Free Web-Based Services May Cost More Than Nothing:

What You Might Not Know, They Just Might Know About You

Robert B. Fried, BS, MS

The Twentieth Century will inevitably bring with it an enormous surge of technological innovations. Today, as the world's technology sector continues to expand, more and more people are compelled to become involved. The Internet, specifically, the World Wide Web, provides a medium in which the average individual can experiment with the benefits associated with the emerging computerized society we are in the midst of developing.

Within the last five years, both the growth and usage of the Internet has expanded at an enormous rate. It can be safe to assume that the Internet and the terms associated with it are becoming a part of the vernacular. Unless you have been living under a rock or have been the unfortunate owner of a "dinosaur," the term used to describe an old and antiquated personal computer, you have probably come into some contact with the Internet. Whether you've been exposed to it or not is a totally different issue.

As public usage of the Internet continues to expand, many new Internet based services are in need of development and at a price the average user can afford. Recently, there have been numerous amounts of Internet-related companies providing such services at a price the average user could and would not refuse: for free.

The truth is that many new "free" Internet-based or related services are becoming and will become more widely available. Some may view such services as a means of making life in this emerging Technological Era a little more convenient. Many of the "free"

services available today seem to do just that. Services which amount to such things as free electronic mail addresses, retrieval of music from musical recording artists, Internet based phone calls, newsgroups, Instant Messenger™ services, electronic greeting cards for any occasion, web based anti-virus programs, virtual hard disk space through storage on a server provided by a commercial website, and even as far as free Internet access through a direct dial-up connection using a conventional modem are all quite appealing.

This may all seem phenomenal to the average individual. However, to the experienced and rather savvy Internet user, these "free" services are somewhat sketchy. The experienced computer user would know that the Internet was originally designed to mainly cater to government agencies and academic institutions. Now with the advent of graphical browsers, the Internet has become easier to navigate and has rapidly developed into a commercial enterprise.[1]

I am a true believer of the coined phrase, "there is no such thing as a free lunch." The intent of this paper is to examine some of the many emerging "free" Internet based services. My primary focus is to specifically evaluate and determine the true cost of such services to their users. Furthermore, I am interested in investigating how the companies providing such services ultimately profit. Moreover, I am interested to learn whether or not such companies have hidden agendas that their users don't exactly know about.

In order to begin to examine the true nature of Internet related services, it is important to understand why they have rapidly gained an enormous amount of popularity. Rebecca Winters a columnist for Time Digital gives some insight as to why "free" Internet access has become popular. Winters states, "the chief lure of these offerings:

---

[1] Kenworthy, Karen. (1998, September). Cookie Crumbs. Windows Magazine [Online]. Available: http://www.winmag.com/Karen. [2000, July 26].

annual savings of up to $300, compared with that you would pay for America Online, Earthlink or other fee-based services. And they come with a solid array of baseline services: unlimited surfing time, e-mail, personalized start pages, calendars, chat services, shopping, news, sports and stock links. That should be enough stuff to get even your stingy Aunt Mae online to see your new baby photos."[2] In his article entitled "Cheap Shots," Matthew Schwarz, a columnist for Computerworld adds that in a study conducted in November 1999, "Jupiter Communications Inc. in New York found that 23% of customers said they would be interested in free online access in return for viewing advertising and letting their buying patterns be tracked. But 16% said they would rather pay $5 per month to their Internet service provider in exchange for not viewing advertising."[3] It seems like quite the bargain. Most everyone would want to save money wherever they could in this day and age. The Internet is just another expense and if it's offered for free by some, why not grab it?

The truth is many people have signed up to receive "free" Internet service. Winters, in her column of Time Digital entitled, "Free Economy" provides some astounding statistics. In her research on the subject, she learned that, "according to Jupiter Communications, free-access providers are used by 7% to 8% of US households connected to the Net." "Jupiter expects that number to jump to 13% by 2003." Millions of people have signing onto services such as NetZero, Juno, Excite@Home, BlueLight and the number continues to grow each day.[4] How can these companies handle such enormous growth? Software needs to be written to allow users to allow users to sign on

---

[2] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].
[3] Schwartz, Matthew. (2000, 03 Jul). Cheap Shots. *Computerworld,* 60-61.

and have the programs needed to run such a service resident on their computers hard disk drive, telephone numbers need to be bought and maintained so that users can access the service, severs have to be purchased so that direct access to the Internet can be provided, facilities need to be established to house such computer hardware and staff need to be hired to handle the operations, customer service, and technical support that will inevitably be necessary when dealing with computers and the public. There has got to be a catch somewhere. It just doesn't make sense that these services are deemed totally "free".

So what do these companies giving "free" Internet access gain by providing such a service? As Rebecca Winters' research points out, these companies receive a whole lot of information and marketing strategies. Essentially, "when you sign up, you typically fill out forms that give the provider a wealth of information about you and your spending habits. Armed with your answers, the service providers match you up with the appropriate ads."[5] Is this where these companies make their profit? With these "free" online services come banners and advertisements appearing across the screen, many of which cannot be minimized, closed, or moved. If no sort of advertisement is floating across the user's screen, then there is usually another tactic that is implemented.

Information can also be collected about the user through monitoring the web sites the user connects to. DoubleClick is one such company that monitors a user's traffic patterns online. Essentially, "DoubleClick is able to follow users online because it operates an ad network that serves millions of ads across the Internet. Every ad includes a small

---

[4] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].
[5] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].

"cookie" that tags the computer and Internet connection."[6] Through the monitoring of a user's behavior on the Internet one can learn about their interests and desires. Emails and advertisements can then be sent to that particular user via email or postal mail that had been provided at the time when the "free" account was initially established. These methods of retrieving information about a particular user are quite clever. However, are companies providing such services and displaying these personalized ads, in a sense invading someone's right to privacy?

In order to evaluate whether an individual's privacy is being invaded through the usage of such services, it is essential to examine how information about a particular user is obtained while online. One such way, which has become a common practice as noted previously with DoubleClick, is to place "cookies" onto a user's computer. One may confuse these with the cookies bought at the local bakery. However, as we have begun to realize, computer jargon does not always refer to the obvious.

A cookie is essentially, "a small piece of information (comprising no mother than 255 characters and 4k of disk space), written to the hard drive of an Internet user when he or she visits a website that offers cookies. Cookies can contain a variety of information, including the name of the website that issued them, where on the site the user visited, passwords, and even user names and credit card numbers that have been supplied via forms. Cookies are supposedly only retrievable by the site which issued them, and link the information gathered to a unique ID number assigned to the cookie so that information is available from one session to another."[7] So it is apparent that cookies can

---

[6] Wice, Nathaniel. (2000, February 02). Advocates Declare Privacy War Against DoubleClick. *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,38568,00.html. [2000, July 26].
[7] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Introduction. Available: http://www.cookiescentral.com/ccstory/index.htm [2000, July 26].

be somewhat beneficial to creators or owners of web sites. However, cookies are being used more and more by Internet advertising agencies such as DoubleClick and their increasing usage is worrying proponents of electronic privacy.

Web cookies have been around since 1994, when Lou Montulli of Netscape initially designed them for use with the Netscape Navigator 1.0 web browser.[8] They were initially designed to enhance the online shopping experience. Now new variations of cookies have developed which go beyond what they initially intended to do. One such type of cookie is known as the stealth cookie. Essentially, "stealth cookies are hidden by third parties on web pages (you visit a page and get tagged by cookies from sites you never visited) or security holes (Internet Explorer has one) that will allow third parties to see your cookies."[9] Furthermore, now, "with the proper cookie scheme web site developers can tell which demographic group goes where, and how many people are interested in a particular product or service." If designed correctly, a web cookie can even determine the popularity of a certain ad or other marketing device appearing on a web site.[10] It's no wonder why so many businesses are using cookies these days. The question that concerns many is how are the users of such services protected from unwanted cookies? Does the information that however, is collected, get misused? Furthermore, do the customers read policy statements and recognize some of the associated drawbacks prior to signing on to such services?

---

[8] Whalen, David. The Official Cookie FAQ: version 2.53. Available: http://www.cookiecentral.com/faq.. [2000, July 27].
[9] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].
[10] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Introduction. Available: http://www.cookiescentral.com/ccstory/index.htm [2000, July 26].

Many new software packages and prevention techniques are now widely available to help users of such services from receiving unwanted and often hidden cookies. However, many companies who design cookies often do not provide any assistance in regards of deleting them from a system. Marc Slayton, a columnist for Webmonkey suggests users take the following actions to try and avoid their computer from essentially becoming a cookie jar. He suggests that users learn about their web browser options to see if there are any options in regards to the acceptance or denial of cookies onto a system's hard disk drive. Furthermore, Slayton suggests that user's designate a specific region of their hard drive to store cookies as unreadable. Moreover, Slayton recommends that users utilize sites that have an anonymous account when one logs into a password-protected section of the web site.[11]

The issue over misuse of information obtained from cookies was and continually is a big concern of the Internet Engineering Task Force. The I.E.T.F. set forth guidelines they felt reasonable in regards to web sites issuing web cookies to their users. In their proposal RFC 2109, the I.E.T.F. proposed controls on how cookies can be set and transferred to a user's hard disk drive. The proposal was not designed to totally eliminate web cookies; it attempts to fix some of the problems (privacy and such) associated with their usage. Since, many web sites do not provide much assistance in the area of deleting web cookies, RFC 2109 proposed ways in which companies designing web-browsing software can implement an automatic cookie rejection shortcut within the browser itself. Many Web designers are not too fond of having to redesign their software. The fact, that software companies feel this way is music to the heart of many web-based advertising

[11] Slayton, Marc. (1996, November). It Ain't All Cookies and Cream. *Webmonkey* [Online]. Available: http://www.media-awareness.ca/eng/issues/priv/resource/cookies.htm. [2000, July 27].

agencies. However, concerns coming from users of the Internet continue to grow and it seems as though they are often left in the dark with such issues.[12]

Being that DoubleClick has been deemed the Internet's largest advertising agency, concern regarding the usage of the data they collect comes into question. William Dowell, a columnist for Time Digital gives some insight as to how these companies use the data they collect in his column "The Cookie Jar (a.k.a. Your Computer)". He states, "Most companies couldn't care less about the data they have on specific individuals. It's the topography of contemporary culture that they 're really after." He suggests, "the reason for compiling massive databases is "data mining," a process that involves unleashing supercomputers on vast quantities of data to spot customer trends that might otherwise go unnoticed."[13]

On the surface, companies like DoubleClick do not seem to be misusing the information they collect. However, the more they collect, the more desirable their data is to other companies who are looking to benefit from what the trends in the collected data may show. Many companies have recently sought to merge with DoubleClick. As a result, DoubleClick has been in the hot seat as people try to figure out why they are so valuable. In November 1999, DoubleClick had announced that it would be acquiring Abacus Direct. This immediately concerned advocates of Internet privacy such as the I.E.T.F. "Abacus Direct is a company which profiles 88 million households that use snail mail to buy merchandise from catalogs. The merger promised a wholesale linkup of Abacus's address and phone numbers with the ID numbers on Internet cookies – once

---

[12] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Privacy Issues. Available: http://www.cookiescentral.com/ccstory/cc4.htm [2000, July 26].
[13] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

you've been tagged with a cookie a lot of other people are going to be aware of who you are, and where you've been."[14] If this merger doesn't infringe on an individual's right to privacy I don't know what does.

For most people, having a little bit of their privacy exposed does not bother them. For the amount of money they save as compared to fee-based Internet access providers and services; they feel it is worthwhile. So, you have to give them your name, a phone number and maybe even a street address; and subject yourself to an overwhelming amount of advertisements. Most people feel that this way of connecting to the Internet is better than dishing out $300 for a year of connection with a fee-based service. Without advertisers investing in this medium, there would most likely be no such thing as a "free" Internet service provider.[15] Furthermore if the users to such services continue to sign on, these companies will continue to expand their influence on the way people surf the Internet.

Personal Privacy may be one of the sacrifices of getting involved with "free" Internet services; however, there are several other tradeoffs. Among the other tradeoffs of using such services are the risks associated with their security and integrity. Furthermore, the users of such services may have to deal with the glitches that may occur while utilizing the service.

The question then becomes, how safe is someone using a "free" Internet based service? The truth of the matter is that no matter what you do on the Internet you are never safe. Not only can your activities be traced while surfing the net, your exact

---

[14] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].
[15] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

geographic location can be determined as well. Privacy.net, a consumer information organization reveals several other ways a user can be traced while using the Internet. A geographic location or the location of a computer that exists on a network can be determined by obtaining a user's Internet Protocol address. It is the IP address (a series of specific and individualized numbers), which allows a user to connect onto the Internet. IP addresses are found in email messages, cookies, or even in software that allows for others to access your computer while it is on the Internet.[16]

Many people engaged in certain activities on the Internet try very hard to make their IP address invisible to other users. One such "free" Internet service that exposes the IP addresses of its users to hackers is Napster. Napster, a software program run via the Internet has become a medium in which a community of individuals interested in music, swap song files amongst themselves. This act violates copyright laws and many people in the music industry are willing to prosecute those engaging in such illegal acts. Having the IP addresses of such individuals brings the music industry one step closer to taking down Napster. So as anonymous as the users of Napster may think they are, an experienced computer user or hacker can find ways of determining the identity the users and what geographic locations they are connecting from. Eddie Kessler, a spokesman for Napster claims that the software will be analyzed to see how they can make it more secure.[17] However, the truth is if a professional or hacker has the will, they will always find a way to beat or disrupt security.

---

[16] "Being Traced Over the Internet", http://www.internetprivacy.com/Traced/.
[17] Festa, Paul. (2000, January 26). Security Problem Discovered in Napster Music Software. *CNET News.com* [Online]. Available: http://news.cnet.com/news//0-1005-200-532962.html?tag=st.cn.sr.ne.1 [2000, July 14]

Even when those companies who are believed to be most trusted offer, "free" Internet services there can still be problems. On July 12, 2000, it was reported that Microsoft's "free" email service known as Hotmail experienced a "data spill". According to Stephanie Olsen a staff writer for CNET, "data spills can occur when an HTML page contains an image, or GIF, that is served by a third party company such as an ad network. When the image is served, the web address, including any personal data, is sent to the third party so that ad network can know where to deliver the image"[18] Hotmail has nearly 67 million subscribers, many of which subscribe to HTML newsletters. It is essentially through these newsletters that the data leak occurs. It is also important to note that this recent glitch with the email service is only one of several that Microsoft has "admitted" to the public.[19] Incidents such as this bring reality to the fact that even the most reputable of companies can sometimes not be fully trusted or safe.

As can be seen, "free" online services, do in fact come with a price. They may not be collecting money, but they are surely collecting something. These online services are goldmines to the Internet based advertising agencies that fund them. It is amazing how much information can be collected on a user based on the web sites they visit or the online searches they do. Information that helps advertisers specifically cater to a user's interests. One's online activity often leads to the generation of advertisement banners that the user may find appealing. These marketing strategies are rather clever.

As the number of subscribers to such services continues to grow many advertising agencies are beginning to see the potential of such a medium. So, these advertising

---

[18] Olsen, Stephanie. (2000, July 12). Hotmail Glitch Exposes Email Addresses. *CNET News.com* [Online]. Available http://news.cnet.com/news//0-1007-200-2247861.html?tag=st.cn.sr.ne.1 [2000, July 14]
[19] Olsen, Stephanie. (2000, July 12). Hotmail Glitch Exposes Email Addresses. *CNET News.com* [Online]. Available http://news.cnet.com/news//0-1007-200-2247861.html?tag=st.cn.sr.ne.1 [2000, July 14]

agencies decide to invest a little for the massive amounts of marketing information they will obtain in return. However, their desire to learn more about the users of the Internet may be going a step too far. The Internet user's personal privacy and security are often sacrificed in return for utilizing the "free" services that are funded by such agencies.

Who is to blame, the suppliers or subscribers of such services? Every body essentially benefits from this sort of arrangement. The advertisers obtain the information about the user that they want, and the user gets the service he or she craves. Although, the benefits to the user are obvious, the disadvantages aren't always as clean cut.

A majority of the users of such services aren't always the most Internet savvy. They are generally those individuals who are more interested in getting something for nothing. Companies offering, "free" Internet services is often seen as a wish come true. More often then not, it happens to be these individuals who neglect reading the privacy and security policies of the companies offering these "free" online services. Furthermore, it is often their lack of concern and familiarity with what they are ultimately getting themselves into which allows for them to be the most vulnerable.

In an his article entitled "Cheap Shots," Matthew Schwarz, quotes Timothy Hoffman, a psychotherapist and the director of Ambrosian Associates in Pastoral Counseling in Spencer, Massachusetts, who says it best when he states the following:

> "The drive to get Internet tools for free isn't derived from some evolved sense of household budgeting; it's innate. Its part of our animal instinct. It isn't a question of morality. Its why Eve made that tragic mistake – the apple was hanging around for free. Really, it was just a survival instinct to grab it"[20]

[20] Schwartz, Matthew. (2000, 03 Jul). Cheap Shots. *Computerworld,* 60-61.

Most people do just that and forget about the risks they take or the sacrifices they make when they get something in return for nothing.

The issue of "free" online services and the risks and sacrifices to the users involved needs to be further researched. There is no question that some of the users of such services are sacrificing some of their personal privacy and security. Companies who offer such things, as "free" email, Internet access etc. should be further researched. They claim to only be collecting data for marketing their products and services. Are they telling the complete truth? How do the users of such services and even the users of the Internet in general know if the policy and security statements on the websites they view are being enforced?

Questions such as these are of great concern. As a result, there has been a growing need for government intervention. In an attempt to help government recognize that the growing use of online profiling was an important issue to consider analyzing, officials of a popular periodical, Business Week spoke up on the issue. In a message to Congress, these officials stated:

> "… Who is going to hold DoubleClick – or any other data mining company – to the promises in their privacy policies? Most online companies insist that they can regulate themselves. Maybe. But as online direct marketing becomes more successful, the value of personal information will soar – as will the temptations to abuse it. Right now victims have no clear legal recourse… only the federal government can fill these shoes."[21]

[21] Network Advertising Initiative: Principles not Privacy, July 2000, July 2000, http://www.epic.org/privacy/internet/NAI_analysis.html.

In a verbal statement before a US Congress Committee, Fred Cohen, a premier leader in the world of computer forensics, investigations and vulnerabilities, offered some excellent insight. He stated, "The Internet today is an anarchy. Nobody is in charge, there are few rules, and almost no enforcement."[22] In the real world, if a complaint against a business needs to be filed, one would know to contact the Better Business Bureau. However, in the virtual world, who is one to turn to when a complaint needs to be addressed? If proper legislation is proposed and passed in the near future, there may be reasonable answers to such questions.

One of the problems with policing enforcing policies on the Internet is that there are millions of active websites and only a given amount of time in a day. Furthermore, because the Internet is expanding at an enormous rate it is becoming more difficult to keep track of what is truly occurring in Cyberspace.

We must stop for a moment and face reality. The Internet has become a medium for exploitation of all sorts. With proper research comes further knowledge. The Internet is a valuable tool if used correctly. It needs to be beneficial to all who use it. Although, it has many obvious advantages, the risks associated with the Internet need to be brought out more into the light. Once the risks are exposed, awareness grows. With proper awareness, comes the ability to make better decisions.

---

[22] Verbal Statement of Fred Cohen, a world renowned computer forensics investigator, before a Congressional committee on serious cyber threats to the economic well being of the United States, http://fc@all.net/journal/vertbal.html.

Bibliography

"Being Traced Over the Internet", http://www.internetprivacy.com/Traced/.

Cohen, Fred. Verbal statement before a U.S. Congressional committee:

Serious Cyber Threats to the Economic Well Being of the United States.

http://fc@all.net/journal/vertbal.html.

Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital*

[Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html.

[2000, July 26].

Elchelberger M.L.I.S, Lori. The Cookie Controversy: Introduction.

Available: http://www.cookiescentral.com/ccstory/index.htm [2000, July 26].

Elchelberger M.L.I.S, Lori. The Cookie Controversy: Privacy Issues.

Available: http://www.cookiescentral.com/ccstory/cc4.htm [2000, July 26].

Festa, Paul. (2000, January 26). Security Problem Discovered in Napster Music

Software. *CNET News.com* [Online]. Available:
http://news.cnet.com/news//0-1005 200-532962.html?tag=st.cn.sr.ne.1 [2000, July 14].

Kenworthy, Karen. (1998, September). Cookie Crumbs. *Windows Magazine* [Online].

Available: http://www.winmag.com/Karen. [2000, July 26].

Network Advertising Initiative: Principles not Privacy, July 2000, July 2000,

http://www.epic.org/privacy/internet/NAI_analysis.html.

Olsen, Stephanie. (2000, July 12). Hotmail Glitch Exposes Email Addresses. *CNET*

News.com [Online]. Available:

http://news.cnet.com/news//0-1007-200-2247861.html?tag=st.cn.sr.ne.1 [2000, July 14].

Schwartz, Matthew. (2000, 03 Jul). Cheap Shots. *Computerworld,* 60-61.

Slayton, Marc. (1996, November). It Ain't All Cookies and Cream. *Webmonkey* [Online]. Available: http://www.media-awareness.ca/eng/issues/priv/resource/cookies.htm. [2000, July 27].

Whalen, David. The Official Cookie FAQ: version 2.53. Available: http://www.cookiecentral.com/faq. [2000, July 27].

Wice, Nathaniel. (2000, February 02). Advocates Declare Privacy War Against DoubleClick. *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,38568,00.html. [2000, July 26].

Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].

Footnotes

[1] Kenworthy, Karen. (1998, September). Cookie Crumbs. Windows Magazine [Online]. Available: http://www.winmag.com/Karen. [2000, July 26].

[2] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].

[3] Schwartz, Matthew. (2000, 03 Jul). Cheap Shots. *Computerworld,* 60-61.

[4] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].

[5] Winters, Rebecca. Free Economy: Internet Service Providers. *Time Digital* [Online]. Available: http://www.time.com/time/digital/reports/free/isp.html. [2000, July 26].

[6] Wice, Nathaniel. (2000, February 02). Advocates Declare Privacy War Against DoubleClick. *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,38568,00.html. [2000, July 26].

[7] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Introduction. Available: http://www.cookiescentral.com/ccstory/index.htm [2000, July 26].

[8] Whalen, David. The Official Cookie FAQ: version 2.53. Available: http://www.cookiecentral.com/faq.. [2000, July 27].

[9] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online].

Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

[10] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Introduction. Available: http://www.cookiescentral.com/ccstory/index.htm [2000, July 26].

[11] Slayton, Marc. (1996, November). It Ain't All Cookies and Cream. *Webmonkey* [Online]. Available: http://www.media-awareness.ca/eng/issues/priv/resource/cookies.htm. [2000, July 27].

[12] Elchelberger M.L.I.S, Lori. The Cookie Controversy: Privacy Issues. Available: http://www.cookiescentral.com/ccstory/cc4.htm [2000, July 26].

[13] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

[14] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

[15] Dowell, William. (2000, June 15). The Cookie Jar (a.k.a. Your Computer) *Time Digital* [Online]. Available: http://www.time.com/time/digital/daily/0,2822,47451,00.html. [2000, July 26].

[16] "Being Traced Over the Internet", http://www.internetprivacy.com/Traced/.

[17] Festa, Paul. (2000, January 26). Security Problem Discovered in Napster Music Software. *CNET News.com* [Online]. Available: http://news.cnet.com/news//0-1005-200-532962.html?tag=st.cn.sr.ne.1 [2000, July 14]

[18] Olsen, Stephanie. (2000, July 12). Hotmail Glitch Exposes Email Addresses. *CNET News.com* [Online]. Available http://news.cnet.com/news//0-1007-200-2247861.html?tag=st.cn.sr.ne.1 [2000, July 14]

[19] Olsen, Stephanie. (2000, July 12). Hotmail Glitch Exposes Email Addresses. *CNET News.com* [Online]. Available http://news.cnet.com/news//0-1007-200-2247861.html?tag=st.cn.sr.ne.1 [2000, July 14]

[20] Schwartz, Matthew. (2000, 03 Jul). Cheap Shots. *Computerworld,* 60-61.

[21] Network Advertising Initiative: Principles not Privacy, July 2000,

July 2000, http://www.epic.org/privacy/internet/NAI_analysis.html.

[22] Verbal Statement of Fred Cohen, a world renowned computer forensics investigator, before a Congressional committee on serious cyber threats to the economic well being of the United States, http://fc@all.net/journal/vertbal.html.

About the Author

Robert Fried holds a B.S. and an M.S. in Forensic Science with a concentration in Advanced Investigation. He also holds Certificates in Law Enforcement Science, Forensic Computer Investigation, and Information Protection and Security from the University of New Haven and SEARCH. Fried has extensive knowledge of forensic science, however, most recently he has worked extensively in the developing field of "digital forensics" and has published in this area by organizations such as the SANS Institute. He is also a member of the NorthEast chapter of the High Technology Crime Investigation Association (HTCIA).