**Handouts of Lecture 19 Professional Practices (IT)**

**Lecture Title: Information Disclosures**

**Data Gathering and Privacy Implications**

* Facebook tags
* Enhanced 911 services
* Rewards or loyalty programs
* Body scanners
* RFID tags
* Implanted chips
* OnStar
* Automobile “black boxes”
* Medical records
* Digital video recorders
* Cookies and flash cookies

**Facebook Tags**

In the Facebook social network, a tag is a label identifying a person in a photo. When you post a photo to Facebook, you can tag the people in the photo who are on your list of Facebook friends. In a similar way, any of your Facebook friends can tag you in photos they post to the site. People tag photos in Facebook an average of 100 million times per day.

In December 2010, Facebook introduced a new time-saving feature called Tag Suggestions. When a Facebook user adds a new photo, Facebook uses facial recognition software to suggest the name of the friend appearing in the photo. In June 2011, the Electronic Privacy Information Center (EPIC) filed a complaint about Facebook Tag Suggestions with the Federal Trade Commission. EPIC claimed that in order to develop its facial recognition technology, Facebook gathered facial data from users’ photos without their consent. Others raised the concern that the introduction of an automatic tagging feature would increase the chance that photos would be improperly tagged, which could cause a problem if the photos were not complimentary.

**Enhanced 911 Services**

All cell phone providers in the United States are required by law to be able to track the locations of active cell phone users to within 100 meters. The safety benefit of this capability is obvious. Emergency response teams can reach people in distress who have dialed 911, even if they are unable to speak or do not know exactly where they are. The ability to identify the location of active cell phone users has other benefits. For example, it makes it easier for cell phone companies to identify where signal strength is weak and coverage needs to be improved. The downside of enhanced 911 service is a potential loss of privacy. Because it is possible to track the location of active cell phone users, what happens if information is sold or shared? Suppose you call your employer and tell him you are too sick to come into work. Your boss is suspicious, since this is the third Friday this winter you’ve called in sick. Your employer pays your cell phone provider and discovers that you made your call from a ski resort.

**Rewards or Loyalty Programs**

Rewards or loyalty programs for shoppers have been around for more than 100 years. Your grandparents may remember using S&H Green Stamps, the most popular rewards program in the United States from the 1950s through the 1970s. Shoppers would collect Green Stamps with purchases, paste them into booklets, and redeem the booklets by shopping in the Sperry & Hutchinson catalog for household items. Today many shoppers take advantage of rewards programs sponsored by grocery stores.

Companies can use information about the buying habits of particular customers to provide them with individualized service. For example, ShopRite grocery stores have computerized shopping carts. The shopping cart has a card reader and an LCD screen. Customers identify themselves by swiping their loyalty card through the card reader. A computer taps into a database with the customer’s buying history and uses this information to guide the customer to frequently purchased products. As the cart passes through the aisles, pop-up ads display items the computer predicts the customer may be interested in purchasing.

**Body Scanners**

In some stores in the United Kingdom, you can enter a booth, strip to your undergarments, and be scanned by a computer, which produces a three-dimensional model of your body. The computer uses this information to recommend which pairs of jeans ought to fit you the best. You can then sit in front of a computer screen and preview what various pairs of jeans will look like on you. When you have narrowed down your search to a few particular brands and sizes, you can actually try on the jeans. Body scans are also being used to produce custom-made clothing. At Brooks Brothers stores in the United States, customers who have been scanned can purchase suits tailored to their particular physiques.

**RFID Tags**

RFID, short for radio frequency identification. An RFID is a tiny wireless transmitter. Manufacturers are replacing bar codes with RFIDs, because they give more information about the product and are easier to scan. An RFID can contain specific information about the particular item to which it is attached (or embedded), and a scanner can read an RFID from six feet away. When bar codes are replaced by RFIDs, checkouts are quicker and companies track their inventory more accurately. However, because RFIDs are not turned off when an item is purchased, the new technology has raised privacy concerns. Imagine a workplace full of RFID scanners. A scanner in your cubicle enables a monitoring system to associate you with the tags in your clothes. Another scanner picks up your presence at the water cooler. The next thing you know, your boss has called you in for a heart-to-heart talk about how many breaks you’re taking. Some privacy advocates say consumers should have a way to remove or disable RFIDs in the products they purchase.

**Implanted Chips**

In Taiwan, every domesticated dog must contain a microchip implant identifying its owner and residence. The microchip, about the size of a grain of rice, is implanted into the dog’s ear using a syringe. When a dog gets lost, the authorities can easily retrieve the address and return the pet to its owner. Verichip Corporation created an RFID tag approved for use in humans. The company claimed that 2,000 people worldwide had a Verichip implant. The most common reason for getting an implanted RFID chip was to allow doctors to learn about the medical conditions of unconscious patients. However, in some trendy European nightclubs, patrons have used their implanted RFID chips as in-house “debit cards” for purchasing food and drinks. After some highly publicized incidents of abducted or missing children, the media have reported parents ruminating on the idea of implanting microchip tracking devices in their kids.

**OnStar**

OnStar Corporation manufactures a communication system incorporated into an automobile’s rear-view mirror. OnStar provides emergency, security, navigation, and diagnostics services to its subscribers. For example, a driver who runs out of gas can push the Blue OnStar button to initiate a conversation with an OnStar representative. The driver does not have to know his or her exact location, because the system automatically sends the GPS location of the automobile to OnStar, which can send help. The driver does not always need to initiate the communication with OnStar representatives. For example, whenever the air bags deploy on an OnStar-equipped vehicle, the system automatically communicates the location of the vehicle to an OnStar center, which can initiate a 911 call.

**Automobile “Black Boxes”**

You probably know about airplane flight data recorders, also called “black boxes,” which provide information useful in postcrash investigations. Did you know that modern automobiles also come equipped with a “black box”? A microprocessor attached to the car’s air bag records information about the speed of the car, the amount of pressure being put on the brake pedal, and whether the seat belts are connected. After a collision, investigators can retrieve the microprocessor from the automobile and view data collected in the five seconds before the accident.

**Medical Records**

The change from paper-based to electronic medical records has the potential to lower the costs and improve the quality of medical care by making it quicker and cheaper for information about patients to be shared among nurses, physicians, and other caregivers. The US government has been promoting the conversion to electronic medical records as one way to rein in the rapid increase in health care costs. The Health Information Technology for Economic and Clinical Health (HITECH) Act calls for doctors and hospitals to move from paper records to electronic records by 2015. However, once an individual’s entire medical history is consolidated in a database accessible by many, it can be more difficult to control how that information is disseminated, with potentially significant consequences. An employer may choose to pass over a job candidate who has had serious medical problems. A woman who has successfully completed a treatment program for drug addiction may be discriminated against if information about her former drug use is revealed.

**Digital Video Recorders**

TiVo, Inc. is a well-known manufacturer of digital video recorders. TiVo provides a service that allows its subscribers to more easily record programs they are interested in watching later. For example, with a single command a subscriber can instruct the TiVo to record every episode of a TV series. TiVo collects detailed information about the viewing habits of its users. Because the system monitors the activities of the users second by second, its data are more valuable than those provided by other services. For example, TiVo’s records show that 66 percent of the ads shown during primetime on broadcast networks are skipped.

**Cookies**

A cookie is a file placed on your computer’s hard drive by a Web server. The file contains information about your visits to a Web site. Cookies can contain login names and passwords, product preferences, and the contents of virtual shopping carts. Web sites use cookies to provide you with personalized services, such as custom Web pages. Instead of asking you to type in the same information multiple times, a Web site can retrieve that information from a cookie. Most Web sites do not ask for permission before creating a cookie on your hard drive. You can configure your Web browser to alert you when a cookie is being placed on your computer, or you can set your Web browser to refuse to accept any cookies. However, some Web sites cannot be accessed by browsers that block cookies.

In recent years Web sites have begun using another kind of cookie called a flash cookie, which is a file placed on your computer’s hard drive by a Web server running the Adobe Flash Player. Two attributes of flash cookies have raised privacy concerns. First, a flash cookie can hold 25 times as much information as a browser cookie. Second, flash cookies are not controlled by the browser’s privacy controls. Some Web sites take advantage of this loophole and use flash cookies as a way of backing up ordinary cookies.

**Data Mining**

**Data Mining Defined**

A record in a database records a single transaction, such as a particular item you purchased at the grocery store. A database record is like a single snapshot of a person. It tells you something about the person, but in isolation its value is limited. Data mining is the process of searching through many records in one or more databases looking for patterns or relationships. Data mining is a way to generate new information by combining facts found in multiple transactions, and it can also be a way to predict future events. By drawing upon large numbers of records, data mining allows an organization to build an accurate profile of an individual from a myriad of snapshots. Google’s personalized search and collaborative filtering are two examples of how companies are using data mining to create more personal relationships with their customers.

**Google’s Personalized Search**

Google keeps track of your search queries and the Web pages you have clicked. When you type in a new query, it can use this information to infer what you are interested in and return pages more likely to be what you are seeking. For example, the word “bass” has multiple meanings, but if you have a history of queries and page clicks related to fishing, but not music, that can help the search engine return the most appropriate pages.

Google is able to personalize search results whether or not you have a Google account. If you are signed in to Google, the search engine examines your Web history to personalize the search results. This information is held indefinitely, unless you delete your Web history. If you are not signed in, Google creates a cookie linked to your computer’s browser, and it stores records of all queries associated with that cookie, as well as results that have been clicked, for up to 180 days.

**Collaborative Filtering**

Collaborative filtering algorithms draw upon information about the preferences of a large number of people to predict what an individual may enjoy. An organization performing collaborative filtering may determine people’s preferences explicitly, through rankings, or implicitly, by tracking their purchases. The filtering algorithm looks for patterns in the data. Perhaps many people who purchase peanut butter also purchase jam. If a new customer buys a jar of peanut butter, the software may instruct the register to print out a discount coupon for a particular brand of jam along with the sales receipt. Collaborative filtering software is also used by online retailers and movie sites to make recommendations.

**Ownership of Transaction Information**

What rules should govern the sharing of information collected by organizations selling products or services? Two fundamentally different policies are called opt-in and opt-out.

The opt-in policy requires the consumer to explicitly give permission for the organization to share the information with another organization. Opt-in policies are preferred by privacy advocates. The opt-out policy requires the consumer to explicitly forbid an organization from sharing information with other organizations. Direct marketing associations prefer the opt-out policy because opt-in is a barrier for new businesses. New businesses do not have the resources to go out and collect all the information they need to target their mailings to the correct individuals.

In an opt-out environment, most people will not go through the effort required to actually remove themselves from mailing lists. Hence it is easier for new businesses to get access to the mailing lists they need to succeed. Another argument for opt-out is that companies have the right to control information about the transactions they have made. Information is a valuable commodity. An opt-in policy takes this commodity away from companies. At this time opt-out policies are far more common than opt-in policies. Information about customers has itself become a commodity. Organizations sell or exchange information with other organizations. This is a common way for organizations to gather large databases of information they can mine. For example, a company selling time-share condominiums purchases from a hotel chain the names and addresses of people who have vacationed in a resort area in the past two years. From another organization it purchases a database that gives the approximate annual household income of a family, based on that family’s nine-digit ZIP code. Combining these lists allows the time-share agency to target people most likely to have both the interest and the financial resources to purchase a share of a vacation condominium. It uses direct mail to send brochures to these people.

**Credit Reports**

Credit reports are a great example of how information about customers has itself become a commodity. A credit bureau is a company that keeps track of an individual’s assets, debts, and history of paying bills and repaying loans, using this information to determine the creditworthiness of that person. Credit bureaus sell credit reports to banks, credit card companies, and other potential lenders.

Thanks to the national credit bureau system, you can get a credit card from a bank or store that you’ve never done business with. When you want to borrow money to purchase a home, you don’t have to go to your local bank. You can get the money from a bank across the country that trusts you to repay the loan because of your high credit score. Competition among banks leads to lower interest rates, a definite advantage for consumers.

***Reference***

***Lecture 19 slides: Information Privacy cont.***

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