

Ethics Topic – Internet Privacy

June 30, 2005

By

Rama Etekallapalli

Senior, Plastics Engineering Technology

Pittsburg State University

For

Dr. Christopher C Ibeh, Director

2005 PSU-CNCMM REU/RET

Professor, Plastics Engineering Technology

Pittsburg State University

Advisors

Dr. Christopher C Ibeh

Dr. Ivan Javni

June 30, 2005

Dr. Christopher C. Ibeh, Director
2005 PSU-CNCMM REU/RET
Professor, Plastics Engineering Technology
Pittsburg, KS 66762

Re: Ethics paper project on "Internet Privacy"

Dear Dr. Ibeh:

I am very pleased to inform you that I have successfully completed the above stated project and submitting you this report as a part of the 2005 PSU-CNCMM REU/RET program.

The main purpose of this report is to provide information about the privacy problems encountered in internet and how to safeguard the personal information.

I hope that this report will meet with your approval. If you have any questions, you can email me at erk151@yahoo.com or call me at 620-875-1154.

Sincerely,

Rama Etekallapalli
Senior, Plastics Engineering Technology.
Pittsburg State University

Encl: A formal report on Internet privacy

Table of Contents

- 1. Abstract..... 4**
- 2. Introduction..... 4**
- 3. Literature Review..... 5**
- 4. Privacy on the Internet..... 5**
- 5. Methodology..... 6**
- 6. Results and Discussion about Internet Privacy..... 6**
- 7. Conclusion..... 7**
- 8. Recommendations..... 7**
- 9. Acknowledgements..... 7**
- 10. References..... 8**

Ethics Topic – Internet Privacy

Rama Etekallapalli, Senior, Plastics Engineering Technology, Pittsburg State University

1. ABSTRACT

The ease and efficiency with which computers and computer networks can be used to gather, store, search, compare, retrieve and share personal information make computer technology especially threatening to anyone who wishes to keep various kinds of "sensitive" information (e.g., medical records) out of the public domain or out of the hands of those who are perceived as potential threats. During the past decade, commercialization and rapid growth of the internet; the rise of the world-wide-web; increasing "user-friendliness" and processing power of computers; and decreasing costs of computer technology have led to new privacy issues. In this era of computer "viruses" and international spying by "hackers" who are thousands of miles away, it is clear that computer security is a topic of concern. There are also problems with frauds and scam artists who elude law enforcement authorities through anonymous mailings and postings. Other users are concerned about the proliferation of information on the Internet. The right to privacy in Internet activity is a serious issue facing today's society.

2. Introduction

The Internet offers many benefits. Web sites provide a vast world of information, entertainment, and shopping at our fingertips. Electronic mail, instant messaging, and chat rooms enable us to communicate with friends, family, and strangers in ways we never dreamed of a decade ago. But the Internet also creates many threats to our personal privacy. Unless you know the "rules of the road," your online activity may lead to significant privacy problems. Today in western societies more people are employed collecting, handling and distributing information than in any other occupation. The question before us now is whether the kind of society being created is the one what we want. There are many unique challenges we face in this age of information. Information is the means through which the mind expands and

increases its capacity to achieve its goals, often as the result of an input from another mind. Thus, information forms the intellectual capital from which human beings craft their lives and secure dignity. However, the building of intellectual capital is vulnerable in many ways. For example, people's intellectual capital is impaired whenever they lose their personal information without being compensated for it, when they are precluded access to information which is of value to them, when they have revealed information they hold intimate, or when they find out that the information upon which their living depends is in error. The social contract among people in the information age must deal with these threats to human dignity.

3. Literature Review

[1] New and enhanced Microsoft technologies allow consumers and business to significantly reduce e-mail, guard against spyware and online fraud, and restrict how private data is used or shared. Microsoft is committed to helping customers understand the privacy resources and provide to help them protect the privacy of their information.

[2] Microsoft's top privacy executives discuss the combination of technologies, practices, and government and industry cooperation that drive the company's strategy for promoting customer privacy online.

[3] Internet becomes a communication tool and available to all. As the Internet permeates ever more domains of social and political, and even personal life, and as its technological capabilities expand, the problem of Internet ethics will become ever more central, perhaps even more so than in "ordinary" life. The potential for abuse grows with use, as well as with technological power.

4. Privacy on the Internet

Privacy is a critical element of a secure computing experience. The Internet is a great place to share genealogical information about your own or someone else's family, but be aware that this information could be used by identity thieves searching for personal data to hijack your credit. When it comes to revealing personal information, you are largely in control. You alone decide what to type into a form and what to keep to yourself. Internet users sometimes do not realize the amount of

privacy that is lost when accessing the online world. Email is stored in servers as it passes on its merry way and you have no idea where your words or information may end up. A good rule to remember is on the Internet nothing ever completely disappears and nothing can be completely controlled.

One particularly disturbing trend involves an increase in fraudulent Web sites or bulk e-mail solicitations. They contain links to Web sites that ask recipients to reveal sensitive information such as bank account, social security, or personal identification numbers. The look and feel of the e-mail or the fake site so closely mimics the Web sites of legitimate, reputable companies such as eBay, Citibank, or Microsoft® that they have successfully tricked many users into giving out sensitive personal information or infecting their own computers.

There is no fool-proof way to protect your children online - or anywhere else for that matter! As in the real world, there are precautions that families can take in the online world to reduce the chances of children encountering dangerous or unsuitable material. Help your child choose a screen name or e-mail address that does not reveal anything personal about the child -- age, sex, hobbies, what school they go to, where they live and like to play, etc. Keep any computers connected to the Internet out of kids' rooms, and put them in a central location, such as the family room. Talk with your child often about what they do online and who they talk to. Taking an interest in what your child or teen does online doesn't necessarily mean a lack of trust: just as you're interested in their "real world" friends.

Any reputable Web site will have a privacy policy or privacy statement that explains how and why the Web site collects your information, and how it plans to use it. Ideally it should be written in a clear, straightforward manner. Look for the Web site's privacy policy (or statement) at the bottom of its home page (if not every page). You may also find it within a site's "Terms & Conditions" or "Terms of Use" section.

5. Methodology

For this research paper, apart from computers no other machines and materials are used. Therefore, this was solely a research paper from previous articles and websites. The Google and ask search engine was very helpful in finding the necessary information for preparing this research paper.

6. Results and Discussion about Internet Privacy

Protection of individual privacy on-line is best achieved through cooperation between employers, service providers, software developers, governments, and information collectors. The burden of protection should fall on those collecting or using data, not on the multitude of individuals using the net to go about their daily activities.

There are so many simple ways to protect oneself from identity theft.

- Be defensive with personal information
- When online, only give the information required often marked with an asterisk (*) and no more

- Create strong passwords and keep them secret
- Improve the computers security from hackers, viruses and worms by using a firewall, installing antivirus software and updating it routinely, and keeping your Windows software up to date
- Never respond to emails that request personal information
- Don't enter the sensitive information into a public computers
- Don't save the login information when using public computers
- Don't take any downloads from strangers
- Visit websites by typing the web address (URL) – not by clicking a link in an email or pop-up window

Typical problems with privacy notices, policies, or practices on commercial websites include:

- privacy policy may be hard to find or difficult to read and understand
- it may not contain all the disclosures
- it may use vague and unspecific language ("we do not generally share information with third parties"; "we only share information with companies and parties that do business with us")
- it may not comprehensively list all of the types of information being collected
- it may fail to provide a contact address or procedures for dealing with complaints, corrections, or conflict resolution

- it may not state the site's commitment to data security
- it may not have clear access requirements or procedures for verifying a valid requester before granting access.

To do if someone steals the identity

- File a report with the local police department
- Immediately place a fraud alert on the credit reports with each of the three major U.S. credit bureaus
- Immediately close accounts accessed or opened fraudulently
- Immediately change the passwords on ALL online accounts
- File a complaint with the U.S. Federal Trade Commission (FTC)
- In the United States, report the fraud to Fraud.org, the National Fraud Information Center.
- Record and save everything you do to clear up the wrongdoing including copies of e-mail messages, written correspondence, and records of telephone calls

7. Conclusion

The problem of internet privacy gets more complex and more provocative every day as the reach of the Internet, its uses, and its technical capabilities increase exponentially. As computer technology rapidly advances -- creating ever new possibilities for compiling, storing, accessing and analyzing information -- philosophical debates about the meaning of "privacy" will

likely continue. As a result of digital technology, private space will shrink and public space will increase. Therefore, be defensive with personal information.

8. Recommendations

Internet Explorer 6 helps in managing security and privacy preferences while on the Internet with tools that help you safeguard your family's browsing experience. Manage cookies to help control the personal information that Web sites collect about you, set different levels of security for different sites on the Web with Security Zones, and use Content Advisor to help block access to objectionable content. These tools support the Platform for Privacy Preferences (P3P), a technology under development by the World Wide Web Consortium (W3C).

9. Acknowledgement

- ❖ Dr. Christopher C Ibeh, Director, CNCMM
- ❖ Dr. Ivan Javni, Research Scientist, KPRC
- ❖ Dr. Hensley Oliver D, Professor, Special services & leadership studies
- ❖ Dr. Donovan Marjorie E, Associate Professor, Social sciences

10. References

1. *Privacy Resources of Microsoft Trustworthy Computing* – www.microsoft.com
2. *Microsoft's steps to enhancing online privacy* – www.microsoft.com
3. *Ethics and the Internet* – Cezar M. Ornatowski, Rhetoric & Writing Studies, SDSU, *July 2001*
4. Privacy foundation – www.privacyfoundation.org
5. Privacy rights clearing house – www.privacyrights.org
6. Privacy activism – www.privacyactivism.org
7. Center for democracy and technology – www.cdt.org
8. Computer professionals for social responsibility – www.cpsr.org
9. Electronic frontier foundation – www.eff.org
10. Electronic privacy information center – www.epic.org
11. www.microsoft.com
12. www.msn.com
13. www.google.com
14. www.ask.com
15. www.wikipedia.org