**Handouts of Lecture 31 Professional Practices (IT)**

**Lecture Title: Privacy and the Government**

**Electronic Communications Privacy Act**

Congress updated the wiretapping law in 1986 with the passage of the Electronic Communications Privacy Act (ECPA). The ECPA allows police to attach two kinds of surveillance devices to a suspect’s phone line. If the suspect makes a phone call, a pen register displays the number being dialed. If the suspect gets a phone call, a trap-and-trace device displays the caller’s phone number. While a court order is needed to approve the installation of pen registers and trap-and-trace devices, prosecutors do not need to demonstrate probable cause, and the approval is virtually automatic.

The ECPA also allows police to conduct roving wiretaps (following suspect from phone to phone).

**Stored Communications Act**

The Stored Communications Act, part of the Electronic Communications Privacy Act, has significant privacy implications related to the collection of email messages. Under this law, the government does not need a search warrant to obtain from an Internet service provider email messages more than 180 days old. In other words, when a computer user allows an Internet service provider to store his or her email messages, the user is giving up the expectation of privacy of that information.

Nearly 50 companies and privacy rights organizations, including AOL, the American Civil Liberties Union, the American Library Association, AT&T, Consumer Action, the Electronic Frontier Foundation, Facebook, Google, IBM, Intel, and Microsoft, have joined forces to form an organization called Digital Due Process, which is lobbying Congress to update the Electronic Communications Privacy Act. Today most Internet service providers supply convenient, long-term storage of their customers’ emails, and millions of customers take advantage of this service to hold their messages indefinitely. With the advent of cloud computing, companies such as Amazon, Google, and Microsoft are storing sensitive documents and other materials that in the past would have been held on personal computers.

**Communications Assistance for Law Enforcement Act**

The implementation of digital phone networks interfered with the wiretapping ability of the FBI and other organizations. In response to these technological changes, Congress passed the Communications Assistance for Law Enforcement Act of 1994 (CALEA), also known as the Digital Telephony Act. This law required that networking equipment used by phone companies be designed or modified so that law enforcement agencies can trace calls, listen in on telephone calls, and intercept email messages. CALEA thereby ensured that court-ordered wiretapping would still be possible even as new digital technologies were introduced.

The FBI asked for many capabilities, including the ability to intercept digits typed by the caller after the phone call was placed. This feature would let it catch credit card numbers and bank account numbers, for example. In 1999 the FCC finally issued the guidelines, which included this capability and five more requested by the FBI [38]. Privacy rights organizations argued these capabilities went beyond the authorization of CALEA.

**USA PATRIOT Act**

**Provisions**

The Patriot Act amended many existing laws. Its provisions fall into four principal

Categories:

1. Providing federal law enforcement and intelligence officials with greater authority to monitor communications

2. Giving the Secretary of the Treasury greater powers to regulate banks, preventing them from being used to launder foreign money

3. Making it more difficult for terrorists to enter the United States

4. Defining new crimes and penalties for terrorist activity.

**Critics say Act undermines 4th Amendment rights**

Law enforcement agencies seeking to install a wiretap or a pen register/trap-and trace device have always been required to get a court order from a judge with jurisdiction over the location where the device was to be installed.

The Patriot Act broadened the number of circumstances under which roving surveillance can take place. Previously, roving surveillance could only be done for the purpose of law enforcement, and the agency had to demonstrate to the court that the person under investigation actually used the device to be monitored. The Patriot Act allows roving surveillance to be performed for the purpose of intelligence, and the government does not have to prove that the person under investigation actually uses the device to be tapped.

Under the Patriot Act, law enforcement officials wishing to intercept communications to and from a person who has illegally gained access to a computer system do not need a court order if they have the permission of the owner of the computer system.

The Patriot Act allows courts to authorize law enforcement officers to search a person’s premises without first serving a search warrant when there is “reasonable cause to believe that providing immediate notification of the execution of the warrant may have an adverse effect.”

**National Security Letters**

The Patriot Act expanded the use of National Security Letters, making it easier for the FBI to collect Internet, business, medical, educational, library, and church/mosque/ synagogue records. To obtain a search warrant authorizing the collection of records about an individual, the FBI merely needs to issue a National Security Letter stating that the records are related to an ongoing investigation.

A typical National Security Letter contains a gag order that forbids the letter’s recipient from disclosing receipt of the letter. National Security Letters are controversial because, unlike warrants, they do not require the approval of a judge. That means there is no need for the FBI to show probable cause. Between 2003 and 2006, the FBI issued 192,499 National Security Letters.

**NSA Access to Telephone Records**

Edward Snowden leaked documents to the Guardian newspaper. These call records, also called telephony metadata, included the date and time of each telephone call, the location of the phone making the call, the duration of the conversation, and “other identifying information.” Verizon was not asked to provide the contents of the conversations.

Guardian revealed Foreign Intelligence Surveillance Court had ordered Verizon to provide NSA with all of its telephone metadata for 3-month period in 2013 (date, time, location, and length of call, but not contents of call)

Guardian critique: NSA’s mission now “focuses increasingly on domestic communications”

Obama administration: Court orders for telephone records “are something that have been in place a number of years now.

**Regulation of Public and Private Databases**

**Code of Fair Information Practices**

The secretary’s Advisory Committee of Automated Personal Data Systems, Records, Computers, and the Rights of Citizens produced a report for Congress, which included the following “bill of rights” for the Information Age.

* There must be no personal data record-keeping systems whose very existence is secret.
* There must be a way for a person to find out what information about the person is in a record and how it is used.
* There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person’s consent.
* There must be a way for a person to correct or amend a record of identifiable information about the person.
* Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

**Privacy Act of 1974 Falls Short**

The Privacy Act of 1974 represents Congress’s codification of the principles described in the Code of Fair Information Practices. While the Privacy Act does allow individuals in some cases to get access to federal files containing information about them, in other respects it has fallen short of the desires of privacy advocates.

The Privacy Act has the following principal limitations.

1. The Privacy Act applies only to government databases.

2. The Privacy Act only covers records indexed by a personal identifier.

3. No one in the federal government is in charge of enforcing the provisions of the Privacy Act.

4. The Privacy Act allows one agency to share records with another agency as long as they are for a “routine use.”

**Legislation for Private Institutions**

Although the Privacy Act applies only to government databases, Congress has passed legislation regulating how some private institutions manage databases containing sensitive information about individuals, and these laws put into effect many of the principles of the Code of Fair Information Practices.

***The Fair Credit Reporting Act***, passed in 1970 and revised in 1996, was designed to promote the accuracy and privacy of information used by credit bureaus and other consumer reporting agencies to produce consumer reports. It also ensures that negative information does not haunt a consumer for a lifetime.

***The Fair and Accurate Credit Transactions Act*** of 2004 requires the three major credit bureaus to provide consumers a free copy of their credit report every 12 months. Consumers can use this opportunity to detect and correct errors in their credit reports. The bureaus do not issue the reports automatically; consumers must take the initiative and request them from AnnualCreditReport.com.

***The Financial Services Modernization Act*** (also called the Gramm-Leach-Bliley Act of 1999) contains dozens of provisions related to how financial institutions do business. One of the major provisions of the law allows the creation of “financial supermarkets” offering banking, insurance, and brokerage services. The law also contains some privacy-related provisions. It requires financial institutions to disclose their privacy policies to their customers. When a customer establishes an account, and at least once per year thereafter, the institution must let the customer know the kinds of information it collects and how it uses that information.

**Data Mining by the Government**

Data mining is the process of searching through one or more databases looking for patterns or relationships among the data. In this section we continue our coverage of the information-processing category of Solove’s taxonomy by surveying a few well-known data-mining projects run by government agencies.

**IRS Audits**

To identify taxpayers who have paid less in taxes than they owe, the Internal Revenue Service (IRS) uses computer-matching and data-mining strategies. First, it matches information on the tax form with information provided by employers and financial institutions. This is a straightforward way to detect unreported income.

Second, the IRS audits a couple of million tax returns every year. Its goal is to select the most promising returns—those containing errors resulting in underpayment of taxes. The IRS uses a computerized system called the discriminant function (DIF) to score every tax return.

**Syndromic Surveillance Systems**

Another application of data mining by the government is protecting society from imminent dangers.

A syndromic surveillance system is a computerized system that analyzes 911 calls, visits to the emergency room, school absenteeism, purchases of prescription drugs, and Internet searches to find patterns that might indicate the onset of an epidemic, an environmental problem leading to illnesses, or bioterrorism.

In the fall of 2002, a syndromic surveillance system in New York City detected a surge in people seeking treatment for vomiting and diarrhea.

**Telecommunications Records Database**

Shortly after September 11, 2001, several major telecommunications providers began turning over the phone call records of tens of millions of Americans to the National Security Agency, without a court order. The NSA was not monitoring or recording the actual conversations; instead, it was analyzing calling patterns in order to detect potential terrorist networks.

After USA Today revealed the existence of the database in May 2006, more than a dozen class-action lawsuits were filed against the telecommunications companies. In August 2006, a federal judge in Detroit ruled the program to be illegal and unconstitutional, violating several statutes as well as the First and Fourth Amendments to the US Constitution [70]. In July 2007, the US Court of Appeals for the Sixth Circuit overturned the ruling on the grounds that the plaintiffs did not have standing to bring the suit forward.

**Predictive Policing**

Predictive policing is the use of data mining to deploy police officers to areas where crimes are more likely to occur. It is based on the observation that individual criminals act in a predictable way. For example, criminals tend to frequent familiar areas. If a car is burglarized, the probability increases that another car in the neighborhood will be burglarized. The times at which crimes occur can also fall into predictable patterns. Police in Santa Cruz and Los Angeles saw significant declines in property crime.

**National Identification Card**

**Social Security Number**

The Social Security Board contracted with the US Postal Service to distribute applications for Social Security cards. The post office collected the forms, typed the Social Security cards, and returned them to the applicants. In this way over 35 million Social Security cards were issued in 1936–1937.

The US government initially stated that Social Security numbers (SSNs) would be used solely by the Social Security Administration and not as a national identification card. In fact, from 1946 to 1972, the Social Security Administration put the following legend on the bottom of the cards it issued: “FOR SOCIAL SECURITY PURPOSES— NOT FOR IDENTIFICATION.” However, use of the SSN has gradually increased.

Unfortunately, the SSN has serious defects that make it a poor identification number. The first problem with SSNs is that they are not unique. When Social Security cards were first issued by post offices, different post offices accidentally assigned the same SSN to different people.

A second defect of SSNs is that they are rarely checked. Millions of Social Security cards have been issued to applicants without verifying that the information provided by the applicants is correct.

A third defect of SSNs is that they have no error-detecting capability, such as a check digit at the end of the number. In the case of SSNs, if a person accidentally types in the wrong number, there is a high likelihood that it is a valid SSN (albeit one assigned to a different person). Hence it is easy to contaminate databases with records containing incorrect SSNs.

**Arguments for National ID Card**

A national identification card would be more reliable than existing forms of identification.

* Social Security cards and driver’s licenses are too easy to forge.

A modern card could incorporate a photograph as well as a thumbprint or other biometric data.

* A national identification card could reduce illegal immigration.

Requiring employers to check a tamper-proof, forgery-proof national identification card would prevent illegal immigrants from working in the United States. If illegal immigrants couldn’t get work, they wouldn’t enter the United States in the first place.

* A national identification card would reduce crime.

Currently it’s too easy for criminals to mask their true identity. A tamper-proof national identification card would allow police to positively identify the people they apprehend.

* National identification cards do not undermine democracy.

Many democratic countries already use national ID cards, including Belgium, France, Germany, Greece, Luxembourg, Portugal, and Spain.

**Arguments against National ID Card**

* No card positively guarantees identification
* No biometric-based system is 100% accurate
* No evidence it will reduce crime
* A national identification card makes it simpler for government agencies to perform data mining on the activities of its citizens.
* While most people may feel they have nothing to fear from a national identification card system since they are law-abiding citizens, even law-abiding people are subject to fraud and the indiscretions and errors of others.

**The REAL ID Act**

In May 2005, President George W. Bush signed the REAL ID Act, which would significantly change driver’s licenses in the United States.

The REAL ID Act requires that every state issue new driver’s licenses. These licenses will be needed in order to open a bank account, fly on a commercial airplane, enter a federal building, or receive a government service, such as a Social Security check. The law makes it more difficult for impostors to get driver’s licenses, by requiring applicants to supply four different kinds of documentation and requiring state employees to verify these documents using federal databases.

Although each state is responsible for issuing new driver’s licenses to its citizens, these licenses must meet federal standards. The license must include the person’s full legal name, date of birth, gender, driver’s license number, digital photograph, legal address, and signature. All data on the license must be in machine-readable form. The license must have physical security features designed to prevent tampering, counterfeiting, or duplication.

Supporters of the measure say making the driver’s license a more reliable identifier will have numerous benefits. Law enforcement is easier when police can be more certain that a driver’s license correctly identifies the individual carrying it. Society is better off when parents ducking child support and criminals on the run cannot change their identities by crossing a state border and getting a new driver’s license under a different name.

**Information Dissemination**

**Family Education Rights and Privacy Act (FERPA)**

The Family Education Rights and Privacy Act (FERPA) provides students 18 years of age and older the right to review their educational records and to request changes to records that contain erroneous information. Students also have the right to prevent information in these records from being released without their permission, except under certain circumstances. For students under the age of 18, these rights are held by their parents or guardians. FERPA applies to all educational institutions that receive funds from the US Department of Education.

**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

**Health Insurance Portability and Accountability Act**

As part of the Health Insurance Portability and Accountability Act of 1996, Congress directed the Department of Health and Human Services (HHS) to come up with guidelines for protecting the privacy of patients.

These guidelines went into effect in April 2003. They limit how doctors, hospitals, pharmacies, and insurance companies can use medical information collected from patients. The regulations attempt to limit the exchange of information among health care providers to that information necessary to care for the patient. They forbid health care providers from releasing information to life insurance companies, banks, or other businesses without specific signed authorization from the person being treated.

**Freedom of Information Act**

The Freedom of Information Act is a law designed to ensure that the public has access to US government records. Signed into law by President Johnson in 1966, it applies only to the executive branch of the federal government, not the legislative or judicial branches. The act carries a presumption that the government will release the requested records. If an agency does not disclose records, it must explain why the information is being withheld.

**Toll Booth Records**

E-ZPass is an automatic toll collection system used on most toll roads, bridges, and tunnels between Illinois and Maine. Drivers who have installed an E-ZPass tag (an RFID transponder) in their vehicles are able to pass through toll booths without stopping to pay an attendant. Instead, an E-ZPass reader installed in the automated toll lane gets information from the tags of the cars that pass through and deducts the appropriate toll from each driver’s account. Records have been provided in response to court orders in criminal and civil cases.

**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**

Responding to this desire for greater privacy, the FTC (Federal Trade Commission) created the National Do Not Call Registry (www.donotcall.gov), a free service that allows people who do not wish to receive telemarketing calls to register their phone numbers. The public reacted enthusiastically to the availability of the Do Not Call Registry by registering more than 50 million phone numbers before it even took effect in October 2003.

The Do Not Call Registry has not eliminated 100 percent of unwanted solicitations. The regulations exempt political organizations, charities, and organizations conducting telephone surveys. The creation of the registry is a good example of how privacy is seen as a prudential right: the benefit of shielding people from telemarketers is judged to be greater than the harm caused by putting limits on telephone advertising.

**CALM Act**

* Television watchers have complained to FCC about loud commercials since 1960s
* CALM 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**

In an effort to curb the illegal production of methamphetamine (“meth”), federal and state governments have passed laws limiting access to products containing pseudoephedrine, which is used in the manufacture of methamphetamine. The Combat Methamphetamine Epidemic Act limits the quantity of pseudoephedrine that an individual can purchase in a month. Whether the laws have been effective is a matter of debate. In most states, original Sudafed is still sold behind the counter to adults, but 304 Chapter 6 Privacy and the Government they must show an identification card and fill out a sales log with their name, address, and signature.

**Advanced Imaging Technology Scanners**

Transportation Security Administration began installing AIT scanners in 2007. AIT scanners revealed anatomical features. Electronic Privacy Information Center sued government in 2010, saying systems violated 4th Amendment and various laws. TSA announced it would develop new software that would replace passenger-specific images with generic outlines.

In February 2011, the Transportation Security Administration announced that it was about to begin testing new software on its advanced imaging technology machines that would eliminate passenger-specific images. The tests were successful, and in January 2013 the TSA announced that all body scanners producing passenger-specific images would be removed from airport checkpoints by June 2013.

***Reference:***

***Lecture topic: Privacy and the Government Chapter 6***

***Gao, Y. (2012). Ethics for the Information Age by Michael J. Quinn. World Libraries, 20(1).***