

Chapter 6: Privacy and the Government



COMP422 Ethics and Professional Issues in Computing
Dr. Patrick Pang

Based on
Ethics for the Information Age (5th Ed.)
by
Michael J. Quinn



澳門理工學院
Instituto Politécnico de Macau
Macao Polytechnic Institute

Chapter Overview

- Introduction
- Information collection by the government
- Covert government surveillance
- Regulation of public and private databases
- Data mining by the government
- National identification card
- Information dissemination
- Invasion

6.1 Introduction

A Balancing Act

- Federal, state, and local governments in United States have had significant impact of privacy of individuals
- Government must balance competing desires
 - desire to be left alone
 - desire for safety and security
- National security concerns increased significantly after 9/11 attacks

Solove's Taxonomy of Privacy

- **Information collection:** Activities that gather personal information
- **Information processing:** Activities that store, manipulate, and use personal information that has been collected
- **Information dissemination:** Activities that spread personal information
- **Invasion:** Activities that intrude upon a person's daily life, interrupt someone's solitude, or interfere with decision-making

6.2 Information Collection by the Government

Census Records

- Census required to ensure every state has fair representation
- Number of questions steadily rising
- Sometimes Census Bureau has broken confidentiality requirement
 - World War I: draft resisters
 - World War II: Japanese-Americans

Japanese-Americans on Way to Internment Camp in 1942



National Archives, file #210-G-3B-414)

After the Japanese attack on Pearl Harbor, the Army used information illegally obtained from the Census Bureau to round up Japanese-Americans.

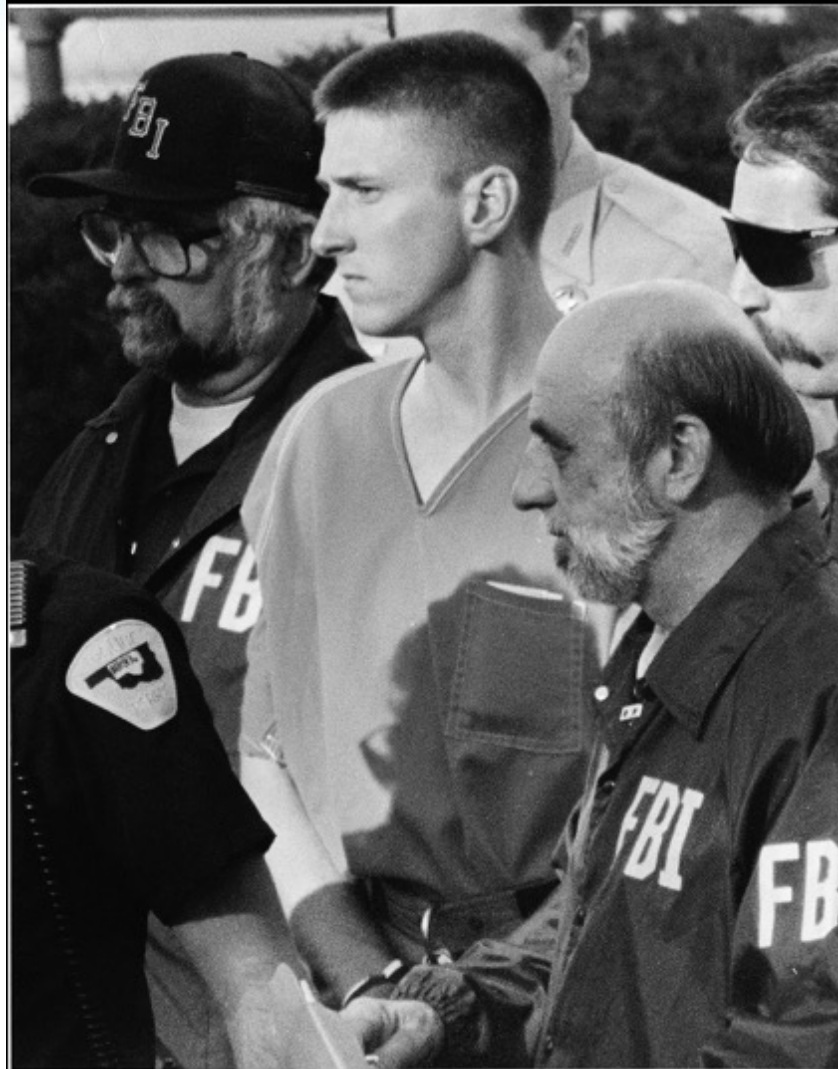
Internal Revenue Service Records

- The 16th Amendment to the U.S. Constitution gives the federal government the power to collect an income tax
- IRS collects more than \$2 trillion a year in income taxes
- Income tax forms contain a tremendous amount of personal information: income, assets, to whom you make charitable contributions, medical expenses, and more

FBI National Crime Information Center 2000

- NCIC
 - Collection of databases related to various crimes
 - Contains > 39 million records
- Successes
 - Helps police solve hundreds of thousands of cases every year
 - Helped FBI tie James Earl Ray to assassination of Dr. Martin Luther King, Jr.
 - Helped FBI apprehend Timothy McVeigh for bombing of federal building in Oklahoma City

Timothy McVeigh



© Bob E.Daemmrch/Sygma/Corbis

OneDOJ Database

- Database being constructed by U.S. Department of Justice
- Gives state and local police officers access to information provided by five federal law enforcement agencies
 - Incident reports
 - Interrogation summaries
 - Other information not available through NCIC
- Criticisms
 - OneDOJ gives local police access to information about people who have not been charged with a crime
 - There is no way to correct misinformation in raw police reports

Closed-circuit Television Cameras

- First use in Olean, New York in 1968
- Now more than 30 million cameras in U.S.
- New York City's effort in lower Manhattan
 - \$201 million for 3,000 new cameras
 - License plate readers
 - Radiation detectors
- Effectiveness of cameras debated

Number of Surveillance Cameras Keeps Increasing



6.3 Covert Government Surveillance

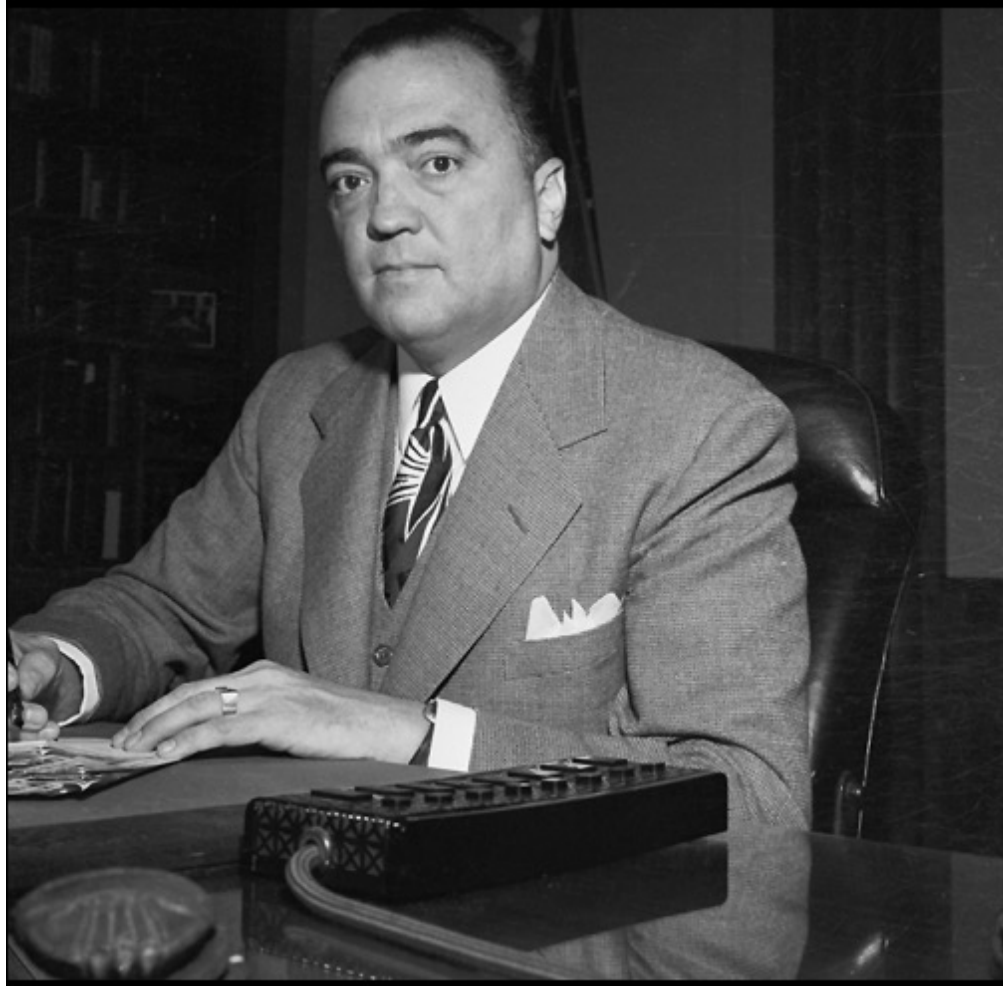
4th Amendment to U.S. Constitution

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

Wiretaps and Bugs

- *Omstead v. United States* — wiretapping OK
- Federal Communications Act — wiretapping made illegal
- *Nardone v. United States* — wiretapping not OK
- FBI continues secret wiretapping
- *Katz v. United States* — bugs not OK

J. Edgar Hoover



© Bettmann/CORBIS

Operation Shamrock

- Continuation of World War II interception of international telegrams
- National Security Agency (1952)
- Expanded to telephone calls
- Kennedy
 - Organized crime figures
 - Cuba-related individuals and businesses
- Johnson and Nixon
 - Vietnam war protesters
- Nixon
 - War on drugs

Carnivore Surveillance System

- Created by FBI in late 1990s
- Monitored Internet traffic, including email exchanges
- Carnivore = Windows PC + “packet-sniffing” software
- Captured packets going to/from a particular IP address
- Used about 25 times between 1998 and 2000
- Replaced with commercial software

Covert Activities after 9/11

- September 11, 2001 attacks on World Trade Center and Pentagon
- President Bush authorized new, secret, intelligence-gathering operations inside United States

National Security Administration

Wiretapping

- President Bush signed presidential order
 - OK for NSA to intercept international phone calls & emails initiated by people inside U.S.
 - No search warrant required
- Number of people monitored
 - About 500 people inside U.S.
 - Another 5,000-7,000 people outside U.S.
- Two al-Qaeda plots foiled
 - Plot to take down Brooklyn bridge
 - Plot to bomb British pubs and train stations

TALON Database

- TALON – Threat and Local Observation Notices
- Created by U.S. Department of Defense in 2003
- Supposed to contain reports of suspicious activities or terrorist threats near military bases
- Reports submitted by military personnel or civilians
- Reports assessed as “credible” or “not credible” by military experts
- Reports about anti-war protests added to database
- Many of these reports later deleted from database
- In 2007 new Under Secretary of Defense for Intelligence recommended that TALON be terminated

6.4 Regulation of Public and Private Databases

Genesis of Code of Fair Information Practices

- 1965: Director of Budget asked committee of economists to look at problems caused by decentralization of statistical data across federal agencies
- Committee recommended creation of a National Data Center
- Citizens and legislators expressed concerns about possible abuses of such a system
- Another group formed to draft guidelines for government databases

Code of Fair Information Practices

- No secret databases
- People should have access to personal information in databases
- Organizations cannot change how information is used without consent
- People should be able to correct or amend records
- Database owners, users responsible for reliability of data and preventing misuse

Privacy Act of 1974 Falls Short

- Applies only to government databases
- Only covers records indexed by a personal ID
- No federal employee responsible to enforcing Privacy Act provisions
- Allows agencies to share records with other agencies

Legislation for Private Institutions

- Fair Credit Reporting Act
- Fair and Accurate Credit Transactions Act
- Financial Services Modernization Act

Fair Credit Reporting Act

- Passed in 1970, revised in 1996
- Promotes accuracy and privacy of information used by credit bureaus
- Major credit bureaus: Equifax, Experian, [Trans Union](#)
- Negative information kept only 7 years
- Exceptions
 - Bankruptcies: 10 years
 - Criminal convictions: indefinitely

Fair and Accurate Credit Transactions Act

- Passed in 2004
- Requires three major credit bureaus to provide consumers a free copy of their credit report every 12 months
- Not automatic: consumers must request credit reports
- Provisions to reduce identity theft

Financial Services Modernization Act

- Also called Gramm-Leach-Bliley Act of 1999
- Creates “financial supermarkets” offering banking, insurance, and brokerage services
- Privacy-related provisions
 - Privacy policies must be disclosed to customers
 - Notices must provide an opt-out clause
 - Companies must develop procedures to protect customers’ confidential information

6.5 Data Mining by the Government

Definition of Data Mining

- Data mining: Process of searching through one or more databases looking for patterns or relationships among the data

IRS Audits

- IRS uses computer matching and data mining to look for possible income tax fraud
- Computer matching: matching tax form information with information provided by employers, banks, etc.
- Data mining: searching through forms to detect those that appear most likely to have errors resulting in underpayment of taxes

Syndromic Surveillance Systems

- Syndromic surveillance system: A data mining system that searches for patterns indicating the outbreak of an epidemic or bioterrorism
 - 911 calls
 - emergency room visits
 - school absenteeism
 - Internet searches
- Example: A system in New York City detected an outbreak of a virus in 2002

Telecommunications Records Database

- Created by National Security Agency after 9/11
- Contains phone call records of tens of millions of Americans
- NSA analyzing calling patterns to detect terrorist networks
- Phone records voluntarily provided by several major telecommunications companies
- *USA Today* revealed existence of database in May 2006
- Several dozen class-action lawsuits filed
- August 2006: Federal judge in Detroit ruled program illegal and unconstitutional
- July 2007: U.S. Court of Appeals overturned ruling, saying plaintiffs did not have standing to bring suit forward

6.6 National Identification Card

History, Role of Social Security Number

- Social Security cards first issued 1936
- Originally used only for SS purposes
- Use of SSN has gradually increased
- SSN is a poor identification number
 - Not unique
 - Rarely checked
 - No error-detecting capability

Arguments for a National ID Card

- Current ID cards are second-rate
- Would reduce illegal entry to U.S.
- Would prevent illegal aliens from working
- Would reduce crime
- Other democratic countries have national ID cards

Arguments against a National ID Card

- No card positively guarantees identification
- No biometric-based system is 100% accurate
- No evidence it will reduce crime
- Makes government data mining simpler
- Make law-abiding people more vulnerable to fraud and indiscretions

The REAL ID Act

- Signed in May 2005
- Significantly changes driver's licenses in the United States
- New licenses
 - Issued by end of 2013
 - Required to open bank account, fly on commercial airplane, or receive government service
 - Requires applicants to supply 4 different IDs
 - Will probably contain a biometric identifier
 - Must contain data in machine-readable form
- Half of the states have resisted implementation of REAL ID; doubtful 2013 deadline will be met

Possible Consequences of New Licenses

- Better identification means better law enforcement
- People won't be able to change identities
 - Parents ducking child support
 - Criminals on the run
- New, centralized databases could lead to more identity theft

6.7 Information Dissemination

- Legislation to restrict information dissemination
 - Family Education Rights and Privacy Act
 - Video Privacy Protection Act
 - Health Insurance Portability and Accountability Act
- Examples of information dissemination
 - Freedom of Information Act
 - Toll booth records used in court

Family Education Rights and Privacy Act (FERPA)

- Rights given to
 - Students 18 years and older
 - Parents of younger students
- Rights include
 - Reviewing educational records
 - Requesting changes to erroneous records
 - Preventing release of records without permission

Video Privacy Protection Act

- Videotape service providers cannot disclose rental records without consumer's written consent
- Rental stores must destroy personal information related to rentals within a year of when it is no longer needed

Judge Robert Bork



AP Photo/Charles Tasnadi

Health Insurance Portability and Accountability Act

- Limits how doctors, hospitals, pharmacies, and insurance companies can use medical information
- Health care providers need signed authorization to release information
- Health care providers must provide patients with notice describing how they use medical information

Freedom of Information Act

- Federal law designed to ensure public has access to U.S. government records
- Signed by President Johnson (1966)
- Applies only to executive branch
- Nine exemptions
 - Classified documents
 - Trade secrets or financial information
 - Documents related to law enforcement investigations

Toll Booth Records

- E-ZPass: an automatic toll-collection system used on most toll roads, bridges, and tunnels between Illinois and Maine
- Drivers with E-ZPass tags pass through without stopping to pay attendant
- Records have been provided in response to court orders in criminal and civil cases

6.8 Invasion

- Government actions to prevent invasion
 - Do Not Call Registry
 - CALM Act
- Invasive government actions
 - Requiring identification for pseudoephedrine purchases
 - Advanced Imaging Technology scanners at airports

National Do Not Call Registry

- FTC (Federal Trade Commission) responded to public opinion
 - Created Do Not Call Registry in 2003
 - More than 50 million phone numbers registered before it even took affect
- Example of how privacy is treated as a prudential right
 - Benefit of shielding people from telemarketers judged to be greater than harm caused by limiting telephone advertising

CALM Act

- Television watchers have complained to FCC (Federal Communications Commission) about loud commercials since 1960s
- CALM (Commercial Advertisement Loudness Mitigation) Act signed by President Obama in 2010
- Requires FCC to ensure television commercials are played at same volume as programs they are interrupting

Pseudoephedrine Purchases

- Pseudoephedrine an ingredient of Sudafed and other cold medications
- It is also an ingredient of methamphetamine (“meth”)
- Federal and state governments have passed laws limiting access to pseudoephedrine
 - Limits quantity that can be purchased in a month
 - Identification and signature required for purchase in most states

Advanced Imaging Technology Scanners

- Transportation Security Administration began installing AIT scanners in 2007
- AIT scanners reveal anatomical features
- Electronic Privacy Information Center sued government in 2010, saying systems violate 4th Amendment and various laws
- February 2011: TSA announced it was developing new software that would replace detailed image with generic outline of a person

Advanced Imaging Technology Scanner

