government DBs

        - federal government does not enforce it well
        - allows agencies to share records amongst themselves for “routine use”, which is also undefined
- Fair Credit Reporting Act: credit bureaus must provide one free copy per year and can keep negative information temporarily (with exceptions, such as criminal records)
- Financial Services Modernization Act: financial institutions must disclose their privacy policies to customers

Chapter 6 (Privacy and the Government): 6.8 Data Mining by the Government

- used to audit tax returns by IRS to catch people and hand out penalties
- syndromic surveillance systems used to find general patterns that might indicate an epidemic, bioterrorism, etc
- predictive policing used to deploy police officers to crime-ridden areas
- **potential harm: learning algorithms can construct erroneous potential terrorist files, hard to clear up the individual’s name**

Chapter 6 (Privacy and the Government): 6.9 National Identification Card

- SSN pro: de facto national identification number in the USA
- SSN cons: not unique (historical beginnings), rarely checked, easy to fake, no error-detecting capability
- national ID card pros: more reliable than social security card + driver's license, reduces illegal immigration, reduces crime via identification, does not undermine democracy
- national ID card cons: can still probably be forged, never will be 100% accurate for identification, does not reduce crime since prosecution needs evidence and not identification, simpler for governments to perform data mining, erroneous information will haunt individuals longer
- REAL ID Act pros: biometric identifier (stronger than previous licenses), more levels of security for administration
- REAL ID Act cons: essentially makes driver license a national ID card, too much personal information shared with federal and state governments

Chapter 6 (Privacy and the Government): 6.10-6.11 Information Dissemination + Invasion

- government has full authority to withhold documents for: national defence, foreign policy, trade secrets, confidential commercial or financial information
- even tollbooths used to gather information, can even be used in court
- privacy is just a prudential right

    - telemarketing can still allow certain unsolicited advertisements to reach you, even if you are on the Do Not Call Registry
    - TV commercials must be played at the same volume
    - **respects your privacy rights, but only to a certain degree, for the greater benefit of society**

<u>Chapter 6 (Privacy and the Government) Food for Thought</u>

- in times of national security concerns, individual privacy seems to always be compromised
- **government seems to violate laws regarding individual privacy pretty often**
    - usually for valid concerns, but always susceptible to misuse, has happened many times
- **government loves using fancy wording and policies to justify their activities**
    - eg REAL ID Act makes the driver's license pretty much a national ID card