May 2007

Privacy and Security in Information Technology

Tyler H. Boone
Worcester Polytechnic Institute

Privacy and Security in Information Technology

An Interactive Qualifying Project

submitted to the Faculty of the

Worcester Polytechnic Institute

in partial fulfillment of the requirements for
the Degree of Bachelor of Science

by

Tyler Boone

Date: 05/30/07

Professor Brigitte Servatius, Advisor

Table of Contents

Abstract

This is an analysis of privacy in the modern world. It includes suggestions and ideas that can be implemented by governments, companies and individuals to maintain their privacy. This study strives to find the correct balance between privacy, economics and security. Above all, this study is to help the reader understand some of the complicated issues and technologies that are involved with privacy in a modern technological society.

Introduction

Privacy is a hot and complicated topic in the modern society within which we live. Deeply intertwined with other issues, like national security and freedom of speech, privacy rests precariously atop a double edge sword. In some respects privacy protects the individual and his freedoms. However, the same protections of privacy can bring harm, or even death, to the very people it was intended to protect. This phenomenon can be seen in cases such as the September, 11th terrorist attacks on the World Trade Center where the computer-assisted passenger pre-screening system used by the Federal Aviation Administration was purposefully weakened because of privacy concerns, as will be discussed later. Freedom of speech has been limited by the courts in the name of privacy, even in some cases where there were no factual inaccuracies and the offending party spoke only the truth.

Beyond the precarious nature of the ideology of privacy is the actual practice of maintaining and violating privacy. Certainly modern technology has allowed for the invasion of privacy in new and previously inconceivable ways. Telescopic lenses, parabolic microphones, heat sensing video devices, ultra-small video cameras, and other surveillance equipment can allow an individual to continuously monitor a person in his own house without the person's knowledge. Other advances in the world of computers and the Internet have allowed companies to use, sell, and abuse information about customers and people in an increasing number of ways. It is cheap to obtain large databases of information and extremely profitable to sell them. However, as is often the case, the debate over privacy has not been one-sided. In many ways there is more privacy now for the average person than ever before in the history of man. A person can now do all his business from his own home with curtains shut and not admit outsiders

into his world. Anyone that can use a search engine has the ability to perform an anonymous search for anything he is interested in. A teenager can order a pregnancy test; a married and well respected politician can look up information about syphilis; and a terrorist can order materials for bombs, all without the knowledge of a single other person.

The purpose of this study is two fold. First and foremost, it is to analyze the different kinds of privacy intrusions. This involves identifying, understanding and clarifying the various methods which jeopardize privacy. Furthermore, this entails a cost-benefit analysis involving the benefits of increased privacy to society and the individual and the benefits and costs of limiting personal privacy. Secondly, this study will make suggestions of actions to take by citizens, companies, and the government based on the findings and analysis of this study.

Additionaly, this study is a response to David Holtzman's Privacy Lost. Holtzman lays out many arguments which seem compelling upon first observation, but which could use some in-depth analysis. In my opinion, Holtzman overstates the cost of lost privacy and presents the status quo as much worse than it actually is. He also ignores the benefits of the loss of personal privacy to society and in effect to the people in the society.

This study will go over a number of different technologies, cultural practices, and governmental actions that threat our privacy. Privacy violations, in this paper, have been broken down into four main types. The first type is labeled *invasion*. This occurs anytime someone's private space is entered or viewed without permission. The second form of privacy violation is *profiling*. This is the act of making assumptions or speculations about a person based on information that does not necessarily justify these assumptions. This is made possible by the ever-increasing ability to store information

about people, and the amazing ability of computers to analyze the relationships between these facts. Third is *identity theft*, which is currently a red-hot topic, and which does not appear to be cooling down. The final form of privacy violation is *stalking*. Stalking is the practice of tracking and gathering private information about a person. This paper discusses the various methods with which all of these privacy violations are conducted, discuss the societal harm derived from the violations, and justify a response to these methods.

Invasion

Analysis

Invasion is perhaps the most obvious form of privacy violation in our modern society. Hollywood has glorified the tools of the trade with movies like the James Bond series and *Enemy of the State*. Surveillance equipment like cameras and microphones have become digital and their power has been caught up in Moore's Law. Anytime someone is observed while they have a reasonable expectation of privacy, they are victims of invasion.

The case against invasion is compelling. In democratic societies, there is a benefit for people to have privacy because they are allowed to discuss and create and share only with those that they want to allow into their private space. During Stalin's rule in the Soviet Union people were too afraid to say anything negative about the government for fear of retribution. This culture of fear and oppression allowed for the massacre and starvation of millions of people (Johnson). However, in America today there is absolutely no fear of speaking out against the government because it is known that there is no danger of political oppression or repercussions to dissenters. The freedom of speech, in this way, protects Americans from retributions for speaking out against the government or politicians. If someone turns on the television or radio, or goes to the bookstore, he is likely to see, hear or read someone disparaging the government and politicians. It seems almost obvious that this is at least part of what makes America a great place to live and, furthermore, makes the United States a rich and powerful nation. Paul Graham states that "Civil liberties make countries rich," and hypothesizes the existence of a Laffer style curve of government power (Graham 54). For some evidence that this correlation does hold true see appendix A.

Why then is there a need for seclusion? The answer lies in human behavior and interaction in society. A democratic and capitalist society benefits by having untroubled citizens who are at their creative and productive best. Creativity comes from a free flow of ideas between people. This flow of ideas is stifled by a lack of privacy because people that are creative and have new ideas are inherently different from the norm. Unless these creators thought differently than most people, their ideas and inventions could not be considered revolutionary. Not surprisingly when people act different or strange they are more likely to be watched by authorities.

The proliferation of cheap and small electronics has had an amazing effect on the ability of people to spy on others. Ever since the invention of the digital camera photography and video equipment have been swept away by Moore's Law, which states that the number of transistors on a circuit will double every 24 months. This has led to cameras that are more powerful, cheaper and (most importantly) much smaller than their predecessors. Dell's website offers a 7.1 megapixel camera with 2.4X zoom, capable of taking video, for $350 which has a volume of just 105 cubic centimeters. This tiny device could be easily concealed as photographs or videos are taken of unsuspecting people. Other digital cameras and optical lenses on the market could be used to photograph people with amazing clarity from great distances. Most cell phones sold today also have fairly high quality digital cameras built-in. With the prevalence of cameras today it is impossible to go into public without at least risking being photographed.

However, the argument could be made that being photographed in public is not a violation of privacy. Certainly when you are in public you cannot expect people to not know you are there. It is not the act of being photographed in public that is the privacy risk. Instead it is the possibility of a log of all your doings existing for analysis and

interpolation by computers. This theme will appear many times in this study. Most of the violations would, by themselves, not be invasive. However, with the power of the computer to store and analyze amazing amounts of data, all the small violations can be fused together to form a potent threat to personal privacy.

Here, for instance, is a case where the combining of several records could threaten a person's privacy when none of the records alone would imply anything: The government, for some reason, is interested in knowing who a business man is meeting. For dinner this business man picks up takeout from his favorite restaurant. A government computer monitoring his credit card transactions notices the purchase of two meals from the Chinese restaurant, and the computer automatically checks the phone log. The logs indicate that the man made three calls to a business partner that day. From there, the computer checks video feeds from intersections and finds the business partner's license plate at an intersection near the man's house. This makes a pretty strong case that the man met with that particular business partner. This could be damaging information if this man had previously been indicted for fraud or embezzlement connected with this particular business partner. The government agents dutifully note their conclusion that the man met with the business partner. In reality, the man was having a quiet night alone with his wife. Unfortunately for him, the government's circumstantial evidence that he met with his business partner that day could be hard to disprove without a more verifiable alibi.

The kind of information that can be deduced by this kind of analysis is often the actual danger. This has been made possible by the advances in data storage in the last twenty years. Although this analysis is one of the best examples of privacy violation, it will be dealt with in the profiling section. However, the information has to be recorded

before it can be stored; and this is often done with the ever increasing array of cameras in public.

One of the most often used examples of surveillance technology in action is Great Britain. As of 1999 Britain had an estimated 300,000 surveillance cameras in public use (privacy.org). Whether these cameras have been successful in preventing and prosecuting crime seems to be a matter of some debate. According to Simson Garfinkel the "Cardiff City Center showed a 13.4% drop in crime" after installing video cameras (Garfinkel 105). In Newcastle, during a study period, 1,800 people were arrested after being caught on camera. Of those, 1,000 went to court, and all of them either plead guilty or were convicted ("Privacy Police caution Big Brother"). This conviction rate is incredibly high considering that Conviction rates throughout England are currently averaging below 10%. *The Guardian* points out that the best deterrent to crime is not strict sentencing and punishment, but instead increasing the chance of being caught and convicted ("Crime rate soars as criminals walk free"). This seems to indicate that surveillance cameras are a great deterrent to crime. They increase the conviction rate, which in turn makes people commit crimes less often because they have a higher chance of being caught.

However, there is an argument that the cameras are not being used fairly. According to a study by Dr. Clive Norris and Gary Armstrong of the Center for Criminology and Criminal Justice at Hull University:

- 40% of people were targeted for "no obvious reason", mainly "on the basis of belonging to a particular or subcultural group." "Black people were between one-and-a-half and two-and-a-half times more likely to be surveilled than one would expect from their presence in the population".

- 30% of targeted surveillances on black people were protracted, lasting 9 minutes or more, compared with just 10% on white people.
- People were selected primarily on the basis of "the operators' negative attitudes towards male youth in general and black male youth in particular. ...if a youth was [categorized] as a "scrote" they were subject to prolonged and intensive surveillance."
- Those deemed to be "out of time and out of place" with the commercial image of city centre streets were subjected to prolonged surveillance. "Thus drunks, beggars, the homeless, street traders were all subject to intense surveillance".
- 1 in 10 women were targeted for entirely "voyeuristic" reasons by the male operators. (privacy.org)

This study makes it very clear that the surveillance cameras in public are not being used fairly. This seems to be a large problem, since it is unfair to monitor black people more closely than white people. However, nowhere did I read that this extra attention to the minorities led to superfluous arrests or innocent people being inconvenienced. Even if the cameras caught 100% of minority law breakers and 0% of the majority law breakers, this doesn't change the fact that it is only catching outlaws. Furthermore, to say that it is "unfair" to watch certain groups more closely implies that all people are equally likely to commit a crime, but this is not necessarily the case.

While this paper is not intended to be a study of racial profiling, this is an important topic when discussing the use of surveillance equipment. As noted above, one of top arguments against using this equipment is the unfair attention given to minorities, even when the person in question hasn't committed any crimes in his life. While this

practice might seem inherently bad to some people, it is an effective method to increase the safety of the general public. According to counter-terrorism consultant Daveed Gartenstein-Ross, "New York [law enforcement agencies] could spare resources, spare expenses, and make passengers safer if it used terrorist profiling" in their subway system ("Spare No Resource").

An excellent example when profiling could have been effective was September 11, 2001. The computer-assisted passenger pre-screening system (CAPPS) had been developed by Northwest Airlines in 1994. In 1996, after the explosion of TWA flight 800 (which, according to the official investigation, was not caused by terrorists), a federal commission led by Vice-president Al Gore recommended the adoption of CAPPS by the entire airline industry. However, because of pressure by Arab-American and civil liberties groups the system was overhauled. The resulting system had to take precautions against selecting people based on certain characteristics, including race, nationality and religion. To make matters worse, the Justice Department examined the system in 1997 for evidence of racism. Even though no evidence of racism was found, the Justice Department recommended that the Federal Aviation Administration (FAA) require airlines to take steps to ensure that the system's profiling did not become discriminatory or insensitive. The suggestion that a system, whose sole purpose is to profile, be made to not discriminate between various groups is preposterous. By definition, profiling necessarily involves discriminating between various groups. Nevertheless, the FAA complied with this recommendation and discouraged the use of personal searches of passengers in favor of searching baggage and taking steps to ensure that the targeted passengers actually board the same plane as their luggage. These steps worked according to the Council on American-Islamic Relations (CAIR); "profiling complaints dropped from 27 when CAPPS first came online in 1997, to two in 1999, and finally none in

2000" ("Profiles in Cowardice"). While the system had accomplished the political goal of not offending anyone, it failed miserably at protecting people. Only two of the eleven 9/11 hijackers were flagged by the system, and because of the politically correct treatment of the FAA, neither were put through any extra screening, searching or questioning! If the CAPPS would have used ethnicity, race and religion as factors it would have probably flagged all eleven hijackers. If the FAA would have performed personal searches and questioning FAA employees probably would have noticed an extremely alarming trend: multiple Arab Muslims were boarding airplanes together; all of them were in first class; and all of them were carrying box cutters!

There is little doubt that among the Islamic radicals and jihadists, the most detested country in the world is Israel. However, Tel Aviv's Ben Gurion airport "has now gone more than 30 years without a serious terrorist incident" and Israel is "generally regarded as having the safest air travel in the world" ("High Profile"). Israel airports divide passengers into three groups: Israelis and foreign Jews; foreign non-Jews; and anyone with an Arabic name. Furthermore, they actively monitor, question and search the people that are flagged as suspicious.

Holtzman quotes the same Privacy International source that is cited above () as an argument against the use of surveillance cameras (Holtzman 158). However, as explained, this argument is naive at best. To say that surveillance cameras are bad or harmful just because they monitor one group more closely than another group implies that all groups are equally likely to commit a crime. This line of thinking might be comfortable and politically correct, but reality is not determined by convenience. The Israeli airports are safe because they have identified the most likely threats based on data that includes race, religion and nationality. Likewise, surveillance cameras increase the conviction rate and lower overall crime rates, and most so-called abuses of the cameras

are usually harmless, and sometimes even helpful in the fight against crime. For instance, if a camera were installed to monitor, predict and identify perpetrators of violent crime in the United States, the camera would be spending its time better watching American Indians than African Americans. Furthermore, African Americans are more likely to perpetrate and be victims of violent crimes than Caucasians. However, the camera should spend the least amount of time watching Asian Americans since they have the lowest violent crime rates of any race in the United States (Violent Victimization and Race 6). This is not to say that the cameras should ignore Asian Americans and other low threat races entirely. The important thing to keep in mind when analyzing the use of surveillance technology is that it exists to protect the citizens of the community, and by taking into account these parameters, it will have a better chance to witness, and hence deter, crime.

However, not all cameras in public are being used to deter crime. Private citizens now have the ability to buy very small cameras for very little. Because of the cameras that are inside most cell phones on the market today, health clubs have started banning cell phones in their gyms because people have been taking pictures of other members in compromising positions (Holtzman 156). Furthermore, “there have also been several widely reported cases of 'upskirting,' [which is] the practice of surreptitiously maneuvering a camera underneath a woman's skirt and taking pictures” (Holtzman 156). While the health clubs' method of banning cellular phones probably decreases the chance of having a picture taken of you while you are working out, there are problems to this solution. Firstly, it punishes many for the actions of few. For every person that has used a cell phone to take pictures in a health club of someone who is unaware, there are hundreds that now cannot bring their phone into the gym, causing them to potentially miss calls. Secondly, this measure will not completely eliminate the problem.

Presumably, the people taking the pictures were covert and tried to avoid being caught taking the pictures. It would be hard to identify and stop someone from bringing in a cell phone if he was determined to bring it in. Finally, health clubs are private organizations with members that choose to go there. This allows the health clubs to create rules that ban cell phones. Health clubs that do impose this rule can even use it to help market their gym since people that are concerned about privacy might enjoy having the protection of the ban while they are working out. However, there are many other places where people would probably not want to be photographed that cannot adopt a cell phone ban just because they are concerned about the privacy threat imposed by the cameras. Many high schools require that students take a number of PE classes in which the students must dress out in the locker rooms. Judging from my own experience, a large majority of high school students have their own cell phones, and it is impractical for the school to place a ban on them. Students need them in order to contact their parents or friends to arrange for a ride home or to coordinate other activities. Perhaps a better solution than an all out ban on cell phones in certain areas is to impose a rule against taking pictures in the area with the promise of a strict punishment if the rule is broken. While a ban on cell phones might be impractical in a high school, how many students would risk expulsion or a fine just to take a picture of a classmate?

Laws banning the use of cellular phones are taking away freedom. When private organizations create rules banning cell phones it is acceptable because citizens can choose whether or not they want to patronize the organization. However, when a government organization, like a high school, bans cell phones the citizens have no choice but to loose their freedom. The responsibility of policy makers is to determine if the threat to personal privacy because of the possibility of a picture being taken is worth the loss of freedom. As I have pointed out above, there are alternatives to banning cell

phones that emphasize strict punishment for actual privacy violators and allow greater freedom for the average citizen.

Another possible way to intrude on someone's privacy is through auditory eavesdropping. Indeed, a lot of the fancy technology employed by government agencies to monitor and spy on people is sound equipment. Whether it is hidden microphones in The Italian Job, parabolic sonar dishes in Enemy of the State or even lasers that can read the vibrations of windows to record a conversation, popular culture and the real world are filled with methods to listen in on other peoples' conversations ("Listening in on Block Talk").

One thing that is important to note about eavesdropping is that most of the complaints and problems with it more tangible than the problems with pictures and video. The most common problem people seem to have with being photographed or video taped without their knowledge is a loss of dignity, because they might be photographed doing something embarrassing, they could be in a compromising position, or their body could be exposed to someone whom they did not wish to see it. However, the effects of listening in on somebody's conversations can be much more serious. For instance, if there is an information leak to the media, the informant's identity could be compromised by audio wiretapping. The right of the press to not reveal its informants' identities has long been an important value in America. Without these informants, politicians would be able to get away with scandalous behavior because there would not be anyone on the inside passing information to the press and the voters. One such example is William Felt, otherwise known as Deep Throat, who was Woodward and Bernstein's informant during the Watergate scandal. It is possible that without the cover of secrecy, Felt and other such informants would not have cooperated with the press and leaked sensitive information.

Another valid concern dealing with audio eavesdropping is the possibility of something being taken out of context or interpreted incorrectly. If a camera records a murder there is little room for doubt that the murder occurred and the photographic evidence pointing to the identity of the perpetrator is straight forward. However, if the police are investigating a murder and they wiretap a suspect's phones there is a chance for the suspect's words to be misused. If the wiretap records the suspect as saying something to the effect of, "I killed Alice," this could be damning evidence in court, even if it was a bad joke or just a phrase in a conversation that was taken out of context.

Aggravating the privacy threat of the telephone system is the current trend towards increased mobility. In the days when both parties had to hold a receiver to their ear to talk to each other on the phone there were only three ways to eavesdrop on a call. One method is to have a microphone in the same room as one of the parties. This is both dangerous and expensive. People have to physically go in or near the room to plant the device, and then there is the risk that the target of the eavesdropping will find the device. Another method is to insert an actual tap on a line somewhere between the two ends of the phone call. Since this is only effective where there is not many other lines of communication interfering with the call, this must also be done near one of the end points of the call. This also requires specialist equipment and personnel to install. The third method is to implement the tap at the phone company itself. This has the benefit of being harder to detect and easier to implement. However, this also requires that the eavesdropper be a law-enforcement officer and obtain a warrant.

Unfortunately, this changed with the advent of the cordless phone. Now when someone is on his cordless phone, the handset and phone base happily communicate with each other wirelessly. Even though most modern cordless phones use some form of cloaking mechanism, it is still possible to buy a scanner that can eavesdrop on a phone

conversation using a cordless telephone from outside the caller's house and without installing a tap on the physical line (Holtzman 161). The problem is even worse with cellular phones. Not only can scanners intercept cell phone conversations because they are generally not encrypted (Holtzman 161), but there are devices that can be used to listen to cell phone calls from anywhere. In the movie Enemy of the State, one of the characters plugged a hacked cell phone into a laptop and was able to listen to conversations of a US Senator. According to *Mobile Phone News* such devices are not only possible to make, but one has been found by police that can store up to 99 electronic serial numbers and mobile identification numbers, which is how it eavesdrops on conversations ("Agents find scanner/eavesdropper disguised as a cellular phone").

One reason people often do not worry about encryption and security in their communications is because the average person isn't hiding anything interesting from the government. Perhaps they have cheated on their taxes, but the IRS probably won't tap your phone just to collect a couple hundred dollars. However, with these scanners and eavesdropping devices it no longer takes professionals with warrants to listen to a phone call. A jealous ex-spouse or stalker, who has sufficient knowledge and resources, could employ these devices without you knowing.

Suggestions

While, in my opinion, the threat to our privacy caused by advances in technology has been overstated by Holtzman and others 10, this does not mean that privacy is not a real issue. Furthermore, even though in many cases the benefits of surveillance equipment outweighs the loss of privacy, it is up to the people to maintain checks and balances on the government use of surveillance technology.

One of the best ways to maintain checks on governmental surveillance is through education. The more people know about the use of cameras and microphones used by the

police, the less likely it is that they will be misused. An excellent way to stay educated is to read books like Holtzman's Privacy Lost and Garfinkle's Database Nation as well as newspapers, and to watch and listen to local broadcasts. While some of these sources might go too far in their accusations against the government and law-enforcement agencies, they present good information that a well informed citizen should be aware of. Personally, I listen to talk radio on the way to work and on my way home which has been an excellent way to stay up to date on all sorts of topics, including privacy matters. Recently I heard reports on the radio about surveillance cameras being installed in Boston, which seems to be a completely reasonable measure in response to the horrific spike in homicides recently. Boston's homicide rate is up 50% from last year ("Boston and Beyond"). However, there was also discussion about Massachusetts Secretary of State William Galvin, whose official website has links to personal information that could be used to commit identity theft, which is a topic that will be discussed later (34). Interestingly, Galvin has refused to take down the links even though he admits they are a problem and says that "personal information will be 'scrubbed' clean within a few weeks" ("Privacy Advocates Blast Galvin"). According to the Worcester Telegram & Gazette *News* the site contains "Social Security numbers, bank account numbers, home addresses and [telephone] numbers of Massachusetts residents." It is important that the public be informed about these things because in order to take action and fight for privacy rights, one must at least know what is happening in the world.

While the best way to avoid being watched by the government is to not break the law, and to not act suspicious in high privacy areas (like airports and subway stations), there are steps that can be taken to avoid being surveilled by private entities as well. If you are worried about someone taking pictures of you at the gym try and locate a gym nearby that has banned cell phones and cameras. If there is not one nearby you can

always bring it up to the management of your gym for consideration. Gold's Gym, the largest coed gym in the world, already has a ban on cell phones on the gym floor through all its locations. However, if you are a high school student or parent of a high school student, your school probably does not have the same rules as a private gym. If there are not already strict penalties for students (or faculty) that violate someone's privacy in the locker rooms or in the school gym, a group of parents can have a big impression on local school boards. By imposing harsh sentences on those that violate others' privacy, rules can be a strong deterrent for prospective violators.

The technology to eavesdrop on telephone conversations is not in the mainstream. Unless someone is paranoid, is dealing with extremely sensitive information, or has a reasonable suspicion that his phone calls are being listened to by a third party, he probably does not need to take any steps to secure his conversations. However, there are steps that can be taken. First, anytime that you are dealing with sensitive information it is best to use the most secure communication medium possible. Instead of making a cell phone call, there are more secure ways to communicate. There are free programs that can send encrypted email and messages, and if you need audio communication, there are solutions for that as well. PGPfone and Skype offer solid encryption for voice data from computer to computer (Skype Security Evaluation), and there are also voice over IP (VOIP) phones that offer strong encryption for their users. The downside to these solutions is that they tie the user to a location with broadband Internet access. There are cell phones on the market that offer end-to-end encryption. Unfortunately, this solution requires both ends be using the same cellular phone, and at $2,000+ for each phone, this solution is too pricey for most businesses and individuals. Luckily, as is the trend with almost all things electronic, the price for these devices will surely fall. Just ten to fifteen years ago cell phones were extremely rare and expensive. Intuitively, as the production

costs fall (because of Moore's Law 8) and consumer demand increases, the price of mobile phones that offer encryption and secure communication will drop. One thing that is important in this process though is transparency in the internal workings of the cryptographic system. Cryptophone, a brand which currently offers two encrypted mobile phones, has taken the initiative and made the entire source code to the phone public so that people can spot weaknesses in the encryption algorithm and implementation. Another important thing is standardization. Without standardization, to communicate securely with other cell phone users you will have to either have the same phone or make sure that the two phones comply with a certain protocol. This could mean that both phones be made by the same company. The Internet is a perfect example of the success of standardization, which is currently done by the Institute of Electrical and Electronic Engineers (IEEE). If the IEEE or similar organization were to create a standard for secure mobile encryption, this would be a great benefit to the mobile community and to privacy as a whole.

Profiling

Analysis

As mentioned earlier (9), much of the danger to privacy caused by new technology is not caused by better microphones and cameras. Instead it is caused by the ever increasing ability of computers to store and analyze data. For just a couple hundred dollars one could buy a hard drive capable of storing over 21 days of near CD-quality audio[1]. Furthermore, the processing power to analyze all this stored information is getting cheap as well. However, just this fact does not pose a serious privacy threat.

Without networking and interoperability, a computer could only analyze data that was captured by itself or imported through some manual process. This does not scale very well for the millions of people in American cities. However, due to interoperability and networks, hundreds or thousands of sensors and smaller computers can all send data to a single data center where storage and processing can be centralized. With advertising agencies and companies collecting more information about consumers that ever before, companies can start to use information to target certain people with individualized advertisements and service (or the lack thereof).

One of the problems with collecting all this information is an entity's ability to positively identify an individual based on certain criteria. For instance, if a large chain company put a video camera in front of its stores to identify all the people that walked by their store, could they identify most of the people that show up in the video? Through the use of various types of biometrics, a sufficiently capable computer should be able to identify all the people that walk by their store that are within the company's database. “British Telecom ... has developed a high-speed iris scanner that can capture the iris print

[1]Assuming MP3 encoding at 1 MB/minute and a 300 GB hard drive. (300 GB * 1024 MB/GB) / (60 minutes/hour * 24 hours/day) = 21.333 days / hard drive.

of a person driving at 50 miles per hour" (Garfinkel 56). A person can also be identified by the way they walk and by facial recognition as well as other forms of biometrics. Currently there are two things stopping companies from employing these kinds of things in and near their stores. First, the price is prohibitive for a camera with resolution sufficient to perform positive identification. Furthermore, the computers to collect, analyze and store the data are expensive. However, consumers cannot rely on this being the case for long. The price of computing power and storage space has dropped steadily since the inception of the computing age. Within only a few decades the computing power available only to large businesses with multi million dollar information technology budgets can now be purchased by people and carried in their pockets. Without much doubt, the ability to store and analyze all this information will be within the price range of many large companies in the near future.

This does not, however, mean that companies will be employing these techniques wholesale as Holtzman suggests (Holtzman 173). Public disdain and outcry over privacy violations have been strong motivators to governments and businesses alike to adopt stronger privacy legislation and policies. One such example is the case of Judge Robert Bork, who was appointed to the United States Supreme Court by President Ronald Reagan. During his confirmation hearings a "journalist from Washington, D.C.'s liberal *City Paper* visited a video rental store in Bork's neighborhood and obtained a printout from the store's computer of every movie that Bork had ever rented there" (Garfinkel 72). The judge's rental choices were fairly mild, but the outcry against the invasion of privacy was enough to prompt the passage of the Video Privacy Protection Act (Garfinkel 72). While this legislation is extremely narrow minded and would be much more effective if it covered more than just video rental stores, this is most certainly a case of public outcry forcing a change in policy to help protect individual privacy.

Some widely used collections of personal information are contained in databases maintained by the credit reporting bureaus Experian, Trans Union and Equifax. The power of the information in these databases is staggering. In our modern society it is hard to live without using credit. Except for the rich, everyone that purchases a home has to obtain a mortgage. It is also difficult to purchase a car, which is needed in many places if someone needs to commute to work, without obtaining credit. Furthermore, without a major credit card, certain businesses, like car rentals and hotels, will not sell someone their products. This could be disabling for someone who travels a lot for his work. Anytime a company extends a line of credit to someone, they will most likely get a credit report from one or more of the credit bureaus.

The problem with credit reports having such an impact on modern life is that they often contain misleading or false information. "Privacy activists say that more than 50% of all consumer files have a significant error in them" (Garfinkel 28). When Consolidated Information Service conducted an analysis of 1,500 credit reports from the three major credit bureaus they found errors in 43% of the reports (Garfinkel 28). In 1991, 1,400 homeowners in Norwich, Vermont were mistakenly identified by TRW (which later became Experian) as tax delinquents because a "TRW contractor gathering home mortgage information mistakenly noted tax bills on town records as tax liens" (Garfinkel 28). Some sources have even reported worse numbers among credit reports:

> ... a study released by the U.S. Public Interest Group in June 2004 showed that as many as 79 percent of credit reports had errors, with more than 50 percent containing outdated information or data belonging to someone else, as well as 25 percent containing mistakes serious enough that credit could be denied.
>
> (Holtzman 20)

Another problem with credit reports is the kind of information recorded. Dr. Alan Westin, Professor of Public Law and Government at Columbia University, testified

before Congress that the credit bureaus may include “facts, statistics, inaccuracies and rumors ... about virtually every phase of a person's like: his marital troubles, jobs, ... sex life, and political activities” (Garfinkel 22).

Even worse is that when inaccuracies do exist in a credit report it is often extremely hard to get the incorrect data removed. When an error is found on a credit report, the bureau will ask for a written statement or explanation and perhaps a letter from the organization that the record deals with. However, even if all of this paperwork is sent which proves that the record is completely incorrect, the credit bureau might not correct the report. “When you have an unfavorable note in your credit report, they don't take it out; they just put your explanation with it” (Garfinkel 27). When Bonnie Guiton, the White House Advisor on Consumer Affairs in 1989 requested a copy of her credit report she discovered a credit card account that a stranger had opened under her name. Guiton wrote to the credit bureau asking for the incorrect information to be deleted and received a letter back stating that it had been corrected. However, a few months later when she requested another copy of her report, she found that the account was still listed (Garfinkel 29). Not only is it hard to get the companies to remove inaccuracies from the credit reports, but after they are removed it is possible that the database will become reinfected with bad data from a source that had already purchased that information from them earlier. For example, a credit bureau has an incorrect piece of information and sells it to another company that maintains a database of consumer information. The credit bureau corrects the report after the consumer has gone through considerable effort to prove his innocence. Then the credit bureau purchases the consumer database from the company they had sold the bad information to in order to keep their files as up to date as possible. The computers merge all the data and put the incorrect data straight back in the credit

report. Credit reports are so notoriously filled with inaccuracies that credit card companies have come to expect them and account for them (Garfinkel 28).

Not only are many credit reports filled with inaccuracies, but the Fair Isaacs Corporation (FICO) credit score is based on a secret formula. When lenders are determining a consumer's credit worthiness, they will often look at the credit score, which is available from the credit bureaus for an additional charge. The credit score is the number that can be heard passed around on advertisements to make your credit better. It is a number from 300 to 850 that supposedly gives an overall rating of the credit risk a person is for the lender. However, since the credit score is not actually data in the credit report, it is not covered by the Fair Credit Reporting Act and therefore you have no right to see it or understand how it is calculated.

Credit reports are just a single example of profiling. Any system that systematically processes data about people and comes to conclusions that are not implicitly stated inside the data is profiling. In essence, profiling is just guessing carried out by computers using rules and algorithms programmed by people. Obviously these rules can be faulty and unfair, but even if a rule does work, there are always exceptions.

Casinos are a perfect example of profiling, and they show that not all profiling is bad. Casinos will often treat their larger customers better by giving them free meals, tickets and nights at their hotels ("High roller Las Vegas suites"). Casinos categorize their customers into levels and give them service comparable to their level. For instance, there are sections of certain casinos which you can only enter if you are a "high roller." These sections may have things like a free drink bar, but they also have tables with minimum bets in the multiple thousands. While the average casino-goer might enjoy a free martini, I doubt he would be interested in a table were the minimum bet was more

than he makes in a month! The casinos watch their customers' gambling behavior and make guesses about their future gambling habits based on these observations.

When I worked at Panera Bread Co. we performed a simple form of profiling. We certainly treated the customers that came in every day differently than those that we did not recognize. Occasionally we might give a "regular" some free bagels, and we would be more lenient on certain rules, allowing them to go in the back and talk to a manager, or opening the doors for them before the store was officially open. Our profiling system was not programmed into the computers; the cashiers just recognized certain customers. Blockbuster Video also performs this kind of customer profiling (Brennan interview). The top 5% of customers in each store are invited to be "gold rewards members" for free. A gold rewards member receives a variety of perks including: free rentals; "special considerations regarding late fees"; the ability to "jump" people in a waiting list for a movie; and access to a special customer service line to call with complaints. According to Matthew Brennan, who worked as Assistant Store Manager for Blockbuster Video, the ability to jump people in waiting lists was not an advertised perk, but rather an internal practice to keep the gold members happy. Nevertheless, this implies that a customer who does not fall within the top 5% will systematically receive inferior service from Blockbuster compared to a customer within the top 5%. This is facilitated by the company's interconnected computer system. When a customer's card is scanned at any location the computer screen displays to the clerk information about the account, including its status as a gold member.

Many companies keep records of past business they have done with their customers. Whenever I go to Best Buy they always attach my purchase to a record they have for me. If I use my credit card they use the credit card number to find my record. I also take part in their *Best Buy Rewards Zone* program where I have them scan a card

every time I purchase something there, and in return they send me coupons in the mail. Even when I pay with cash and don't use my Rewards Zone card, they ask me for my phone number. If I chose to give it to them they can attach the sale to my record using my phone number. I do not mind this because if I have a problem with an item I bought there I don't need a receipt. I just give them my phone number or credit card and they can find the purchase. Furthermore, they are lenient with my returns and allow me to return things that are actually against company policy to be returned. For instance, I have returned head phones that were damaged when I dropped them. Best Buy might choose to allow me to return these kinds of items because their computers tell them that I am a good customer. I have spent thousands of dollars there, and have returned very little. However, if someone else tried to return something, and the store's records showed that he returns half the items he buys, the store might not allow him to return the item. While such discrimination does not bother me because I have not been targeted, such a system would not be foolproof. If a record was corrupted or wrong and showed that a customer had returned items that he actually had not returned, he might be denied service.

More companies record the purchases of their customers than just Best Buy. Grocery stores have been saving all their customers' purchases for many years now. They advertise their “reward cards” as giving customers better prices. In exchange for these lower prices, customers agree to allow the grocery store to collect certain information including “the date that your order was rung up, the items that you purchased and the total dollar amount of your purchases” (Rewards Card Privacy Policy). One might wonder why the grocery stores are interested in maintaining a record of every purchase you have made in their stores. The answer, in short, is service and marketing.

> Dorothy Lane Market, an upscale grocery chain in Ohio, already uses the data from its loyalty cards to determine the value of individual customers. The company analyzes the data it collects and uses them to

> identify the customers who spend the most. Customer Specific Pricing allows the chain to charge different prices to each segment of customers, with most of the discounts going to the top 30 percent of shoppers.
> (Holtzman 44)

Shaw's, a New England based grocery store chain, provides detailed information about the use of purchase information obtained through their rewards cards in their privacy policy. Their policy explicitly states that the information can be used to target specific advertisements and offers to the people they think will be interested in them. Furthermore, while they promise not to share any personally identifiable information with third parties, they do share aggregate purchase information with third parties. Luckily, Shaw's offers a way to receive their "discounted" prices while not having your purchases recorded by calling or visiting a customer service desk.

While many companies collect information about their customers by their purchasing behavior, the problem is amplified by the amount of information sharing among these companies and the advertising agencies. Macy's department store sold data about 1.5 million customers "including their credit-card numbers, birth dates, and email addresses" for $90 per thousand names (Holtzman 16). For an extra $15 per name they would include additional information including household income and the ages of children. Luckily, consumers have fought back against some of the information sharing. Lotus and Equifax created a CD-ROM called "Lotus Marketplace: Households" which included demographic information for every household in the United States. Fortunately, "the project was canceled when more than 30,000 people wrote to Lotus demanding that their names be taken out of the database" (Garfinkel 9). However, cases like this have not significantly stemmed the sale of personal information between businesses. Due to high bandwidth networks, the sale of personal information is extremely cost effective. If

a company can sell information, they achieve practically 100% profit on the sale, because the cost of transporting the data is effectively zero.

Even when customers think that they are protected by a company's privacy policy, their information might not be safe. Courts have rules in favor of customers in most cases involving privacy policies. When Toysmart.com went bankrupt in 2000, the company and Disney (its parent company) attempted to sell its customer database with 250,000 names, thereby breaking its own privacy policy. The Federal Trade Commission filed a lawsuit against them, and the company eventually agreed to destroy the database. In 2001, Massachusetts Attorney General Tom Reilly blocked bankrupt Essential.com from breaking its privacy policy and selling a customer database of 70,000 (Holtzman 116). Unfortunately, a company does not have to be declaring bankruptcy to be morally bankrupt! Since the year 2000 many companies have been sued for violating their privacy policies and selling customer information to third parties, including: eTour, Sears, Procter & Gamble, Pfizer, Albertson's and JetBlue Airlines (Holtzman 116). This is not even to mention the breaches in security at many companies and loss of customer information that will be covered in the section on identity theft.

Suggestions

One of the simplest ways to protect you against companies buying and selling information about yourself is to read privacy policies. Many times reading a privacy policy can alert a customer as to a company's bad practices in regards to information sharing and using. Facebook, a popular social website among college students, has many interesting phrases in their privacy policy:

- *We may use information about you that we collect from other sources, including but not limited to newspapers and Internet sources such as blogs, instant messaging services and other users of Facebook*
- *Facebook may use information in your profile without identifying you as an individual to third parties. We do this for purposes such as ... personalizing*

advertisements and promotions so that we can provide you Facebook. We believe this benefits you.

- *We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you.*

(Facebook)

Privacy policies are almost always written to be as forgiving and lenient for the company as possible. Facebook's policy is no different, and as such limits the company as little as possible. In their privacy policy Facebook blatantly states that they will: collect information about you from other sources; personalize advertisements to you using your information; share your information with other companies so that they can target advertisements toward you; and share your information with third parties if it is "reasonably necessary to offer the service" or "permitted by you", two phrases which can have extremely broad interpretations.

Beyond reading privacy policies and only doing business with companies that have acceptable conditions in them, you need to stay informed with news. If you hear about a company that you have done business with violating their privacy policy, spread the word. 30,000 people stopped Lotus from releasing *Lotus Marketplace*, but it takes far fewer voters to get the attention of politicians. While the government is often one of the largest adversaries to privacy, they are also one of the strongest advocates. The government forced Toysmart.com to destroy their customer database when they tried to violate their own privacy policy. If a company is using or trying to use information about you in a way that is illegal, try and get the government involved by organizing a group to lobby politicians, or write a letter to the editor of a local newspaper.

When it comes to consumer credit reports, the most important thing is to know what is on your credit report. By law, all credit bureaus must provide consumers with one free copy of their credit report per year upon request. The official website from

which to obtain your free credit report is www.annualcreditreport.com. The best way to protect your credit rating is to know what is on your credit report. Obtain credit reports from all three of the credit bureaus listed on annualcreditreport.com every year. Make sure none of them contain inaccuracies or accounts that you did not open. If they do, ask for them to be removed. If the mistakes are serious you might have to seek the help of a lawyer or credit specialist to deal with the credit bureaus.

If you do not like the idea of grocery stores tracking all your purchases, read their privacy policy. If it is available like at Shaw's, call the store's customer support and ask them not to track your purchases. Even if a store does not provide this service there are ways to throw off the system. Put down fake information when you sign up for the card. If you do not want to receive their special promotions in the mail, the best protection is to not give them your address. If you know other people that go to the same stores, you can occasionally swap loyalty cards with them so their records are never of just a single person. If this is not good enough you can always just not use the rewards card. Usually when I go to the grocery store I tell the checker that I do not have a card, and they will swipe their own card that they keep next to the register.

All of the suggestions in this section have been based on the (perhaps incorrect) assertion that the reader would like to limit companies' ability to profile him. It is important to remember that profiling does serve a purpose. If a company maintains information about customers, they can do selective advertising to the customers that have a greater chance to purchase the product. This is beneficial because it would decrease the amount of uninteresting advertisements that we are shown. For instance, I receive a lot of advertisements in the mail from local colleges and community colleges advertising their summer classes. These institutions obviously have some information about me. They know my name and where I live. They probably know that I am the right age for

taking summer classes. However, what they do not know sometimes is my current enrollments for summer classes. I receive many letters advertising courses that are offered at the same time as courses that I have already registered for. If these institutions knew that I had already enrolled in classes for the period they were advertising they could save money by not sending me these advertisements. I currently pay $34.95 per month for a Digital Subscriber Line (DSL) from Verizon. Nonsensically, Verizon sends me an advertisement in the mail almost every week to get a slower DSL service that costs only $14.95 per month. I wish that Verizon would perform some simple profiling and not send its own customers advertisements for cheaper products than they already subscribe to. This would not only save Verizon money on printing and mailing advertisements, but it would save me the time of opening the envelope and throwing it away.

Identity theft

Analysis

Identity theft has received lots of media attention in the last couple years, and for good reason. Identity theft has been consumers' top complaint for the past seven years, and last year identity fraud cost consumers $49.3 billion ("FTC finds identity theft remains consumers' top complaint"). The average cost for someone who's identify is stolen is $4,800 and 600 hours (Holtzman 26).

There are usually two ways for an identity thief to obtain someone's information. The first way is by obtaining the information directly from an individual. A thief might steal credit card offers from your mailbox, or take bank statements out of your trash. A more high tech way to get account information is by sending out bulk "phishing" emails. A phishing message is usually made to look like a legitimate email from a bank which cites some kind of problem with your account. It includes a link which appears to take you to the page where you sign in to your account. However, the link actually takes you to a page set up by the thieves to capture the targets user name and password. An example of a phishing email that I received can be seen in appendix B. In Europe a common scheme is for a waiter to attach a card reader on his belt and discretely slide customers' cards through when he is ringing up the order. At the end of the night the waiter can save the information onto his computer and either use it himself or sell it. A stolen credit file goes for about $30 (Holtzman 24). If a waiter were to collect information for a year before leaving town and selling the data, not only would the source of the fraud be hard to detect, but the thief would stand to make a lot of money. There are other similar rackets which use insiders to get personal information. One man and his

sister who worked in a collections agency in Houston, Texas went through obituaries and opened credit cards under the names of dead people (Holtzman 26)!

The other way to obtain customer information is by getting it indirectly as through a company or business that stores personal information. Recently TJX, a large department store chain, discovered that its computer system had been hacked and that the credit card information of 45.7 million cards had been compromised ("TJX reports on identity theft"). Similar breaches have made news, including laptops stolen from a contractor for police departments in the United Kingdom which contained payroll information for police officers, and a laptop owned by the Federal Trade Commission which had data collected on people during law enforcement investigations.

Suggestions

There is no doubt that identity theft is a problem. However, it is a problem without clear solutions. One possibility that is being considered in the United States Congress is to impose more strict penalties to companies that lose customer data. Executives analyze the cost of losing customer information against the cost of protecting the information and too often decide that it is cheaper to be reactive to data loss than to proactively protect the data. In four months between the date of this writing and the date that TJX first reported to authorities that they had lost customer data, the stock price has dropped less than a point (-3%)[2]. It is clear that the executives of companies like TJX just do not feel the pressure to protect their customers' information! If legislation is passed that imposes strict punishment for companies and accountability among executives, data integrity will suddenly become more of a priority. The negligence by the executives of the company is appalling, and some of them deserve jail time. What business does TJX have storing credit card information detailed enough to create fake

[2]TJX stock prices: December 22, 2006: 28.75 -- April 5, 2007: 27.89 (source)

cards for years after a purchase? If they were using the information to identify customers, like I described Best Buy doing with their returns, they could simply save a hashed value of the credit card number. Instead TJX stored the credit card number, expiration date, and security code. This is not only in contradiction to common sense, but they were in direct violation of Payment Card Industry data-security standards ("A Matter of Responsibility"). Julie Ferguson, vice president of a consumer identity theft protection company, even states that she has spoken to some businesses that "are waiting for someone to be made an example of."

On an individual basis, it is hard to avoid having your identity stolen if a thief gets your information from a company database. However, by knowing what is on your credit reports, it is possible to tell when someone has probably stolen your identity.

Fortunately, there are many steps to help avoid being the victim of identity theft:

- Tear up or shred junk mail and documents before throwing them in the trash.
- Report an initial "fraud alert" to the major credit bureaus if you suspect your information has been stolen. This makes creditors take extra steps before extending you credit. While this can be useful, it can also make it harder for you to obtain credit.
- Run spyware and virus scans on your computer regularly. Upgrade to the latest version of your web browser. Internet Explorer 7.0 and Firefox 2.0 both contain phishing detection software to alert you when you might be at a phishing site.
- Insist that your employer and everyone you do business with not use your Social Security Number unless it is absolutely necessary.

The above list is not meant to be exhaustive. For more information and steps to prevent identity theft, you can visit the www.annualcreditreport.com section on identity fraud.

Stalking

Analysis

The emergence of technology capable of identifying people based on biometrics might make cities of the near-future more like the small town of yesteryear. In small towns of a few hundred, everyone knew everyone else, and before modern technology all business in these towns was local. Because of this it was basically the case that the people in the town knew what the other people did all day. Now modern technology can monitor people so that at least the computers can know what the people are doing all day!

The enabler of computerized tracking is interoperability and networking. As networking hardware gets cheaper, and the prevalence of wireless area networks (WAN) increases, it becomes easier to network electronics. Without the wireless IEEE 802.11 standard, devices from different makers and made at different times would not be able to interact. However, because wireless communication has been standardized, it is possible for a variety of devices to interact with each other. For some, this could be a useful tool. One common vision of homes in the future is that of the digital and connected kitchen with a refrigerator that will send you emails or text messages on your cell phone when items have gone bad, or are running low. There are currently refrigerators on the market that have an LCD screen, and which connect to the Internet. However, the technology and intelligence to detect when a particular item is running low or going bad has not emerged. Furthermore, there is no consumer trend toward items like this. While it is common to find a television in the kitchen, and in some cases a computer terminal to look up recipes, an interconnected kitchen seems to have been "right around the corner" for many years now. There are exceptions of course, Bill Gates's house senses who is in a room and adjusts the environment accordingly (US News Interactive Virtual Tour).

There are multiple reasons for the lack of progress on a digitized and connected house, some of which will be overcome by the steady advance of technology, others which might not. First, the cost of networking most devices is too high. Even if wireless networking could be built into a device for $1, this is still substantial cost to the manufactures. Normally when an item costs more to make because of added features or quality, it can be accounted for by either increased sales or increased per product prices. However, the market doesn't exist for a toaster than sends text messages when it is done toasting! The competition for household gadgets is driven by quality and price, not features that are more a novelty than useful. Holtzman envisions a house "swarming [with] devices capable of both human and peer-to-peer interaction" (Holtzman 174). However, this is not accounting for some basic principles. First, these devices will only exist if there is sufficient market demand; second, market demand for such devices will only be created if they solve a problem or satisfy a desire. Holtzman also fears that these devices will communicate information back to the company that made them without the user knowing. This has been a topic of some debate among the software industry for a number of years. Winamp, a popular media player for the Windows operating system, by default sends anonymous usage statistics to the Nullsoft, which is the company that makes Winamp. Winamp collects information about the amount of use of various features in the player including, the use of plug-ins, play lists, and session length (Winamp Privacy Policy*)*. While I would not mind if these statistics were collected from myself, some people might not like this kind of information being sent from their applications and household items. The key to these anonymous statistics is that Nullsoft has made it obvious that they are being collected and easy to turn off. During the installation of Winamp there is a screen devoted to information about how Winamp sends this usage information with an option to turn it off. As with modern software, if a

household item is found to send information back to the manufacturer without informing the consumer that this is being done and providing the option to turn the feature off, there will likely be a customer backlash that most companies do not want to deal with.

Another reason why customers are not rushing to the stores to buy networked appliances is that they are not ready for the new technology. Most people do only simple tasks on computers such as surfing websites, using email, using an office suite and listening to music. When something breaks or needs to be changed they have to get help. This phenomenon is the reason Best Buy's Geek Squad does well even when charging $129 to add a computer to a network, $29 to install a piece of software and $129 to install an operating system[3]. Many people in society are suffering from an information overload.

While the future of homes filled with "swarms" of networked devices is anything but determined, there is another technology that holds the promise to easily track goods, items or even people. A new computer chip has been created called a radio frequency identification (RFID) tag. RFID tags work by transmitting an electronic serial number to be picked up by a receiver. The most revolutionary feature of RFID chips is that they do not require an internal power source. This means that they can be extremely small and inexpensive. The Boston Marathon uses an RFID chip attached to runners' shoes in order to officially calculate their times. RFID chips can be a blessing for retailers and distribution centers. At about 5 cents per chip, products can have an RFID chip put into their packaging. This allows retailers to use an RFID scanner at checkouts without taking items out of the shopping cart. RFID chips also allow pallets to be stacked higher and wider, since it is no longer necessary for bar codes to be visible from the outside for an inventory control system to detect. An entire pallet of items can be inventoried at once,

[3]Priced obtained from www.geeksquad.com on 4/11/07. Prices are the lowest quoted price not including phone support.

instead of the manual process off scanning the bar code on each box into a scanner that records the inventory. The technology has received high praise from Wal-Mart, which is actively encouraging suppliers to implant RFID tags into product packaging. "[Wal-Mart] can restock RFID-enabled goods three times faster than nonequipped merchandise" (Holtzman 177).

Certainly, using RFID chips to inventory products and time races is useful and presents only a small risk to privacy. However, because of the small size and ability to operate without a power source, RFID chips can also present a considerable threat to privacy. The US Government is putting RFID chips into passports that transmit more than just an identification number. The passport RFID transmit all the information in the passport as well as a digitized picture of the person. Holtzman fears that RFID chips would be dispersed so widely and put into products themselves in such a way that people would not even know. He illustrates a city covered with sensors that read the RFID chips in these products and can track the movement of people throughout the city.

While this situation seems a bit far fetched at first, the reality of RFID chips is alarming. The FDA has approved RFID implants for human use, and there are actually companies that are doing just that. VeriChip Corporation specializes in creating chips for health care uses. They advertise their chips as providing a safe and reliable way of identifying patients who are hospitalized and perhaps unconscious. They also have touted that the implanted chips can be used a secure form of access control. VeriChip calls RFID based security "the highest level of security" (Veriguard Access Control Pamphlet). While effectively bypassing an RFID system might be difficult, "independent security consultancy Securenet, which is employed by the commercial and public sector to conduct ethical hacking, has proved able to skim and clone information from chips embedded in passports or cards" ("Radio Waves"). However, beyond the glaring security

problems, implanting a device in my arm just so that I can get into a secure area at work seems at the very least demeaning. Requiring employees to have a device implanted into their bodies just to do their work degrades them as humans. In the end, an RFID chip is little more than an electronic bar code. I have seen people with bar codes tattooed to their bodies. Usually, they are making a statement about society and culture, but there are similar markings that have been tattooed onto people that are not. For instance, the Germans tattooed prisoner numbers on some people at Auschwitz during the Holocaust as a way to "dehumanize their prisoners" (Tattoos).

VeriChip also markets an RFID system to be installed in nursing homes that monitors the location of the elderly. While this solution might be beneficial, it is just as dehumanizing as the chip used in employees. Law enforcement could also use RFID implants on criminals to monitor them in jails or to enforce house arrests. The privacy implications are severe for this use however. If prisoners are implanted with RFID chips, there will be a stigma against RFID implants, which will curb their use. However, nothing would stop a store owner from purchasing an RFID reader and placing in his store. They could even configure the device to lock the doors of the store when it sensed an RFID tag that matched certain criteria!

RFID is not the only technology that can be used to track the movement of people. When it comes to location tracking the Global Positioning System (GPS) is head of the class. GPS systems have been used by many employers (including school systems, trucking companies, and waste disposal companies) to track and monitor employees (Holtzman 181). Holtzman and the workers' union imply that companies like WABV-TV, a New York City television station, are violating employees' privacy by monitoring the location of their trucks with GPS. Some companies have also been using "geofencing" technologies to increase employee productivity. Geofencing works by

using a GPS receiver, which is usually placed in a cell phone, that senses when it has entered a geofenced location, like a bar or lounge, and reports to the company the time and duration of the stay. While this might benefit the company, there are privacy risks as well. If a receiver did not stop reporting at work hours, the company would know where you go all the time. A functioning alcoholic, who performs well at his job, could be fired because he spent too much time at bars during the evening and weekends. If an employee calls in sick, and then goes to a geofenced location, the company might reprimand or fire him, even though there could be a valid reason for him to be at that location. For instance, if a company geofences a porn shop and an employee that is out sick visits the porn shop, the employer might think that the employee was not really sick. However, is it the employer's job to determine how sick someone has to be to buy pornography? What if there was a pharmacy next to a geofenced location? The employee might be flagged as visiting a gentleman's club instead of the pharmacy!

Beyond tracking people physically, some websites track users on the Internet. A cookie is a file stored on a user's computer that records information about the web pages that they visit. By using cookies a company can track how often someone visits their website, or other websites that use the same cookies. Another common technique to track users is for a website to allow a partner or advertiser to place an extremely small image on all the pages. When the browser is loading the web page, it contacts the third-party web server that the picture is stored on. This server is configured to save the IP address and browser information of the user. This is also how spammers and mass emailers record information about who is reading their emails. If an advertiser can connect you to an IP address, they could use this information to do targeted advertising based on the web sites that you visit. While targeted advertisements might not cause any harm, it might startle you to receive an offer for airplane tickets to Morocco after viewing a book review

on a travel guide to Morocco! With proper networking and information sharing between companies it might even get worse. Imagine a pharmacist offering a man a free trial of Viagra because the pharmacy computer had received information that you had visited a website with information about Erectile Dysfunction only an hour ago.

Suggestions

The danger to privacy from household items is easily controlled. Simply do not buy appliances that send information about you to other places. In general, it is a good idea to always turn off features of software or devices that report back to a company.

The prevalence of RFID is large and growing. It is expected that 1.7 billion RFID tags will be sold in 2007 and there is projected market growth of over 500% over the next 10 years ("RFID tag sales expected to reach 1.7 billion in 2007"). Products like VeriChip, which are implanted into humans, are demeaning and dehumanizing. While I do not think that the government should control the use of RFID tags, I do think that companies should consider the privacy implications before forging ahead. Employees that work for companies that are considering using implanted devices need to voice their opinions. Sons and daughters of elderly parents need to talk to health care providers about their use of monitoring tools. One thing that is important is that the companies providing the RDIF tags for these purposes need to start telling their customers the truth. VeriChip claims that the chips are not hackable or clonable, but they are. The hospital customers, who were considering having an implant put in their arms so that hospitals could identify them if they were ever brought in incapacitated, should know that anyone with an RFID reader could track their comings and goings from an area.

Employers also need to realize that, as with any solution, there are faults to employee monitoring technologies. If a traveling salesman spent a day in a geofenced bar, he might have been meeting with customers. The ability of employers to know what

their employees are doing while they are getting paid is important, but should not be done lightly. If a company plans on tracking or monitoring employees they need to inform the employees about how and when they will be using the technology. Furthermore, employers need to remember that these solutions might have faults, like the salesman in a bar, or the sick person at the pharmacy.

For online privacy there are a number of steps you can take:

1. Disable cookies in your Internet browser.
2. Disable the loading of third-party content from web sites.
3. Turn off Javascript in your web browser.
4. Use a plug-in, like Tor for Firefox from the Electronic Frontier Foundation, which uses proxy-like technology to anonymize browsing.
5. User a proxy server if you have access to one.

In the end, the best way to protect privacy is for companies to realize the consequences of their actions. If a software company took as much time thinking about protecting their users privacy as they did on how to collect more information about their customers we would see a big change in the way software works. Employers, and care takers need to realize that the people underneath them are exactly that, people! They need to consider the privacy implications of certain technologies. If the people designing systems put themselves in the place of the people their system will track, they might do a better job maintaining a balance in the system. After all, the programmer that created the database that the credit bureaus use probably has a credit card and mortgage just like everyone else. People that run nursing homes and are considering using RFID implants to monitor their clients need to consider the humility of their clients. Would hospital and nursing home administrators want to be RFID tagged around their homes? My guess is not. Governments should not use this technology to monitor anyone. The government has no right to put things in our body that transmits information about us constantly.

Overall, the best way to make sure that all these things happen is to stay informed and be proactive. Voice concerns about the use of these technologies to your local, state and federal government. Stand up to your employer if they tell you that you need an implant to have access to a secure area. Ask them to give you an ID card to wear that has an RFID chip in it instead. Furthermore, do not ignore the loss of privacy for the minority. Just because prisoners are criminals does necessarily not mean they should lose their right to privacy.

Conclusion

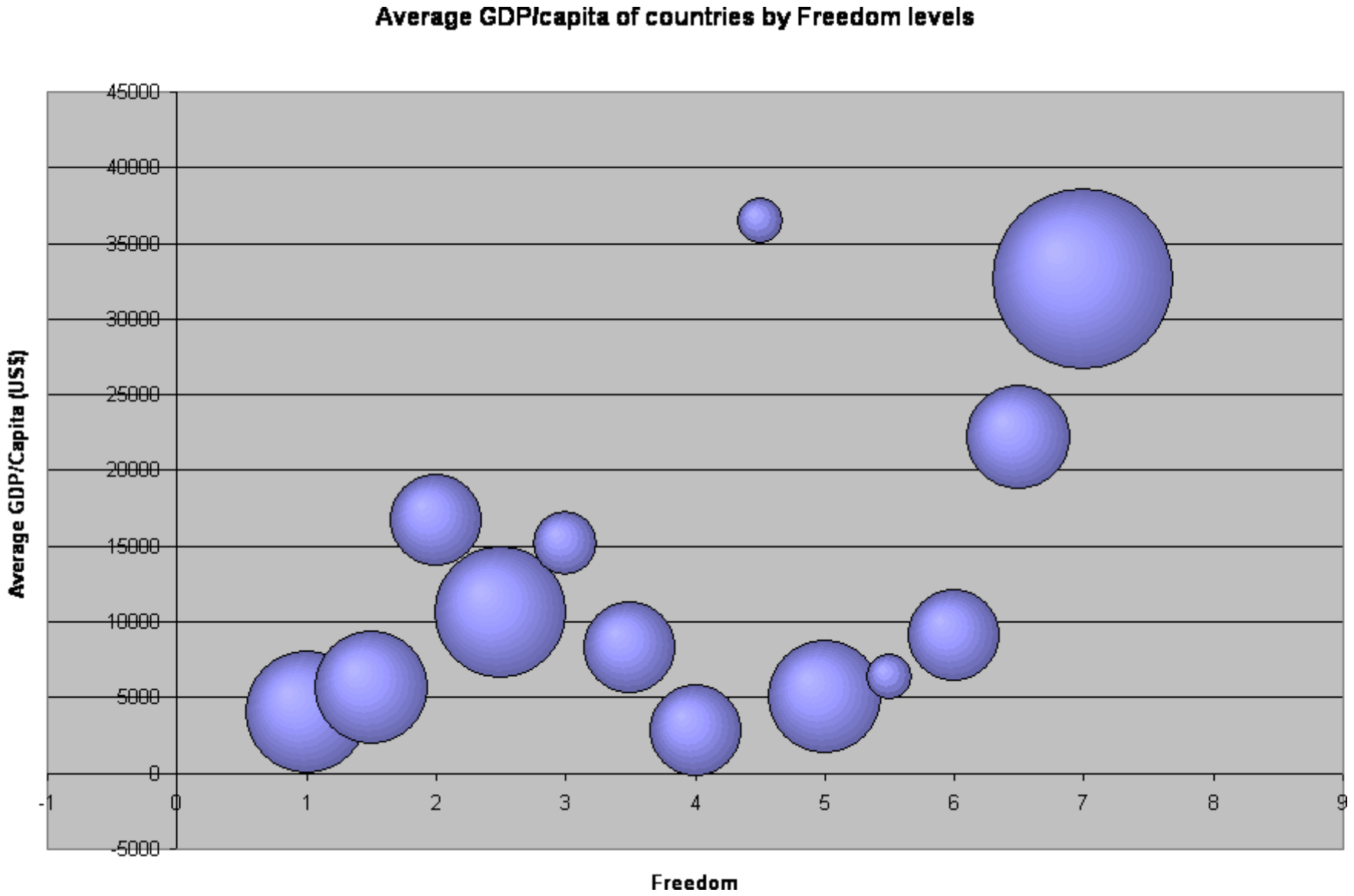
The modern world is not without evil. Numerous groups work and plot to kill or harm us constantly. Whether it is from terrorists training in a far away country; a rapist across town; or an online criminal sending phishing emails from the behind the safety of a proxy server, the dangers of our world are real. Governments are formed for the purpose of protecting the security of citizens ("Michael Graham Podcast, Guest: Rudy Giuliani, wk 4/16/07"). A balance needs to be struck between complete privacy, where the government has little ability to protect citizens against some threats, and total governmental control, where the freedom of the people is compromised.

While it is important that the government take actions to limit its own powers, it is also important that individuals take responsibility for their own privacy. By staying informed and helping to inform others, individuals can raise the awareness of privacy intrusions. Public attention is often a good deterrent to companies and governments that are invading peoples' privacy (29). If your employer requires you to be subjected to a privacy violation, fight back. Talk to your boss or human resources to find an alternative. Read privacy policies to help protect yourself from profiling.

Spend time to learn about new technologies that are coming out and think about their possible implications to privacy. As I have shown, technology has the power to eradicate privacy or to provide more privacy than ever before. Those concerned about their privacy can harness this power to whatever extent they want. The important thing is that people take individual responsibility, and that the government empower people to take this responsibility.

Appendix A

On the following page is a graph compiled from information from the Freedom House and the CIA World Fact Book. The Freedom House is an organization that rates the political rights and civil liberties. Freedom House gives a score from 1 to 7 in categories for every country, where 1 is free and 7 is not free. The graph has been modified so that a 7 represents free and 1 represents not free. The number on the graph is the average of the political rights and civil liberties from the Freedom House subtracted from 7. The more freedom a country's citizens have, the farther right they will appear on the graph. Likewise, the richer countries will be higher than the poor countries. The center of the circles are situated on the average GDP/Capita of all the countries that fall at a certain level of freedom. The size of the circles is proportional to the number of countries making up the average. The larger circles represent more countries, and therefore a more accurate measure of the wealth of countries at that level of freedom than small circles.


Average GDP/capita of countries by Freedom levels
Average GDP/Capita (US$)
45000
40000
35000
30000
25000
20000
15000
10000
5000
0
-5000
-1
0
1
2
3
4
5
6
7
8
9
Freedom

Appendix B

This is a copy of a phishing email I received. This was sent to me by someone probably trying to get my credit card information. The links that appear to point to a bank's website actually take you to a web server set up by the criminals which is made to look like the website of the bank.

Dear Capital One Bank, Capital One, F.S.B., Member,

Because of unusual number of invalid login attempts on your account, we had to believe that, their might be
some security problem on you account. So we have decided to put an extra verification process to ensure your identity
and your account security. Please click the link bellow:

https://service.capitalone.com/oas/login.do?objectclicked=LoginSplashID=?COB495886838

It is all about your security. Thank you. and visit the customer service section.

Capital One ID: COB495886838

Bibliography

Graham, Paul. *Hackers & Painters: Big Ideas From the Computer Age*. O'Reilly Media. Sebastopol, CA. 2004.

The Freedom House. Accessed December 2006. <www.freedomhouse.org>

Privacy.org. Accessed December 2006. <www.privacy.org/pi/issues/cctv/>

"Privacy police caution Big Brother", *New Scientist*, April 12, 1997, Pg. 44

"Crime rate soars as criminals walk free", *The Guardian*, May 28, 2006, Pg. 1

"'Spare No Resource'; Terrorist profiling is the most efficient, and effective, method of anti-terror policing.", *The Daily Standard*, October 16, 2005

"Profiles in Cowardice: How to deal with the terrorist threat-and how not to", *National Review*, January 28, 2002

"High Profile; What American airport security can learn from Israel's behavioral profiling system", *The Daily Standard*, September 1, 2006

Violent Victimization and Race, Bueau of Justice Statistics Special Report: 1993-98, <http://www.ojp.usdoj.gov/bjs/pub/pdf/vvr98.pdf>

Holtzman, David. *Privacy Lost: How Technology is Endangering Your Privacy*. Jossey-Bass, San Fransisco, MA. 2006.

Garfinkel, Simson. *Database Nation: The Death of Privacy in the 21st Century*. O'Reilly Media. Sebastopol, CA. 2001.

"Agents find scanner/eavesdropper disguised as a cellular phone", *Mobil Phone News*, January 8, 1996 <http://findarticles.com/p/articles/mi_m3457/is_n2_v14/ai_17926575>

"Privacy Advocates Blast Galvin: Critics want private data off state Web site", *Worcester Telegram & Gazette News*. April 6, 2007.

Tom Berson. *Skype Security Evaluation*. <http://www.skype.com/security/files/2005-031%20security%20evaluation.pdf>

Robert Smith and Eric Siegel. *War Stories: Accounts of Persons Victimized by Invasions of Privacy*. *Privacy Journal*, Providence, RI, 28577

Personal interview. *Brennan, Matthew*, Blockbuster Video, Assistant Store Manager. April 8, 2007.

"FTC finds identity theft remains consumers' top complaint", *Cardline,* February 9, 2007

"TJX reports on identity theft", *Women's Wear Daily*, March 30, 2007

"A Matter of Responsibility", *Cards and Payments*, April 2007

Nullsoft. *Winamp Privacy Policy.* <http://www.winamp.com/legal/disclaimer.php>

Shaws. *Reward Card Privacy Policy.* <http://www.shaws.com/footer/Rewards_Card_Privacy_Policy/index.html>

Facebook. *Privacy Policy*. <http://www.facebook.com/policy.php>

"Radio Waves", *Computing*, March 8, 2007

VeriChip Corportation. *Veriguard Access Control Pamphlet* <http://www.verichipcorp.com/files/VeriGuard_AccessControl(May06).pdf>

"RFID tag sales expected to reach 1.7 billion in 2007", *Mobile Radio Technology*, April 1, 2007.

Johnson, Daniel. "Evil Emperors (The Dictators by Richard Overy)(Book Review)". *Commentary* (Oct 2004). American Jewish Committee.

The Italian Job, F. Gary Gray. Paramount Pictures, May, 2003.

Enemy of the State, Tony Scott. Don Simpson/Jerry Bruckheimer Films, November, 1998.

Lafferty, Michael B. "Listening in on Block Talk", *Columbus Dispatch.* May 13, 1993

Sowyrda, Kevin John. "Boston and Beyond", *South End News.* April 5, 2007.

Jennifer Leo. "High roller Las Vegas suites", *Forbes Traveler.* <http://www.msnbc.msn.com/id/15332485/>

"Tattoos", *Jewish Virtual Library.* <http://www.jewishvirtuallibrary.org/jsource/Holocaust/Tattoos.html>

Graham, Michael. "Michael Graham Podcast, Guest: Rudy Guiliani, wk 4/16/07", April 11, 2007. <www.969fmtalk.com>