Ashley Jankowski
December 7, 2005

Convenience and Safety at a Price

"On the Internet, nobody knows you're a dog."

- "The state of computer security in the USA is a mess" (Loch, 1992).

SUMMARY:

This paper examines the issues facing online security and the overall convenience gained from technological advancements. In addition, I address the following questions: how convenient is convenient? How safe is safe? Where is the line between protection and violation of human rights?

This paper addresses these issues in order to create a better understanding of the price we pay for safety and convenience. Topics I will be covering will be surveillance, hackers, "big brother", spyware, and the illusion of protection.

PERTINENT ISSUES:

It seems that with new advancements everyday, people are more willing to embrace convenience without first considering the dangers that it may bring. For example, for many people, protection against terrorism is a good idea, but when does that protection turn into a violation? As Massachusetts Governor Mitt Romney suggested, if cameras are set up in mosques, or set up to track foreign students, the threat of terrorist attacks can be monitored (Helman 2005). The question now becomes, is this protection for United States citizens or a violation to those who pray regularly in mosques and are not planning terrorist actions?

Computer scientists from the University of California at Berkeley have found a way to crack a computer user's passwords by listening to the sounds of the keystrokes (Bray 2005). This technology was created by a professor and a student who originally were working on recognizing human speech (Bray 2005). This is a perfect example of how technological advancements start off small and seemingly harmless, and then turn into something potentially harmful that could threaten privacy among everyday computer users.

People are becoming more aware of the problem of security but they are not doing everything in their power to insure safety. A quote from the article, "Threats to Information Systems: Today's Reality, Yesterday's Understanding" reveals an interesting fact that people "seemed well aware of the threats but viewed their risk to be moderately low" (Loch, 1992, p185). What does this mean for big businesses? Computer users are not taking the proper steps to insure their information systems are protected. Businesses understand that there exists threats, but they feel that they will not be affected. This can lead to all kinds of problems involving security and protecting private information. Big businesses are underestimating the amount of system risk and they are unaware of the actions that they can implement to reduce that risk (Straub, 1998, p441). One factor that increases security risk is the presence of hackers.

SAFETY:

Hackers[1] are becoming a much bigger problem in regards to keeping computer systems safe. As technology grows more advanced, so do the capabilities of hackers. Businesses are being targeted through disguised emails and links that seem to be coming from trusted figures within a company or even in the government (Thomas 12). From the article "Enterprise; Business and Civil Servants Put on Security Alert," Roger Cummings director of the NISCC, the National Infrastructure Security Co-ordination Center, comments on the new wave of computer hackers and the destruction that they leave behind: "When you start to measure these attacks, it is clear they come from more than a couple of teenagers, and it's not about stealing money from firms. They are aimed at information-gathering, and the characteristics show that they are extremely well-organized and structured" (Thomas 2005, p 12).

CASE STUDIES:

The following case studies outline three major ways in which technology can be used to invade privacy and commit crimes. They include a teenage hacker who hacked into a celebrity's cell phone in order to steal phone numbers of other celebrities, a spam scam that used bogus emails in order to steal information from big businesses, and spyware, which was supposed to be protecting computers and the information stored in it, but ended up causing annoyances and vulnerability to the computer user.

[1] Hackers: people proficient in computers and skilled in computer programming, administration and security with legitimate goals. Popular media and the general population use the word, hacker, to mean a black hat hacker, that is, a network security hacker who partakes in illegal activity or lacks in ethics. www.wikipedia.com

Case 1: Cell Phone Invasion

Hackers are not only targeting big businesses but also ordinary people and even celebrities. Recently a Massachusetts teenager, who had hacked into Paris Hilton's cell phone account was sentenced to 11 months in prison (AP B7). He was charged for hacking into Internet and telephone service providers, theft of personal information, and posting it on the web (AP B7). This is an example of how there is no age limitation to those committing these crimes; and it also shows that everyone is at risk.

Case 2: Spam Disguised as Email

A lawsuit was filed after an email scam was discovered in Redmond, Washington. An Iowa man was charged on 75 counts of wire fraud. It took almost 2 years for this case to finally be closed. The man had used email scams, which appeared to be coming from legitimate business yet were full of spam. In Florida, the sentence for identity fraud is a maximum of 30 years. This case opened the eyes and ears of many big businesses, and it demonstrated how difficult it is to find these criminals and persecute them. Even though some criminals are put into prison, the threat of identity fraud still exists. There will always be computer hackers and spam e-mails. According to Jim Prendergrast of *Americans for Technology Leadership*, "Cybercrime is here to stay. It's a reality we have to face" (Gussow 2005, p 1D).

Case 3: Spyware and Pop-ups: Necessary or Annoying?

Last year AOL Inc was included in a case against Adverstising.com for installing spyware on people's computers with the premise that the spyware, called SPYBLAST, was needed for protection of the computer and the information stored in it (Bishop 2004, p 1D). The FTC had been participating in a campaign trying to prevent the use of programs that created pop-ups or allow information to be stolen without the knowledge of the computer user. According to the definition of spyware in this article, “spyware and adware are only illegal when they're installed on computers without adequate notice or when used to steal information, but they are often seen as huge annoyances and can be costly” (Bishop 2004 1D). After the case against Advertising.com, the company stopped using the SPYBLAST software.

SPYWARE:

Another issue that is causing problems with computer security is Spyware. Spyware is software that performs behaviors such as advertising, collecting personal information usually without obtaining proper consent. Spyware sometimes appears as pop-ups, in the computer toolbar, or in a browser. Spyware is a threat to computer users because it can keep track of personal information that can later be used against someone. The ads that pop-up on computers sometimes directly correspond to companies which track a computer user’s online activity. According to the article “Spyware was Inevitable” by Steve Gibson (2005), “Spyware is the PC user’s latest and biggest problem; a larger source of worry, concern, and frustration than anything PC users have faced before, and potentially more damaging than the worst computer viruses. (Gibson 2005, p38)” This quote expresses that immediate attention needed to fix a problem such as spyware because of its devastating consequences. Spyware is being used to obtain private information of computer users which can lead to significant threats (Thompson, 2005, p41). Even though spyware has grave consequences, there are possible solutions to fix these problems. According to the article, “Why Spyware Poses Multiple Threats to Security” by Roger Thompson, the first line of defense is through education. (Thompson, 2005, p43)

EDUCATIONAL IMPORTANCE:

I want to educate others on this topic, because if people are not educated, that is when abuse occurs. The word safety is thrown around a lot when discussing why cameras are being placed in cars, churches, mosques, hospitals, and streetlights. As humans, we have basic rights, and the question arises, do these cameras infringe upon these basic rights? Perhaps some feel the cameras do not infringe upon our rights because they have nothing to hide, so who cares if someone is watching you drive through a yellow light or pray in a church, synagogue, or mosque. But what happens when it goes farther than that? What happens when cameras appear in your homes, in your workplaces, at your desk, in bathrooms? Now are these cameras an infringement of your rights?

Now is the time when people need to be educated, so when future more extreme actions take place, people will have a better understanding of the situations that may occur and they will be educated enough to do something about it.

MY OPINION:

The world today is very frightening. What scares me most is not what is happening now, but rather what the future will bring.

When did technology become so scary? At first glance security cameras and computer profiling seem innocent and for the greater good, but when will that end? I am afraid that when I am an adult, Orwell's term "Big Brother" will be a frequently used phrase in everyday life. I don't want to be watched 24/7. I don't want someone to know what I buy and what kind of movies I like; it is just too creepy. Also, what if this information gets into the wrong hands? People can potentially begin stealing identities much easier than it is now. Instead of Hackers that hack into your computer, there will be people that actually take over your life, for example identity fraud[2]. The more educated I become on this topic, the scarier it seems, but that can be a good thing. Being scared of technology is not the same as being scared of the boogey man, but it's the kind of scared that makes you aware and cautious, which is what I feel everyone should be. My motto is, don't take things at face value; question everything. As long as you understand what is going on, you can prepare and insure that you will not fall victim to the dangers that potentially await us in the future.

KEYWORDS:

Cookies: are not software of any sort—they are variables set by Web sites (including advertisers) which can be used to track Web-browsing activity, for instance to maintain a "shopping cart" for an online store or to maintain consistent user settings on a search engine.

[2] Identity Fraud:the deliberate assumption of another person's identity, usually to gain access to their finances or frame them for a crime. www.wikipedia.org

Cookies can only be accessed by the Web site that sets them. www.wikipedia.org

Cracker: A cracker is not the same as a hacker. A cracker compromises the security of a system without permission from an authorized party. They participate in illegal activity and they only modify software. www.wikipedia.com

Firewall: a piece of hardware and/or software which functions in a network environment to prevent some communications forbidden by the security policy. www.wikipedia.org

Hacker: people proficient in computers. In programming communities, the term refers to people skilled in computer programming, administration and security with legitimate goals. Popular media and the general population use the word *hacker* to mean a black hat hacker, that is, a network security hacker who partakes in illegal activity or lacks in ethics. Those inside some programming communities have taken to calling these criminals "crackers".

In computer programming, *hacker* means a programmer who *hacks* or reaches a goal by employing a series of modifications to exploit or extend existing code or resources.

In computer security, *hacker* translates to a person able to exploit a system or gain unauthorized access through skill and tactics. This usually refers to a black hat hacker.

In other technical fields, *hacker* is extended to mean a person who makes things work beyond perceived limits through their own technical skill, such as a hardware.

www.wikipedia.org

Homeland Security: domestic governmental actions justified by potential guerilla attacks or terrorism. www.wikipedia.org

Identity Fraud: deliberate assumption of another person's identity, usually to gain access to their finances or frame them for a crime. Less commonly, it is to enable illegal immigration, terrorism, espionage, or changing identity permanently. It may also be a means of blackmail, especially if medical privacy or political privacy has been breached. www.wikipedia.org

Spam: A collection of unsolicited bulk electronic message,. e.g. by email or newsgroups www.wiktionary.org

Spyware: a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. www.wikipedia.org

Surveillance: close monitoring of behavior, observation from a distance by means of electronic equipment or other technological means. www.wikipedia.org

System Risk: The likelihood that information systems are insufficiently protected against certain kinds of damage or loss. Risk can be managed or reduced when there is awareness of the full range of controls available and implement the most effective controls. (Straub 441)

Virus: a self-replicating program that spreads by inserting copies of itself into other executable code or documents made by crackers (see above for definition of crackers) www.wikipedia.org

Wiretap: monitoring of telephone conversations by a third party, often by covert means. www.wikipedia.org

QUOTES:

Massachusetts Governor Mitt Romney addressing the Heritage Foundation in Washington: The Boston Globe: September 15, 2005

> "How about people who are in settings- mosques, for instance – that may be teaching doctrines of hate and terror are we monitoring that? Are we wiretapping? Are we following what's going on?"

Ali Noorani, executive director of the Massachusetts Immigration and Refugee Advocacy Coalition: The Boston Globe: September 15, 2005

> "Blanket eavesdropping and blanket profiling only erodes the safety and security of our country. People who really know what national security is and what intelligence is realize that we need to build trust between law enforcement and immigrant communities."

Julie Teer, Governor Mitt Romney spokeswoman responding to the criticism of Mitt Romney's comments: The Boston Globe: September 15, 2005

> “The governor believes we can strike a balance between
> what is necessary to protect our homeland while
> respecting individual freedom and liberty.”

Dr. David Himmelstein, associate professor of medicine at Harvard University : The Boston Globe: September 15, 2005

> “But computers don’t offer the panaceas that politicians
> hope for and computer firms are peddling.” (Talking
> about systems that contain electronic medical records and
> computerized drug prescriptions, and how the technology
> might be difficult to implement.)

Doug Tygar, Professor at the University of California at Berkeley addressing article author Hiawatha Bray: The Boston Globe: September 15, 2005

> “This means we can break into one of every 75 people’s
> accounts, on the first try.”
> (Talking about a new way to crack computer passwords
> by listening to the keystrokes)

Spencer F. Katt, from the article “What provides folks with the illusion of comfort and sercuirty” from eWeek: July 12, 2004

> “What provides folks with the illusion of comfort and
> security? Firewalls? Teddy bears? Locks and chains?”

Karen Loch, from the article “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding.” from MIS Quarterly: June 1992
According to a study given to multiple businesses

> “Our findings reveal ironies of computer security. Our
> respondents seemed well aware of the threats but
> viewed their risk to be moderately low.”

Tagline from 1995s movie <u>The Net:</u>

> Her driver’s license, her credit cards, her bank
> accounts, her identity, DELETED! (www.imbd.com)

*How pertinent is this tagline today? Is this something that only seemed like it could happen in the movies? 10 years later, how far have we come to prevent an incident like this?

RERFERENCES:

Associated Press. “Teen Sentenced in Hacking Case.” <u>Boston Globe</u> 15 Sep. 2005: B7.

Bishop, Trishia. “Spyware settlement announced.” The Baltimore Sun 12 Aug 2004: 1D.
www.lexisnexis.com

Bray, Hiawatha. “Careful or They’ll Hear Your Password.” Boston Globe 15 Sep. 2005: C1.

Gibson, Steve. “Spyware was Inevitable.” Communications of the ACM August 2005: Volume 48, Number 8, pg 37-39.

Gussow, David. “Webcrime defense: Use common sense.” St. Petersburg Times Sept 2005: 1D.
www.lexisnexis.com

Loch, Karen D, Housten C Carr, and Merrill E Warkentin. “Threats to Information Systems: Today’s Reality, Yesterday’s Understanding.” MIS Quarterly June1992: 173
www.jstor.org .

Helman, Scott. “Wiretap Mosques, Romney Suggests.” Boston Globe 15 Sep. 2005: A1.

Katt, Spencer F. “What Provides folks with the Illusion of Comfort and Security.” eWeek 12 July 2004: pg 70
http://web.lexis-nexis.com/universe/form/academic/s_guidednews.html .

Straub, Detmar W. “Coping with Security Risk: Security Planning Models for Management Decision Making.” MIS Quarterly Dec 1998: 441 www.jstor.org .

Thomas, Daniel. “Enterprise, Business, and Civil Servants Put on Security Alert.” Computing 23 June 2005: pg 12
http://web.lexis-nexis.com/universe/form/academic/s_guidednews.html .

Thompson, Roger. “Why Spyware Poses Multiple Threats to Security.” *Communications of the ACM* August 2005: Volume 48, Number 8, pg. 41-43.A

Trehan, Veena. “Savings Seen In Computer Health Records.” Boston Globe 15 Sep. 2005: A5..

www.imdb.com “The Internet Movie Database”

www.wikipedia.org “Wikipedia: The Free Encyclopedia”