**Handouts of Lecture 30 Professional Practices (IT)**

**Lecture Title: Work and Health (Cont). Privacy and the Government**

**Winner-take-all phenomena**

Several factors have led toward winner-take-all phenomena in our economy:

***Information technology and efficient transportation systems make it easier for a leading product to dominate the worldwide market.***

For example, consider a music studio that has a digital recording of the world’s best orchestra playing Beethoven’s Symphony no. 5 in C Minor. The studio can produce millions of perfect copies of this recording, enough for every classical music lover on the planet. Why would anyone want to listen to the second-best orchestra when a CD of the best orchestra is available for virtually the same price?

***Network economies encourage people to flock to the same product.***

If by chance you should need to use someone else’s computer, it is far more likely that person will own a Windows PC than a Macintosh. In this respect, knowing how to use a Windows computer has greater utility than knowing how to use a Macintosh. If a person cannot decide which computer to purchase, this factor alone may encourage someone to buy a Windows PC.

***English has become the de facto language of international business.***

English is the native language in 12 countries, including the United States, which is the dominant economic power on the planet. Another 56 countries teach English in their schools. The dominance of English makes it easier for products to find a worldwide market.

***Business norms have changed.***

In the past large businesses promoted from within and would not recruit executives from other firms. Today firms vigorously compete with each other for top executive talent.

**Harmful effects of Winner-take-all phenomena**

Winner-take-all markets create wasteful investment and consumption. For example, there is fierce competition among candidates for slots in the top business and law schools. No one wants to go for an interview looking less than his or her best. For this reason, male interviewees are reluctant to show up for an interview wearing a suit that costs less than $600. But if everyone is wearing a $600 suit, no one has an advantage over the others due to his attire. If they had all spent $300 on their suits, there would have been the same relative equity. The behavior of business school applicants is similar to an arms race. The desire to seek an advantage leads to an escalation of consumption, even if the eventual result is simply parity.

Winner-take-all is not fair because it gives much greater rewards to the top performers than those whose performance is only slightly inferior.

**Reducing Winner-take-all phenomena**

First, societies can enact laws limiting the number of hours that stores remain open for business. These laws ensure parity among competing businesses and prevent them from engaging in positional arms races. Without these laws, one business may extend its hours in order to gain an advantage over its competitors.

Second, in the absence of laws, businesses can form cooperative agreements to reduce positional arms races. An example is when a group of professional sports team owners agree to establish a cap on team salaries.

Third, more progressive tax structures reduce excess competition for the few handsomely rewarded positions. Back in 1961, the marginal tax rate on income in the highest tax bracket was 91 percent. By 1989, the highest marginal income tax rate had been lowered to 28 percent. Consumption taxes and luxury taxes are other ways of targeting the wealthiest people. Heavily taxing those with the highest incomes makes a higher income less attractive and dissuades some people from competing for the highest-paying jobs. Society benefits when these people engage in more productive work.

Finally, reducing the political power of the very wealthy is another way to reduce the attraction of competing for the highest-paying positions.

**A Balancing Act**

Since the terrorist attacks of September 11, 2001, concerns about national security have risen significantly, at the expense of privacy rights. A 2006 poll revealed that a majority of Americans support “expanded camera surveillance on streets and in public places” (70 percent), “law enforcement monitoring of Internet discussions in chat rooms and other forums” (62 percent), “closer monitoring of banking and credit card transactions, to trace funding sources” (61 percent), and even “expanded government monitoring of cell phones and email, to intercept communications” (52 percent). Remarkably, one-third of those polled agreed that “this use of investigative powers by the president should be done under his executive authority without needing congressional authorization”.

Federal, state, and local governments in the United States have had on the information privacy of those living in America. The word “privacy” does not even appear in the Constitution of the United States, and it has been difficult for the legislative, executive, and judicial branches of government to find the right compromise between demands for privacy and competing concerns.

**Solove’s Taxonomy of privacy**

Solove groups privacy-related activities into four categories:

1. Information collection refers to activities that gather personal information.

2. Information processing refers to activities that store, manipulate, and use personal information that has been collected.

3. Information dissemination refers to activities that spread personal information.

4. Invasion refers to activities that intrude upon a person’s daily life, interrupt a person’s solitude, or interfere with someone’s decision making.

**US Legislation Restricting Information Collection**

**Employee Polygraph Protection Act**

The Employee Polygraph Protection Act of 1988 (EPPA) prohibits most private employers from using lie detector tests under most situations. An employer may not require or even request a job applicant or employee to take a lie detector test, and an employee who refuses to take a lie detector test cannot suffer any retaliation.

The law has several important exceptions. Pharmaceutical companies and security firms may administer polygraph tests to job applicants in certain job categories. Employers who have suffered an economic loss, such as theft, may administer polygraph tests to employees whom they reasonably suspect were involved. Most significantly, EPPA does not apply to federal, state, and local governments.

**Children’s Online Privacy Protection Act**

The Children’s Online Privacy Protection Act (COPPA), which went into effect in 2000, is designed to reduce the amount of information gathered from children using the Internet. According to COPPA, online services must obtain parental consent before collecting any information from children 12 years old and younger.

**The Genetic Information Nondiscrimination Act**

The Genetic Information Nondiscrimination Act of 2008 is designed to prevent discrimination in the areas of medical benefits and employment based on genetic information. It prohibits health insurance companies and health plan administrators from requesting genetic information from individuals or their family members, and it forbids them from using genetic information when making decisions about coverage, rates, or preexisting conditions. It also prohibits most employers from taking genetic information into account when making hiring, firing, promotion, or any other decisions related to the terms of employment. The law does not extend these nondiscrimination protections to life insurance, disability insurance, or long-term care insurance, and it does not apply to employers with fewer than 15 employees.

**Information Collection by the Government**

**Census Records**

In order to ensure each state has fair representation in the House of Representatives, the United States Constitution requires the government to perform a census every 10 years. The first census of 1790 had six questions. It asked for the name of the head of the household and the number of persons in each of the following categories: free white males at least 16 years old; free white males under 16 years old; free white females; all other free persons (by sex and color); and slaves.

As time passed, the number of questions asked during the census increased. The 1820 census determined the number of people engaged in agriculture, commerce, and manufacturing. The 1840 census had questions regarding school attendance, illiteracy, and occupations. In 1850 census takers began asking questions about taxes, schools, crime, wages, and property values.

The 1940 census is notable because for the first time statistical sampling was put to extensive use. A random sample of the population, about 5 percent of those surveyed, received a longer form with more questions. The use of sampling enabled the Census Bureau to produce detailed demographic profiles without substantially increasing the amount of data it needed to process.

Today the Census Bureau only uses a single short form when conducting the decennial census. It gathers more detailed information on a continuous basis through the American Community Survey.

According to federal law, the Census Bureau is supposed to keep confidential the information it collects. However, in times of national emergency, the Census Bureau has revealed its information to other agencies. During World War I, the Census Bureau provided the names and addresses of young men to the military, which was searching for draft resisters. After the Japanese attack on Pearl Harbor, the Census Bureau provided the Justice Department with information from the 1940 census about the general location of Japanese Americans. The Army used this information to round up Japanese Americans and send them to internment camps.

**Internal Revenue Service Records**

The United States enacted a national income tax in 1862 to help pay for expenses related to the Civil War. In 1872 the income tax was repealed. Congress resurrected the national income tax in 1894, but a year later the Supreme Court ruled it unconstitutional. The Sixteenth Amendment to the Constitution, ratified by the states in 1913, gives the United States government the power to collect an income tax. A national income tax has been in place ever since. The Internal Revenue Service (IRS) now collects more than $2 trillion a year in taxes.

**FBI National Crime Information Center 2000**

The FBI National Crime Information Center 2000 (NCIC) is a collection of databases supporting the activities of federal, state, and local law enforcement agencies in the United States, the United States Virgin Islands, Puerto Rico, and Canada.

The FBI points to the following successes of the NCIC:

Investigating the assassination of Dr. Martin Luther King Jr., the NCIC provided the FBI with the information it needed to link a fingerprint on the murder weapon to James Earl Ray.

In 1992 the NCIC led to the apprehension of 81,750 “wanted” persons, 113,293 arrests, the location of 39,268 missing juveniles and 8,549 missing adults, and the retrieval of 110,681 stolen cars.

**OneDOJ Database**

The OneDOJ database, managed by the US Department of Justice, provides state and local police officers access to information supplied by five federal law enforcement agencies: the FBI, the Drug Enforcement Agency, the Bureau of Alcohol, Tobacco, Firearms, and Explosives, the US Marshals Service, and the Bureau of Prisons. The database, called OneDOJ, stores incident reports, interrogation summaries, and other information not presently available through the National Crime Information Center. At the end of 2006, the OneDOJ database already contained more than one million records.

Critics of the OneDOJ database point out that it gives local police officers access to information about people who have not been arrested or charged with any crime. Barry Steinhardt of the American Civil Liberties Union said, “Raw police files or FBI reports can never be verified and can never be corrected. The idea that the whole system is going to be full of inaccurate information is just chilling

**Closed-circuit Television Cameras**

The use of closed-circuit television cameras for video surveillance in the United States began in western New York in 1968. Today there are an estimated 30 million surveillance cameras operating in the United States.

The number of surveillance cameras keeps increasing. New York City is spending $201 million to install 3,000 closed-circuit security cameras in lower Manhattan. These surveillance cameras are connected to computer systems with sophisticated image-scanning software that can sound alarms if someone leaves an unattended package. The cameras are part of a larger network of sensors that also includes license plate readers and radiation detectors.

Some critics point to Great Britain as proof that surveillance cameras cannot guarantee public safety. There are 4.2 million surveillance cameras in Britain, one for every 14 people. It has been estimated that the average Briton is caught on camera an average of 300 times per day. Still, the presence of all these cameras did not prevent the suicide bombings in the London subway system in 2005.

**Police Drones**

Nine police departments in six different states have begun operating unmanned drones. Possible uses of the small drones include searching for missing persons, surveying storm damage to isolated neighborhoods, controlling illegal immigration, pursuing fugitive criminals, and performing surveillance at large public gatherings. Some uses of police drones are supported by the public, but others are not. In a recent poll conducted by Monmouth University, 66 percent of Americans expressed privacy concerns related to the use of unmanned drones with high-tech cameras by US law enforcement agencies and 67 percent opposed the use of drones to issue speeding tickets, but 80 percent supported the use of drones in search-and-rescue missions.

**Covert Government Surveillance**

**4th Amendment to US 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**

Wiretapping refers to the interception of a telephone conversation. (The term is somewhat anachronistic, because many telephone conversations are no longer transmitted over wires.) Wiretapping has been taking place ever since the 1890s, when telephones became commonly used. The state of New York made wiretapping a felony in 1892, but the police in New York City ignored the law and continued the practice of wiretapping.

**CHARLES KATZ v. UNITED STATES** A bug is a hidden microphone used for surveillance. In a series of decisions, the US Supreme Court gradually came to an understanding that citizens should also be protected from all electronic surveillance conducted without warrants, including bugs. The key decision was rendered in 1967. Charles Katz used a public telephone to place bets. The FBI placed a bug on the outside of the telephone booth to record Katz’s telephone conversations. With this evidence, Katz was convicted of illegal gambling. The Justice Department argued that since it placed the microphone on the outside of the telephone booth, it did not intrude into the space occupied by Katz. In Charles Katz v. United States, the Supreme Court ruled in favor of Katz.

**Operation Shamrock**

During World War II, the US government censored all messages entering and leaving the country, meaning US intelligence agencies had access to all telegram traffic. At the end of the war, the censorship bureaucracy was shut down, and the Signal Security Agency (predecessor to the National Security Agency) wanted to find a new way to get access to telegram traffic.

When the National Security Agency (NSA) was formed in 1952, it inherited Operation Shamrock. The sophistication of the surveillance operation took a giant leap forward in the 1960s, when the telegram companies converted to computers. Now the contents of telegrams could be transmitted electronically to the NSA, and the NSA could use computers to search for key words and phrases.

In 1961 Robert Kennedy became the new attorney general of the United States, and he immediately focused his attention on organized crime. Discovering that information about mobsters was scattered piecemeal among the FBI, IRS, Securities and Exchange Commission (SEC), and other agencies, he convened a meeting in which investigators from all of these agencies could exchange information.

The Justice Department gave the names of hundreds of alleged crime figures to the NSA, asking that these figures be put on its “watch list.” Intelligence gathered by the NSA contributed to several prosecutions. Also during the Kennedy administration, the FBI asked the NSA to put on its watch list the names of US citizens and companies doing business with Cuba. The NSA sent information gathered from intercepted telegrams and international telephone calls back to the FBI.

**Carnivore Surveillance System**

The FBI developed the Carnivore system in the late 1990s to monitor Internet traffic, including email messages. The system itself consisted of a Windows PC and packet-sniffing software capable of identifying and recording packets originating from or directed to a particular IP address.

In 2000 the Justice Department demanded that Earthlink, an Internet service provider, allow the FBI to use Carnivore without a warrant. Earthlink filed a legal challenge questioning the FBI’s authority to do this under the Electronic Communications Privacy Act, but a US District Court ruled against Earthlink.

Between 1998 and 2000 the FBI used the Carnivore system about 25 times. In late 2001 the FBI stopped using Carnivore, replacing it with commercial software capable of performing the same function.

**Covert Activities after 9/11**

The September 11, 2001, attacks on the World Trade Center and the Pentagon spawned new, secret intelligence-gathering operations within the United States.

**National Security Administration Wiretapping**

President Bush signed a presidential order allowing the NSA to eavesdrop on international telephone calls and international emails initiated by people living inside the United States, without first obtaining a search warrant.

The list of persons being monitored gradually expanded, as the NSA followed connections from the original list of telephone numbers. At any one time, the NSA eavesdropped on up to 500 people inside the United States, including American citizens, permanent residents, and foreigners. The NSA also monitored another 5,000 to 7,000 people living outside the United States at any one time.

Sources told the New York Times that the surveillance program had foiled at least two al-Qaeda plots: Ohio truck driver Iyman Faris’s plan to “bring down the Brooklyn Bridge with blowtorches” and another scheme to bomb British pubs and train stations.

**TALON Database**

The US Department of Defense created the Threat and Local Observation Notices (TALON) database in 2003. The purpose of the database was to collect reports of suspicious activities or terrorist threats near military bases. These reports were submitted by military personnel or civilians and then assessed by Department of Defense experts as either “credible” or “not credible.”

In December 2005, NBC News reported that the database contained reports on antiwar protests occurring far from military bases [29]. In July 2006, the Service members Legal Defense Network reported that the TALON database contained emails from students at Southern Connecticut State University, the State University of New York at Albany, the University of California at Berkeley, and William Paterson University of New Jersey who were planning protests against on-campus military recruiting.

The Department of Defense removed many of these reports from TALON after conducting an in-house review that concluded the database should only contain information related to terrorist activity.

In April 2007, the new Undersecretary of Defense for Intelligence recommended that the TALON program be terminated. The TALON database was shut down on September 17, 2007.

**US Legislation Authorizing Wiretapping**

**Title III**

Congress responded by passing Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Title III allows a police agency that has obtained a court order to tap a phone for up to 30 days. The government continued to argue that in cases of national security, agencies should be able to tap phones without a warrant. In 1972 the Supreme Court rejected this argument when it ruled that the Fourth Amendment forbids warrantless wiretapping, even in cases of national security.

**Foreign Intelligence Surveillance Act**

* FISA provides judicial and congressional oversight of covert surveillance of foreign governments and agents
* Allows electronic surveillance of foreign nationals for up to one year without a court order
* Amended in 2007 to allow government to wiretap communications to/from foreign countries without oversight by FISA Court

 **PRISM Program**

In June 2013, the British newspaper the Guardian disclosed it had received a top secret document outlining how the National Security Agency had obtained direct access to the servers at Google, Facebook, Yahoo, and other Internet giants.

The secret program, called PRISM, enables the NSA to access stored information such as email messages and monitor live communications such as Skype and PalTalk conversations without first obtaining search warrants, when the NSA has a reasonable suspicion that the person being investigated is a foreigner outside the United States. According to the secret document, the NSA gained access to the servers of Microsoft in 2007; Yahoo in 2008; Google and Facebook in 2009; YouTube in 2010; Skype and AOL in 2011; and Apple in 2012.

All the companies that responded to a request for information by the Guardian denied any knowledge of the PRISM program.

***Reference:***

***Lecture topic: Work and Health Chapter 10***

***Privacy and the Government Chapter 6***

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