Introduction

"Panopticon" by zombieite is licensed under CC BY 2.0

Privacy refers to being free from intrusion; it is the right to be left alone, to be free from surveillance, and to have control over the information collected and stored about yourself.

With the digitization of all forms of information and the increasing use of the Internet for all types of activities, it has become easy to collect detailed information about individuals. This has helped businesses to locate customers for their products, allowed government and law enforcement to monitor individuals' behavior, and enabled criminals to find victims.

Loss of privacy is so widespread and is occurring so quickly that some believe that it is too late to do anything about it. Others are interested in maintaining some forms of privacy. Still others are embracing a transparent lifestyle, broadcasting their every action to the world.

The concept of big data emerged from the vast and exponentially-growing amount of data generated by social media, mobile devices, apps, and all the other digital tools wielded by the global population every day. Corporations, and others, are driven to collect all of that data and analyze it to gain useful insights that can be used to make better business decisions. Companies like Google, Facebook, AT&T, and many others have gotten good at collecting the data. Developing software to analyze the massive amount of data being collected is the primary challenge of the big data industry. In coming years, that challenge will become much more complex. Today, the average Internet user owns two Internet- connected devices, typically a smartphone and computer. Over the next couple of years, that number is expected to jump to seven, more than tripling the number of devices on the Internet. The bulk of new Internet devices will represent things rather than people—thermostats, security systems, televisions, electric meters, cars, refrigerators, and other appliances. These devices will increase the amount of big data by adding information like the temperature in every home at every second, the energy usage of each residence and business, eating habits, laundry habits, water usage, waste production, and more. Add this information up, and the Internet of people and things—the Internet of Everything, as Cisco calls it—becomes a source of real-time information about the state of the planet at any given moment in time.

The Internet of Things has been likened to a "global electronic nervous system, with trillions of individual sensors monitoring the status of everything of interest to humans." IBM wants to stream all of those exabytes of data to its cloud-based cluster supercomputers to extract the maximum amount of value from the data, using analytics and neural network-powered software modeled on the human mind. With so much data being collected from each person's life, what data, if any, should remain private? Is it worthwhile to sacrifice privacy to provide valuable insight for improving life on Earth?

Computer technology gives us the ability to collect, maintain, process, and transfer more information than ever before. This power has given rise to a seemingly endless number of public and private databases that include details about many individuals. Combined, these databases could tell a person's life story in terms of daily activities, personal interests, and financial matters. This massive data collection, combined with surveillance technologies that include the increasing use of cameras in public places, has given rise

to legitimate concerns over the invasion of privacy in the digital era. For example, Google's Street View technology has caused a stir over privacy issues because of its 360-degree street-level imagery, which uses satellite technology to take real-time pictures of private and public locations.

Privacy issues include being free from intrusion—the right to be left alone, to be free from surveillance, and to control the information collected and stored about yourself. Information security often comes at the cost of some level of convenience and privacy. This section looks at the extent to which your privacy might be sacrificed in order to provide conveniences offered by the digital world and to increase your personal safety and national security.

Lesson 13.1: Protecting Privacy

Lesson 13.1 Introduction

Everything we do generates information about who we are as people—who we know, what we believe, what we like—and this is truer than ever with the expansion of the Internet into our daily lives. In many ways, this process is unavoidable, short of abandoning society and living in the woods. We can all take steps, however, to reduce the amount of private information we broadcast without our knowledge or consent, and we are not alone in our desire to prevent privacy from disappearing entirely.

Reading: U.S. Privacy-Protective Laws

U. S. privacy-protective laws refer to legislation designed to protect the private information of U.S. citizens.

Library of Congress Prints and Photographs Division (ppmsca-08467.-08467r). Public Domain

Why This Matters

The right to privacy has been a hotly debated topic in countries around the world for generations. Generally, free and democratic governments include laws that protect citizens' privacy to some extent. At a minimum, in a free society, a citizen would expect to have privacy within his or her home. The level of privacy a person enjoys can vary greatly, depending on social circumstances and the political and legal position of the government on privacy issues. Digital technologies have made protecting private information more difficult than ever. Many recent privacy laws focus on digital technology challenges.

Essential Information

You might be surprised to learn that the U.S. Constitution itself contains no express right to privacy. However, the Bill of Rights (the first 10 amendments to the Constitution) refers to privacy issues. The First Amendment protects the privacy of belief; the Third Amendment protects the privacy of the home against demands that it be used to house soldiers; the Fourth Amendment protects the privacy of the person and

possessions against unreasonable searches; and the Fifth Amendment protects a person from self-incrimination.

A later amendment has also been important for privacy issues. Over the years, the Supreme Court has interpreted the word “liberty” in the Fourteenth Amendment to include issues of privacy—particularly in terms of issues such as marriage, procreation, childrearing, and termination of medical treatment. Polls indicate that most Americans support this interpretation of the word “liberty.”

The free flow of digital information has created the need for a number of laws to protect the private information of individuals. When it comes to information privacy, government agencies in the United States and many other democratic countries are regulated more stringently than businesses and health care professionals. However, with the exponential growth of digital information, the government is stepping in to regulate the use of information across many industries.

The Privacy Act of 1974 is the primary law controlling what many U.S. government agencies can and cannot do with the information they hold. The primary tenets of the law include the rights of citizens to know what information certain government agencies store about them and to exercise control over the accuracy of that information and how it is used. Laws that control the handling of information by the government, businesses, and the health care industry are listed below. As technology advances provide additional means of invading individuals’ privacy, new laws will be needed. For example, as unmanned drone aircraft begin entering commercial markets, media companies and others may begin using them to gather video and photographs of private property. Some states have already banned the use of unmanned drones in expectation of just such abuses. Privacy advocates are up in arms in states where drones are being considered for use by police.

U.S. Privacy-Protective Laws

Law	Explanation
Identity Theft Protection Act of 2005	Requires businesses to secure sensitive data physically and technologically and to notify consumers nationwide when data is compromised
Information Protection and Security Act of 2005	Gives the Federal Trade Commission (FTC) the ability to regulate the sale of personal information
Notification of Risk to Personal Data Act of 2003	Requires businesses to notify individuals when their personal information is stolen
Education Privacy Act of 2003	Restricts the collection of data by federally funded schools
Sarbanes-Oxley Act (“Sarbox”) of 2002	Fights corporate corruption by imposing stringent reporting requirements and internal controls on electronic financial records and transactions
Children’s Online Privacy Protection Act of 2000	Gives parents control over what information is collected from their children online, and how such information may be used
Gramm-Leach-Bliley Act (GLBA) of 1999	Requires banks and financial institutions to alert customers of their policies and practices for disclosing customer information
Consumer Internet Privacy Protection Act of 1997	Requires data collectors to alert people that their personal information is being shared with other organizations
Health Insurance Portability and Accountability Act (HIPAA) of 1996	Requires those in the health industry to protect the privacy of health information, and provides policies and procedures for doing so
Computer Matching and Privacy Protection Act of 1988	Regulates cross-references of data between federal agencies
Tax Reform Act of 1979	Controls the collection and use of certain information collected by the IRS
Right to Financial Privacy Act of 1978	Restricts the government’s access to certain financial records maintained by financial institutions
Privacy Act of 1974	Controls what many government agencies can and cannot do with the information they hold

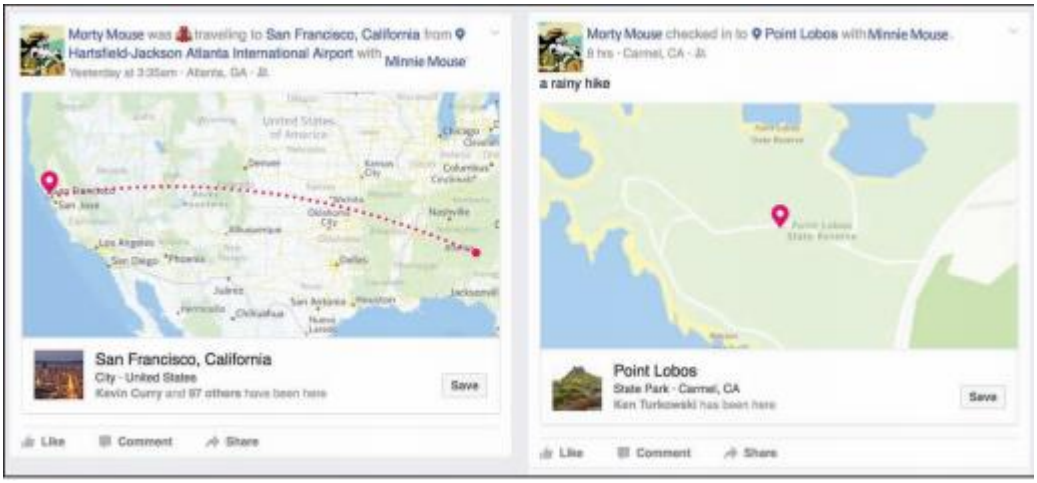
Law	Explanation
Freedom of Information Act of 1966	Gives citizens the right to view their own personal records maintained by federal agencies

Reading: Transparency

Transparency is when a person, business, organization, or government keeps little or nothing secret from the world—an approach that is supported by technologies such as lifestreaming, geolocation, and microblogging.

Why This Matters

So what is the danger in having other people know about your life, the intricacies of your day-to-day dealings, and your secret thoughts? Perhaps the solution to privacy issues is to abandon the concept of privacy altogether. If you aren't doing anything illegal, why should you care what other people know about you? Some individuals subscribe to this philosophy, have abandoned concerns over privacy, and are leading a transparent lifestyle. Businesses, organizations, and governments may support a transparent approach in order to win the trust of the public.



Facebook; created by Ken Baldauf (fictitious users). Fair Use

Essential Information

Some experts in the area of privacy believe that there are three scenarios regarding the relationship between technology, privacy, and society:

Full privacy: Citizens should be assured of 100% privacy. They should have absolute control over what personal information is maintained in public and private databases, and there should be no surveillance of any kind for any purpose.

Full trust: Citizens should trust governments to provide surveillance in a safe and secure manner that respects privacy rights.

Full transparency: All surveillance and information should be accessible to every law-abiding citizen. Governments and law enforcement should not maintain exclusive control over surveillance. Citizens should have the ability to turn the cameras onto authority to ensure that power is not being abused.

It may be too late for full privacy. Technology and its use have progressed past the point of regaining previous levels of anonymity. If full privacy is not attainable, some feel it would be a mistake to fully trust those in power to manage privacy responsibly. Power corrupts, and being responsible for all private

information of a population would imply absolute power. Such a scenario, some fear, could lead to an Orwellian society.

Full transparency is an intriguing notion. How would society change if everyone was openly honest and had equal access to all information and surveillance? No group would hold an advantage over others because of the information it controlled. Any person could view surveillance data from any location. Everyone would hold all the cards. Although there would be little privacy, except perhaps in one's own home, there would also be little opportunity for abuse of power, except by those who cheat.

Social media has provided tools for Internet users to lead a transparent life. Some individuals strap on video cameras and broadcast their every waking moment as a lifestream on the Internet. In a less extreme and more popular form of transparency, people are broadcasting their daily events, using microblogging sites such as Twitter, Tumblr, Instagram, and Facebook updates. Social media makes it possible to share your thoughts, your interests, your photos, your location, your friends, your personal information (like your birthday and love interests), your web activities, and your favorite organizations. Just about everything about yourself can be presented for the world to see.

One possible danger in leading a transparent lifestyle is that it gives others power over you. When people know everything about you, but you know nothing about them, they could take advantage of you. You become more susceptible to identity theft. Someone could break into your residence when they know you are out. There are many ways that the personal information people provide to others over social networks can be used, and is being used, to take advantage of those individuals.

There are also issues surrounding the division of a person's professional life and personal life. Most people are not eager to have their boss and work colleagues analyzing their party photos on Facebook. Nor do most people want their personal friends and business colleagues intermixed in their social networks. People typically behave differently at home than they do at work. A totally transparent lifestyle would not support any division of home life and work life.

Nonetheless, there is a certain feeling of freedom that results from casting away concern for privacy and broadcasting yourself to the world: "Like me or not, I am who I am." It is a trend that may spread voluntarily or out of necessity as privacy becomes increasingly difficult to maintain.

Lesson 13.2: Privacy Threats

Lesson 13.2 Introduction

While we produce a lot of information about ourselves simply by living in a digital society, there are those who profit from far more invasive methods of data mining. Not only do government intelligence agencies engage in sophisticated surveillance, but our privacy is continually threatened by the businesses we interact with. Much of this activity is entirely legal and expected.

Reading: U.S. Privacy-Invasive Laws

U.S. privacy-invasive laws refer to legislation that is invasive to individual privacy for a perceived greater good of the country.

Why This Matters

In the history of the United States and other developed and democratic societies, there have been times when individual privacy and civil liberties have been sacrificed for the sake of national security. These times typically strain the relationship between a government and its citizens, which is sometimes expressed through protests, violence, and arrests. It is at times such as these that citizens must be aware of government action, understand what sacrifices may be required on their part for the sake of the country, and express concern over any civil liberties and privacy that might be sacrificed unnecessarily.

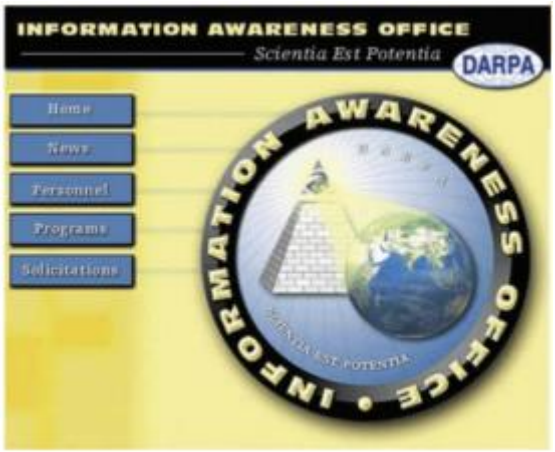
Essential Information

In times of war, U.S. law allows the government to restrict privacy in an effort to capture or defeat an enemy. The Federal Wiretap Act, enacted in 1968 and expanded in 1986, sometimes referred to as Title III, sets procedures for court authorization of real-time surveillance of all kinds of electronic communications in criminal investigations. The Foreign Intelligence Surveillance Act of 1978 allows wiretapping based on a finding of probable cause to believe that the target is a member of a foreign terrorist group or an agent of a foreign power. Both laws allow the government to carry out wiretaps without a court order in emergency situations involving risk of death or serious bodily injury and in national security cases.

Such has also been the case since the attacks of September 11, 2001. The USA PATRIOT Act of 2002 gave the federal government greater access to private information and wider latitude in the treatment of suspected terrorists. It was designed to “deter and punish terrorist acts in the United States and around the world, to enhance law enforcement investigatory tools, and for other purposes.” It includes measures to “enhance surveillance procedures.”

The easing of privacy regulation in time of war causes concern for privacy advocates. They fear that in a state of panic, the government may overreact and needlessly sacrifice civil liberties and rights.

When the Information Awareness Office of the Defense Advanced Research Projects Agency (DARPA) proposed a new tracking information system called Total Information Awareness (TIA) in 2002, privacy advocates complained loudly. Total Information Awareness was designed to capture the “information signature” of people so that the government could track potential terrorists and criminals. An information signature is any unique information stored about an individual, such as information about property, address history, utility connections, bankruptcies, liens, and business filings, as well as a host of other information. Data mining techniques were to be applied to the database developed by the TIA system in order to “connect the dots” and detect potential terrorist activity.



Courtesy of the DARPA. Fair Use

What outraged privacy advocates was that this system could be used to track all citizens, not just those suspected of crimes. It was essentially a form of the “Big Brother” concept introduced by George Orwell in his book 1984. In his story, the government (Big Brother) watched over everyone in society by using information gathering and video surveillance In this Orwellian society, there was little in the way of crime, nor was there any privacy or freedom. It was like living in a prison.

In the case of Total Information Awareness, the privacy advocates won. The name of the program was changed to Terrorism Information Awareness. Shortly after that, Congress cut off funding for the program.

In 2002, following the fiasco with Total Information Awareness, the U.S. government developed a system called MATRIX (Multistate Anti-Terrorism Information Exchange). Once again the system was shut down because of privacy infringements on law-abiding citizens. A few states still use MATRIX-like technologies on the state level to help identify criminals.

In 2016, the FBI requested that Apple assist in providing access to data on the iPhone used by a shooter in the famous San Bernardino attacks. Apple's refusal to do so kicked off a major national debate on privacy vs. protection. Ultimately, the FBI was able to hack the iPhone without Apple's assistance, leaving the impression that Apple's efforts to protect user privacy and data was less than perfect.

Reading: Surveillance

Surveillance is the close monitoring of behavior through electronic technologies such as wiretapping, data mining, remote video and audio monitoring, GPS, and RFID.

Why This Matters

Computer-controlled surveillance technologies, combined with ubiquitous telecommunications networks and powerful information processing systems, have made it possible to gather huge quantities of video, audio, and telecommunications signals and process them to reveal personal information. Although this is mostly done in an effort to curb crime and catch criminals, some people are concerned with the lack of oversight. Who is monitoring those individuals doing the monitoring? Will the information gathered in electronic surveillance be used to invade our privacy?

Essential Information

There are many forms of electronic surveillance, including wiretapping, data mining, video and audio surveillance, Internet monitoring, and GPS and RFID surveillance.

Wiretapping involves secretly listening in on conversations taking place over telecommunications networks, including telephone, email, instant messaging, VoIP, and other Internet communications. Wiretapping has been around as long as there have been wires to tap and now extends to wireless communications. With increased dependence on electronic communications, wiretapping has grown to be an important tool for law enforcement and a major concern for those interested in personal privacy. Laws governing wiretapping allow the government to carry out wiretaps without a court order in emergency situations involving risk of death or serious bodily injury and in national security cases.

With cooperation from Internet service providers, an FBI surveillance system called Carnivore has been used to monitor email correspondence. The system has alarmed privacy advocates and some members of Congress because of the manner in which it surveys all email on the system, not just email of suspected criminals. To avoid public criticism, the FBI switched from Carnivore to its own proprietary system, of which little is known.

In 2013, NSA contractor Edward Snowden leaked classified documents that revealed numerous global surveillance programs, many run by the NSA and the Five Eyes Intelligence Alliance (Australia, Canada, New Zealand, the United Kingdom, and the United States), with the cooperation of telecommunication companies and European governments. The revelation alerted the world to the lengths that governments have gone to in order to gather information about the public and other governments. In many cases since Snowden's disclosures, telecom and tech companies have been discovered to be assisting governments in the collection of user information. These revelations have led to public distrust of governments and companies in areas of privacy.

Increasingly, cities are turning to networked video surveillance to monitor their streets. Video cameras in public places are assisting in capturing criminals who might otherwise escape. For example, video surveillance was critical in the investigation to find the Boston Marathon bombers in early 2013. In

Chicago, a multimillion-dollar system dubbed Operation Disruption includes over 300 street-surveillance cameras with microphones.

In addition to living with permanent mounted cameras, we are now entering the era of flying cameras. Unmanned drone aircraft have become a necessity to the military for scoping out the enemy without risking life. Since the price of the technology has dropped, flying camera-bearing drones has become a favorite past time of hobbyists. The FAA is hustling to create regulations for drones in domestic airspace. High-resolution cameras attached to satellites and pointed at the earth are providing amazing new mapping technologies, as demonstrated through software such as Google Earth. Google's high-resolution satellite cameras can capture images of objects as small as 41 cm. Government-owned satellites can get even finer resolution.

2012 Google. Fair Use

Global positioning system (GPS) and radio frequency identification (RFID) technologies are very useful, but they can also be used to invade privacy. Consider the case of a man who attached a GPS tracking device to the undercarriage of his ex-girlfriend's car to monitor her movements. The man was picked up by police after his ex found him under her car, changing the battery on the device. He's serving time in a California prison. GPS devices are being considered by some states for tracking ex-cons and for use in automobile license plates.

The combination of data mining, consumer and government databases, listening in on electronic communications, video and audio surveillance, satellite surveillance, and GPS and RFID location monitoring adds up to the possibility of serious invasion and abuse of basic privacy rights. Currently, at least in the United States, privacy laws and advocates work to keep government agencies in check. A second deterrent to abuse of surveillance technologies by government is a lack of funding and personnel. It takes a considerable investment to monitor video from thousands of cameras. As technology improves and surveillance becomes increasingly automated, funding and personnel will become a non-issue. We may soon be able to entrust the monitoring of surveillance data to a powerful AI (artificial intelligence) computer system. Once again, this matter becomes a case of trust: Can those monitoring society be trusted to use surveillance only in the best interest of the public without invading the privacy of law-abiding citizens?

Reading: Behavioral Targeting

Behavioral targeting uses information about a person's behavior to inform businesses and marketers so that they can offer products that are likely to be of interest to that person.

Why This Matters

Much of the information gathered about individuals is collected without their knowledge. For example, a person might join a discount club at a local grocery store to enjoy special deals on products and to facilitate a faster checkout process. That person might not be aware that the club membership card also allows the store to digitally track his or her buying patterns. The customer may receive special mailings providing information on products that he or she typically buys. Some customers find this to be a valuable service while others consider it an invasion of privacy. With commerce moving to the web, the tracking of consumer information has become much easier.

Essential Information

Traditional marketing uses a technique known as market segmentation, where ads target customers based on their race, gender, income, education, age, and other general characteristics. Although this is often more effective than mass marketing, which advertises to everyone regardless of their social characteristics, it still can miss the mark.

The Internet allows market segmentation to take place at the level of each individual consumer. By studying a user's web behavior, businesses can learn and even predict what the person may be interested in purchasing. This is referred to as personalized or one-to-one marketing.

The Internet acts as a supercharged tool for invisible information gathering and behavioral targeting. Through the use of cookies, companies can accumulate immense amounts of information about customers visiting their websites. Onsite behavioral targeting involves a company tracking a user's activities on its own site. The information the company collects allows the company to custom-design a website that caters to the individual's interests. Amazon.com uses this approach to custom-design its opening page for each visitor for whom it has data. For example, if you purchase romance novels and kitchen appliances at Amazon, the next time you visit the site, you will see promotions for other romance novels and home appliances.

Courtesy of Amazon.com. Fair Use

Many users find onsite behavioral targeting useful while others find it a bit invasive. Even more invasive is network behavioral targeting. In network behavioral targeting, user behavior is tracked over multiple websites. Web advertising companies that provide ads to many websites, such as DoubleClick by Google, have the power to collect cross-site data about a user through the use of third-party cookies. Such information can be used to create a detailed consumer profile that can be very valuable to businesses. Browsers now offer the ability to block third-party cookies.

Facebook uses “Like” icons on over a billion websites so that its users can share with their friends the products, services, and content they like. Facebook and its partners collect this information, developing a detailed user profile for use in targeted advertising. Google+ uses a similar system. Google+ and Facebook’s Like icons are often found side-by-side on websites.

The ultimate network behavioral targeting exists at the Internet service provider level. An ISP is capable of collecting information on what every user is doing over its connections—and for ISPs like Comcast and AT&T, that can include Internet, television, and phone data. ISPs have come under fire for collecting such data. Verizon and AT&T were found utilizing a technology called super cookies to track users’ online activities through mobile web browsers. It is useful to read the privacy policy of your ISP to find out what it does with that information. Such information would be a goldmine to marketers, and there isn’t much standing in the way of ISPs mining that gold.

Network behavioral targeting is the tip of the iceberg for data aggregation companies such as LexisNexis Risk Solutions, formerly ChoicePoint. LexisNexis Risk Solutions collects and combines information from the three big credit bureaus; public records of numerous local, state, and federal government agencies; telephone records; liens; deeds; and other sources in order to develop detailed information about individuals, companies, and organizations. Over the years, the company has purchased many other personal information services, increasing its database to include drug test records, physician backgrounds, insurance fraud information, and a host of other specialized pieces of valuable personal information. Businesses and organizations contract LexisNexis for data mining to provide information on specific individuals for a variety of uses.

LexisNexis has more information about U.S. citizens than the government does. As a matter of fact, it has a multimillion-dollar contract with the Department of Justice and the IRS. FBI agents use information supplied by LexisNexis Risk Solutions in their criminal investigations. In this way, federal agencies can sidestep privacy laws that restrict the government from collecting and mining such information itself.