Global Information Assurance Certification Paper

Dominique Kilman
February 10, 2003
GSAE version 1.1, option 1, assignments 1,2

Assignment 1:

Anonymity and Privacy in an Internet World

Abstract
A common perception regarding privacy on the Internet is that it is only necessary for individuals who wish to do something "bad". This perception is untrue since every Internet user needs to be concerned with who is tracking their personal information and what that information may be used for. Without a large demand from the public, privacy will not be guaranteed on the Internet for anyone. In a world where privacy cannot be guaranteed, users are beginning to choose anonymous services to try and hide their personal information and browsing habits from the general population.

This paper defines what anonymity and privacy really mean, the reasons behind users' need for anonymity, and some of the legal issues. Some of the technologies available for anonymous communication are discussed. Anonymity and privacy must be a priority for all Internet users. Ignoring the gradual loss of both of these will lead to an online world in which every individual is at risk from every web page they visit.

Introduction
In an age where more and more companies are collecting information from online surfers, the desire to remain anonymous is increasing. But in a changing world, questions arise as to whether anonymity is really a good thing. This paper will discuss the different issues surrounding the anonymity concept including the current methods for providing anonymity, why a person would desire anonymity, the legal issues surrounding the subject and some of the misconceptions regarding anonymity and privacy.

Anonymity vs. Privacy
Merriam-Webster defines privacy as "**a**: the quality or state of being apart from company or observation **b**: freedom from unauthorized intrusion <one's right to *privacy*>."[14] In our discussion, it is the second definition that we are concerned with: "freedom from unauthorized intrusion." In an online sense, a practical definition of privacy is that a company or site will not share the user's personal information with others.

For a definition of anonymity, we must first define anonymous. The definition for anonymous, again from Merriam-Webster is "**1**: not named or identified **2**: of unknown authorship or origin **3**: lacking individuality, distinction, or recognizability."[13] For our discussion, we will use the first definition "not named or identified." Anonymity is the state of being anonymous, therefore the state of being unnamed or unidentified. . Online, anonymity is the inability for one user's actions to be traced back to that user by another.

Many believe that privacy and anonymity are virtually the same thing. In reality, anonymity and privacy are two separate areas of concern. Users who desire privacy are usually supplying personal information to a web site in exchange for a service. This user wants to be assured that the information will not be sold or shared with others unless the user authorizes this action. The anonymous user wants to be able to use all of the features of the Internet without having these actions being linked to the specific user.

Another type of anonymity that is useful in the online world is authenticated anonymity. This occurs when the right of a user to perform an action is known, but the actual identity of the person is not known. This is synonymous with real world key codes: the fact that a person has a key code proves their right to use the code, but which individual actually punches in the numbers is unknown.

Privacy and Anonymity

A common perception in the Internet community is that privacy laws will protect individual rights. In the United States, this belief has some legal basis with HIPPA (Health Insurance Portability and Accountability Act of 1996, [11]) and other laws defining what information can be shared. Most web sites that require personal information also have privacy statements that users should read and agree to [18]. Generally, these statements pledge not to share personal information with outside companies or individuals. Unfortunately, there are recent examples in which companies have violated their own privacy statements. See USA Today article for more details [17]. Another unfortunate quality of privacy statements is the obscure and difficult language. Many users accept the policies without reading or understanding what they are agreeing to.

Privacy Statements

Privacy statements and laws do not address the issue of tracking. A company can potentially track all of the websites that an individual visits. An example of problems with this is that a health insurance company could deny coverage to an individual because that individual had previously visited a cancer website.

What is being tracked?

All websites track some data regarding visitors to their sites. For an example of what can be tracked, visit http://www.somebody.net/someother.html. This page shows exactly what information is collected when you visit their website. The

data shown on this website represent environment variables present for all web surfers. Using cookies (information stored on a users machine for later use), a website can gather more extensive data about a user.

Why do we want it?

So why would a person choose to be anonymous? A common assumption is that anyone who desires anonymity is a criminal or wants to engage in criminal activities. This assumption is incorrect.

Personal Privacy

Some users simply do not want to have their actions monitored by anyone. Much of the monitoring done by websites is used to build a profile of a user. This information can be used to create user-specific pop-up ads that will appeal to the user or possibly to tailor search items based on choices that the user previously made. Not everyone wants to have randomsite.com to be able to monitor every website they visit, how long they spend on those sites, what links they click, etc. To some surfers, this kind of monitoring is akin to having another person follow them around the mall recording every stop and purchase.

Whistleblowers

Other users are providing information that could have a negative impact on themselves if they are revealed as the source in the information. Whistleblowers are the classic example of this user. An individual has evidence that their company is doing something illegal and wants to let the public know. The employee however does not want to loose their job as a result of this disclosure so she wishes to be anonymous. We often see examples of this type of anonymity in the news. "An unidentified source…" and "… on the condition of anonymity…" are common phrases when reading political news articles. If a user's electronic communications are being monitored, it would be possible for the company in question to discover the identity of the whistleblower and retaliate for the released information.

Radical Governments

Individual living in countries where their government monitors all electronic communications may also desire anonymity. In countries where government criticism is illegal, users who wish to espouse different political views must often hide their identity in order to avoid severe penalties.

Criminal Activity

Of course, there are individuals who wish to be anonymous so that they can get away with illegal activities. An individual who wishes to use the Internet for illegal activities such as child pornography will desire anonymity when doing so. Others may wish to post obscene or threatening emails without revealing their identity. Still others may want to arrange criminal activities that take place in the physical world using the Internet without being identified.

The fact that anonymity **can** be used for illegal activities should not mean a ban on all anonymous technology. VCRs can be used for illegal activities, but this does not cause the government (or the movie industry) to ban all VCRs.

Online Voting
A future application for online authenticated anonymity would be online voting. The candidate that an individual votes for should be kept confidential but the fact that the individual voted must be recorded.

How to be anonymous (and how not to be anonymous)
Remailers
Remailers typically take a message and strip off all of the identifying headers before forwarding the message to the recipient. There are two types of services that are often lumped together in the *anonymous remailer* group: pseudo-anonymous remailers and anonymous remailers. When using a pseudo-anonymous remailer, each user has an account with the service which links the anonymous email address to the users true email address. Only the operators of the remailer can see the true identity of their users. Unfortunately, a court order could force the operators to reveal the identity of its customers, or the operator's computer system could be hacked thus exposing the data.

True anonymous remailers (Mixmaster [15], Cypherpunk [8]) do not store information tying their users to their true identities. These services are usually run by volunteers, so individuals using these services do not need to reveal their identities to pay for the service. Since no one in the system knows anyone's true identity, the information cannot be revealed. Most of these systems work by forwarding messages through many hops after the header information has been removed. When a large number of messages are being forwarded through the system, it is impossible to determine where an individual email originated.

If the email messages themselves contain identifying information (like a signature) the anonymity of the system is compromised. Individuals using these types of services should encrypt the messages and should avoid including identifying information within the message.

Off-Record Messaging
A new system developed at Cal-Berkely by Ian Goldberg [3] is off-record messaging. In this system, two parties can authenticate each other, but the sender of a message cannot be revealed at a later time. If one party in the conversation chooses to reveal the messages from the conversation, he could not prove which party sent the message.

Aliases
Another common misconception regarding anonymity is the use of aliases. An alias is a name that a user makes up so as not to reveal his true name. Email services like Yahoo! [19], Hotmail [12] and others all have this feature. What

most users do not realize is that with tracking and monitoring software, a company can build up clues to the identity of the user even when they are using the alias. Also, when signing up for these services, additional personal information is required when the accounts are created. For example, at Yahoo!, I chose a screen name when I signed into the service. I use this name (and a password) to use Yahoo! Messenger, Yahoo! Groups and other parts of the Yahoo! Website. This alias can be tied to any groups that I have joined, the individuals that I chat with, and even an alternate email address that I use for some services. Yahoo! Can be forced to reveal my true identity if faced with a court order. The information that I supplied when I created the account would then be revealed.

Backdoors

In recent years, the US government has tried to legislate cryptography in order to allow law enforcement easy access to encrypted messages. The Clipper Chip is an example of a government backdoor [7]. The government feels that they should have the ability to decrypt any message IF the proper legal procedures have been followed. (I.e. obtain a warrant) Some feel that the same backdoor policy should apply to anonymity.

Control

If these backdoor services are required for anonymous systems, who should control the information? Who would control when and if the information was released? In the US, a common argument is that the court system would control access to the information. Any agency wishing to access the private information must obtain a search warrant for the information. The agency should only be able to retrieve the information for the individual towards which the warrant was issued. This means that some other entity must search through all of the records to find the one that will be released. This leads to the question of who is storing the information. In other countries, the government may be the reason for anonymity, so allowing the government to control access to the information defeats the purpose of anonymity.

Anonymous or not?

If the government can break anonymity, was the service really anonymous in the first place? In order to obtain the details about an individual using anonymous services, the information must be stored somewhere. The potential for someone without the proper authority to break in and steal this information should make users wary of the system. The user must also worry about the integrity of those keeping the information. A malicious individual could sell the anonymity data to the highest bidder. There are already stories in the news about employees selling credit information [5] and other personal data. In an anonymity database, the identity information can be more valuable than any other data stored about an individual.

The Law

Privacy Concerns
New legislation proposed in the wake of September 11, 2001 has many privacy advocates concerned. A recent addition to the Homeland Security Bill [4] would prevent users from suing their ISP over disclosures of information. This takes away the rights of the consumer to keep their own information private. The new additions also include provisions to make it easier for law enforcement to trace online users. The aura of fear created by the terrorist attacks has led to the reduction in online privacy and a fear of those who desire anonymity. Individuals are currently giving up rights (both online and real world) in order to feel safer. Unfortunately, this loss may never be regained.

Criminals
The laws that are crafted regulating privacy and anonymity may not have the effect of making people safer. Laws created in the United States will not apply to online users in other countries. Criminals will not necessarily follow these online laws. Outlawing anonymity services and shutting them down will not stop the technology. The services may go underground in order to avoid prosecution and other means for hiding information will be developed despite and sometimes because of the laws.

Regulated Encryption
Currently, the US government regulates the strength of encryption that can be exported to other countries. To get around these export laws, encryption algorithms have been printed and mailed to other countries. The algorithm is then either scanned or typed into a computer so that the algorithm can be compiled and used. Those who want to circumvent the law regarding encryption find alternate means to share the information.

Digital Millennium Copyright Act (DMCA) [DMCA]
The DMCA laws enable the government to force the removal of code that is a violation of the law. The DeCSS[1][9] technology developed in Russia was found to violate the DMCA. The developer removed the program, but copies are still available on the Internet. Technology that is posted on the Internet and subsequently found to be illegal can rarely be completely removed. There are many copies in many places which makes full removal impossible.

Tracking Systems
Currently, there are some systems that the United States government has or is speculated to have that will track online activity. These capabilities have been speculated about for some time, but not all of the details have been fully disclosed.

Carnivore [6]

[1] DeCSS allows a user to copy DVDs despite the CSS encryption used. The program was developed to allow a user to watch DVDs on a Linux computer

Carnivore is a diagnostic tool used by the FBI to monitor Internet traffic. Carnivore was developed in response to the increase in criminal activity on the web. In order to monitor the traffic, the FBI must obtain a court order to intercept specific traffic. The difference between Carnivore and other commercial programs available to monitor traffic is the ability for Carnivore to distinguish between traffic that can be lawfully intercepted and traffic that cannot. The fact that Carnivore exists leads to speculation that it could be used to monitor any traffic on the network, not just the traffic that is lawfully interceptable.

Echelon [10]
Echelon is a global surveillance program which allows for the capture of virtually all communication data. Echelon reportedly has the ability to capture cellular, fiber-optic, satellite and microwave communication. There are few details regarding the use and specifications of the Echelon program. The website http://www.echelonwatch.org/ is a watchdog group administered by the ACLU which offers what details are available regarding the use and legality of Echelon.

Magic Lantern [1]
Another FBI program is Magic Lantern. Magic Lantern is being developed by the FBI to facilitate password or encryption key discovery. Encryption technology is increasingly used in Internet communication as individuals become more concerned with privacy. As a result, intercepting meaningful information becomes more difficult, unless the keys can be discovered. The FBI confirms that there is a program still in development and has been reluctant to release details. Some reports reveal that Magic Lantern works by logging the keystrokes of a computer user to discover the passwords or keys used. Some experts speculate that the Magic Lantern program can be installed on users' computers without the consent or knowledge of the user.

Conclusions
With governments developing surveillance systems, individuals must demand full disclosure about these systems. The potential loss in personal freedom resulting from these systems may outweigh the possibility of discovering criminal activity in time to prevent the planned actions. All computer and Internet uses must be made aware of the sacrifices that they are making by ignoring these infringements of privacy.

Anonymity on the Internet is an important tool to protect individual freedoms. It is a necessary service that should not be outlawed simply because it has the potential to be misused. All technology has the potential to do harm; it is up to the individual users to make the choice of how the technology will be used. Until we live in a perfect world where individual freedom is guaranteed, the benefits of anonymity, especially for those living in oppressive societies, far outweigh the potential for harm.

References

[1] Eng, Paul. *Shedding Light on magic Lantern.* ABCNews .com. Retrieved January 10, 2003 from http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge011221.html.
[2] Engelfriet, Arnoud "Galactus" (1998). Anonymity: Index. Retrieved November 5, 2002 from http://www.stack.nl/~galactus/remailers/index-anon.html
[3] Goldberg, Ian. July, 2002. Black Hat Briefings. Retrieved December 26, 2002 from http://www.blackhat.com/presentations/bh-usa-02/bh-us-02-goldberg-messaging.pdf.
[4] Krebs, Brian. *Tech Provisions Added to Homeland Security Bill.* November 14, 2002. The Washington Post Online. Retrieved Dec 36, 2002 from http://www.washingtonpost.com/wp-dyn/articles/A54872-2002Nov14.html.
[5] Masters, Brooke A. & Mayer, Caroline E. (2002). *Identity Theft More Often an Inside Job*. SecurityFocus Online. Retrieved December 26, 2002 from http://online.securityfocus.com/news/1727.
[6] Carnivore Diagnostic Tool. Retrieved January 10, 2003 from http://www.fbi.gov/hq/lab/carnivore/carnivore.htm.
[7] Clipper Chip (1994). Retrieved December 26, 2002 from http://www.cpsr.org/program/clipper/clipper.html.
[8] Cypherpunk Remailers. Retreived October 28, 2002 from http://www.csua.berkeley.edu/cypherpunks/remailer/.
[9] DeCSS Central. Retrieved January 2, 2003 from http://web.lemuria.org/DeCSS/
[DMCA] Digital Millennium Copyright Act. Retrieved January 2, 2003 from http://www.educause.edu/issues/dmca.html
[10] Echelon Watch. Retrieved January 10, 2003 from http://www.echelonwatch.org/.
[11] HIPPA. Retrieved January 8, 2003 from http://www.hep-c-alert.org/links/hippa.html.
[12] Hotmail website. Retrieved November 5, 2002 from www.hotmail.com.
[13] Merriam-Webster online dictionary. Anonymous Definition. Retrieved October 28, 2002 from http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=anonymous
[14] Merriam-Webster online dictionary. Privacy Definition. Retrieved October 28, 2002 from http://www.m-w.com/cgi-bin/dictionary?book=Dictionary&va=privacy
[15] Mixmaster Remailer. Retrieved October 28, 2002 from http://sourceforge.net/projects/mixmaster.
[16] Privacy and Security Protection. Retrieved October 28, 2002 from http://www.privacyresources.org/why.htm
[17] US Today (2000). *E_tailers violate own privacy policies*, August 4, 2000. Retrieved November 5, 2002 from http://www.usatoday.com/life/cyber/tech/cti307.htm.
[18] Yahoo! Privacy Policy. Retrieved November 5, 2002 from http://privacy.yahoo.com/.
[19] Yahoo! Website. Retrieved October 28, 2002 from www.yahoo.com.

Assignment 2:

Audit

This is an audit of a generic online privacy policy. The policy itself has links to some other relevant topics included with the company website. In the policy analysis, only the actual privacy policy will be discussed, but some of the linked sections will be discussed within the recommendations section.

Policy Analysis

The privacy policy included in this audit is a generic version of many of the privacy policies that online users must agree to before signing up for services. The policy defines what personal information is, when, how and with whom that information will be shared and some other general information about privacy, account deletion. Along with the actual privacy policy, I have included some definitions that are linked to by the policy which help explain some of the technical details.

Section I

The policy introduction starts by telling the user what the policy will cover: how the company will treat personal information that is collected about an individual. Personal information is defined for the user, but the definition becomes confusing when the policy states that the information (such as name, address, etc) is not publicly available. Some users may be confused as to why name and address is considered "not publicly available". A better definition of what the company means by publicly available would be useful.

Section II

The next section identifies when the company collects the defined personal information. The list is fairly comprehensive and worded in such a way that most users will understand it. Links are provided to technical definitions such as IP address and there are also links provided to company-specific terms defining promotions or services. One area of concern in this section is the statement "…provide anonymous reporting for internal and external clients". There is no definition of who these clients are, and exactly what this anonymous reporting includes would be of interest to the end-user. The list of information collected mentions that the company will record information based on the pages requested, but this section could state more clearly that all surfing activity will be tracked once the user logs in to the service.

A special section is included for children using the service. The company policy states that children under 13 will receive special treatment regarding personal information. In order to receive this protection, a "Family Account" must be created. This is a good policy to have, unfortunately, not all children will read the policy before they create an account for themselves. There is nothing in the

policy to indicate that the company will use the supplied birth date to check that the individual is over 13 before creating the new account.

Section III
Section III discusses when information will be shared with outside companies. The company states that it will share personal information with trusted partners. The end-user has no information regarding these partners and the policy does not give any hints as to who these may be. The policy does state that the partners must have signed agreements with thisCompany and that the partners may not share the information.

Section IV
The subject of cookies is addressed in this section to inform the user that thisCompany will save cookies on the user's computer. A link to the technical definition for cookies is provided for further explanation. Another technology, web beacon, is mentioned and a link to the definition is provided.

Section V
Section V discusses the end-user's ability to change and delete personal information stored by the company. Links are provided in this section to take the user directly to their personal information and a link to the delete account area. Some information may remain in the company database after account has been deleted. Links to what information is persistent is provided. Again, a special section for children under 13 is provided. The only difference between general account maintenance and a child's account maintenance is the ability for parents to edit a child's information. This parental control is only available if the child has signed up using the family account process.

Section VI
This section addresses how the company will secure the information provided by the user. The measures listed include limiting employee access, password protection, and SSL-encryption. The policy also refers to federal regulations, but does not have a link to inform the user about these regulations. A link explaining SSL-encryption would also be beneficial to the user.

Section VII and VIII
The final sections involve changes and comments. The policy states that thisCompany may change the policy and will notify users about significant changes. This implies that the company may make changes to the policy without notifying users of the changes. The final section informs the user that thisCompany is certified by a recognizable Internet privacy organization. The certification only applies to the English version of the thisCompany.com domain. Contact information is provided to the user for any questions or suggestions.

Policy Objectives
The objectives for a policy define the scope of the policy and tell the reader what the policy should accomplish. In this example, the policy objectives are:

- What defines personal information and how is it obtained
- How the information will be shared
- Who will the information be shared with
- What are the safeguards
- Special provisions for children

Controls
Controls are mechanisms that are put in place within the policy to ensure that the policy is being followed. The controls stipulated within this policy are:

- User can opt-out of receiving marketing communications
- User has the option to delete their account if they do not agree with the company policies
- Parents can control the sharing of information if the account is for a child under 13
- Information restricted to need to know employees
- Information will not be transferred to advertisers on the thisCompany domain

Audit Controls
Audit controls are a subset of the controls mentioned above. These controls are those put in place to allow and outside auditor to ensure that the policy is being followed. Currently, there are no audit controls within the policy. Some audit controls that should be included are:

- Log change information for users' information by employees to ensure unauthorized changes are not being made
- Log all access to the information database to ensure there has been no unauthorized access
- Clearly define the regulation being followed for physical security of the machines containing the database
- Detail any encryption being used to protect data, or what type protection is used within the database

Mitigating Controls
Mitigating controls are a subset of the controls mentioned above. These controls are in place to prevent specific known abuses from taking place. The current policy has some existing mitigating controls listed below and I have also listed some additional controls that should be included.

Existing:

- Under-age accounts to safeguard children's information
- SSL-level encryption to protect some transactions
- Physical, electronic and procedural safeguards to protect the database of information
- Confidentiality agreements with trusted partners to ensure information is used appropriately

Needed:

- Users should have the option to disallow their personal information from being transferred if thisCompany is ever sold
- Check date of birth to make sure that a subscriber is an adult before allowing them to sign up for an adult account
- Special protections in place for user's social security numbers, encryption for example
- Notify users when changes are made to the marketing preferences pages so that users will know if they need to update their preferences

Recommendations

This section lists the recommendations that I have to make the policy better. Most of these recommendations involve giving more detail so the users can make a better-informed decision.

- Does the parent need the child's password to delete a child's account?
- Explain what the regulations referred to in section VI are
- Clarify what type of information is tracked and what the boundaries are (does the track continue when the user leaves the thisCompany domain or when the user logs out?)
- Detail who the thisCompany partners are so the user knows who will have access to their information
- Explain what the maximum amount of information required for a child participating in promotions or online activities
- Explain how long updates to marketing preferences would take so users will have a deadline to know when changes should be affected

Define Audit Process

The audit process will define what actions the auditor would take to ensure the privacy policy is being adhered to. This process is divided into two sections: one for a general level audit and another for an aggressive audit. The aggressive audit procedures will try to determine of the controls put in place will protect the privacy of users against a directed attack. The section that the audit step pertains to is listed when appropriate.

General

Accounts

- Create several accounts both for adults and children accounts (Section II)
    - Verify what information is being stored fore these accounts in the database
- Delete some of these accounts (both adult and child) (Section V)
    - Verify that the information remaining in the database corresponds to the information in the privacy policy
- Create an adult account using a date of birth which is for a person under 13 (Section II)
    - This should not be allowed because of the special treatment needed for children under 13
- Turn marketing preferences on or off to make sure these changes are properly recorded and respected (Section V)
- Check that under 13 accounts are segregated from normal accounts

Database

- Verify that the database is only accessible to those with the correct access privileges
    - Verify what employees have access to the database and determine if these employees have a legitimate need to access the database (Section VI)

Online accesses

- Inspect cookies that are stored by thisCompany to determine what information is available (Section IV)
- Try to access thisCompany cookies as an outsider
    - Forge the web beacon information used by thisCompany to access the cookies (Section IV)

Partners

- Verify how information is shared with partners to see that no unallowed information is shared (Section III)
- Check the reporting process for internal/external clients to verify that information is stored anonymously (Section II)
- Ensure that clicking on ads within the thisCompany domain does not transfer any information (Section III)
- Verify that outside companies have policy in place that states the information gained from thisCompany is not shared
- Check if accounts for those under 13 are treated special when information is shared

Aggressive

- Try to access the database from the outside using traditional hacking methods
- Try to buy personal information from thisCompany (Section III)

thisCompany Privacy Policy

I. What This Privacy Policy Covers

- This policy covers how thisCompany treats personal information that thisCompany collects and receives, including information related to your past use of thisCompany products and services. Personal information is information about you that is personally identifiable like your name, address, email address, or phone number, and that is not otherwise publicly available.
- This policy does not apply to the practices of companies that thisCompany does not own or control, or to people that thisCompany does not employ or manage.

II. Information Collection and Use

General

- thisCompany collects personal information when you register with thisCompany, when you use thisCompany products or services, when you visit thisCompany pages or the pages of certain thisCompany partners, and when you enter promotions or sweepstakes. thisCompany may combine information about you that we have with information we obtain from business partners or other companies.
- When you register we ask for information such as your name, email address, birth date, gender, zip code, occupation, industry, and personal interests. For some financial products and services we may also ask for your address, Social Security number, and information about your assets. Once you register with thisCompany and sign in to our services, you are not anonymous to us.
- thisCompany collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.
- thisCompany automatically receives and records information on our server logs from your browser, including your IP address, thisCompany cookie information, and the page you request.
- thisCompany uses information for the following general purposes: to customize the advertising and content you see, fulfill your requests for products and services, improve our services, contact you, conduct research, and provide anonymous reporting for internal and external clients.

Children

- When a child under age 13 attempts to register with thisCompany, we ask that he or she have a parent or guardian create a thisCompany Family Account to obtain parental permission.
- thisCompany will not contact children under age 13 about special offers or for marketing purposes without a parent's permission.
- thisCompany does not ask a child under age 13 for more personal information, as a condition of participation, than is reasonably necessary to participate in a given activity or promotion.

III. Information Sharing and Disclosure

- thisCompany does not rent, sell, or share personal information about you with other people or nonaffiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:
    - We provide the information to trusted partners who work on behalf of or with thisCompany under confidentiality agreements. These companies may use your personal information to help thisCompany communicate with you about offers from ThisCompany and our marketing partners. However, these companies do not have any independent right to share this information.
    - We have a parent's permission to share the information if the user is a child under age 13. Parents have the option of allowing thisCompany to collect and use their child's information without consenting to thisCompany sharing of this information with people and companies who may use this information for their own purposes;
    - We respond to subpoenas, court orders, or legal process, or to establish or exercise our legal rights or defend against legal claims;
    - We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of thisCompany's terms of use, or as otherwise required by law.
    - We transfer information about you if thisCompany is acquired by or merged with another company. In this event, thisCompany will notify you before information about you is transferred and becomes subject to a different privacy policy.
- thisCompany displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click on targeted ads meet the targeting criteria - for example, women ages 18-24 from a particular geographic area.

- thisCompany does not provide any personal information to the advertiser when you interact with or view a targeted ad. However, by interacting with or viewing an ad you are consenting to the possibility that the advertiser will make the assumption that you meet the targeting criteria used to display the ad.
- thisCompany advertisers include financial service providers (such as banks, insurance agents, stock brokers and mortgage lenders) and non-financial companies (such as stores, airlines, and software companies).

IV. Cookies

- thisCompany may set and access thisCompany cookies on your computer.
- thisCompany lets other companies that show advertisements on some of our pages set and access their cookies on your computer. Other companies' use of their cookies is subject to their own privacy policies, not this one. Advertisers or other companies do not have access to thisCompany's cookies.
- thisCompany uses web beacons to access thisCompany cookies inside and outside our network of web sites and in connection with thisCompany products and services.

V. Your Ability to Edit and Delete Your Account Information and Preferences

General

- You can edit your thisCompany Account Information (link to user specific information), including your marketing preferences (link to user specific information), at any time.
- New categories of marketing communications may be added to the Marketing Preferences page from time to time. Users who visit this page can opt out of receiving future marketing communications from these new categories or they can unsubscribe by following instructions contained in the messages they receive.
- We reserve the right to send you certain communications relating to the thisCompany service, such as service announcements, administrative messages and the thisCompany Newsletter, that are considered part of your thisCompany account, without offering you the opportunity to opt-out of receiving them.
- You can delete your thisCompany account by visiting our Account Deletion (link to user specific information) page. Please click here to read about information that might possibly remain in our archived records after your account has been deleted.

Children

- Parents can review, edit, and delete information relating to their child's thisCompany account using tools offered by thisCompany Family Accounts.
- If a parent chooses not to allow us to further collect or use a child's information, parents enrolled in thisCompany Family Accounts can delete their child's account by signing into that child's account and then visiting our Account Deletion (link to user specific information) page. Please click here to read about information that might possibly remain in our archived records after your account has been deleted.

VI. Confidentiality and Security

- We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.
- We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.
- Your thisCompany Account Information is password-protected.
- In certain areas thisCompany uses industry-standard SSL-encryption to protect data transmissions.

VII. Changes to this Privacy Policy

- thisCompany may update this policy. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your thisCompany account or by placing a prominent notice on our site.

VIII. Questions and Suggestions

- thisCompany is InternetPrivacyCo -certified. This certification applies to all English-language sites under the thisCompany.com domain. If you feel that your inquiry has not been satisfactorily addressed, you should contact InternetPrivacyCo, an independent privacy organization. InternetPrivacyCo serves as a liaison with thisCompany to resolve your concern.
- If you have questions or suggestions, please complete a feedback form or you can contact us at:

thisCompany Inc.
Customer Care - Privacy Policy Issues
#1 First Avenue
Somewhere, CA 90210
(408) 555-1234

Supporting Information for Privacy Policy

thisCompany Promotions
Most promotions that are hosted or co-sponsored by thisCompany don't require you to be a thisCompany registered user.

Information Collection and Use Practices

- When you enter a promotion, sweepstakes, or contest hosted by thisCompany or sponsored by thisCompany and/or our many partners, we ask for your name, address, and email address.
- You may be asked to provide additional information or to answer certain questions, some of which may be optional, in order to participate.
- We may contact you in connection with a particular promotion, such as a sweepstakes or contest, in order to update you of your status, administer the promotion, let you know that a promotion has ended, and for other purposes.

Information Sharing and Disclosure Practices

- Promotions that are hosted on thisCompany may be sponsored by thisCompany, may be co-sponsored by thisCompany and another company, or may be sponsored by companies other than thisCompany. Some or all of the data collected during a promotion may be shared with the sponsor(s) or companies indicated on the entry form.
- If data will be shared, then there will be notice prior to the time of data collection or transfer.

Practices Regarding Cookies

- Some promotions, sweepstakes, or contests may use cookies in order to track your progress and number of entries in some of our promotions, sweepstakes, and contests.

Other

- When you participate in a thisCompany-sponsored or hosted promotion, you are subject the Official Rules of that promotion.

This page describes current thisCompany practices with respect to this particular service. This information may change as thisCompany revises this service by

adding or removing features or using different service providers. To find out how thisCompany treats your personal information, please visit our Privacy Policy.

IP Addresses

When your web browser or email application requests a web page or email from another computer on the Internet, it automatically gives that computer the address where it should send the information. This is called your computer's "IP address." (IP stands for "Internet protocol.") For most users accessing the Internet from a dial-up Internet service provider (ISP), the IP address will be different every time you log on.

Information Collection and Use Practices

- thisCompany receives IP addresses from all users because this information is automatically reported by your browser each time you view a web page.
- Your IP address is also stored in our user registration databases when you register with thisCompany.
- IP addresses may be used for various purposes, including to:
    - Diagnose service or technology problems reported by our users or engineers that are associated with the IP addresses controlled by a specific web company or ISP.
    - Send the most appropriate advertising based on geographic area or information derived from your IP address. Many IP addresses are commonly associated with Internet service providers, universities, or major corporations in specific regions or localities. Aggregate information derived from IP addresses may also be reported to advertisers.
    - Estimate the total number of users visiting thisCompany from specific countries or regions of the world.
    - Assist merchants in thisCompany Stores and thisCompany Shopping to track visits to and business at their stores.
    - Help determine which users have access privileges to certain content that we host.

Other

- When a thisCompany web page is requested and viewed, that request is logged on our servers with information including the IP address of the computer that requested the page.
- thisCompany Mail includes IP addresses in outgoing mail message headers, as specified by standard Internet protocol.

- thisCompany Messenger sometimes uses a peer-to-peer connection during its operation, including times when you may be using it for instant messaging (text conversations), file sharing, and webcam streaming. Peer-to-peer means that your computer connects directly to the other user's computer in the conversation without needing to go through thisCompany servers. As such, your IP address is available to users you share a peer-to-peer connection with.

Cookies
A cookie is a small amount of data, which often includes an anonymous unique identifier that is sent to your browser from a web site's computers and stored on your computer's hard drive.
Each web site can send its own cookie to your browser if your browser's preferences allow it, but (to protect your privacy) your browser only permits a web site to access the cookies it has already sent to you, not the cookies sent to you by other sites.

Choices about Cookies

- You can configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is set. (Each browser is different, so check the "Help" menu of your browser to learn how to change your cookie preferences.)
- If you reject all cookies, you will not be able to use thisCompany products or services that require you to "sign in," and you may not be able to take full advantage of all offerings. However, many thisCompany products and services do not require that you accept cookies.

thisCompany's Practices Regarding Cookies
thisCompany uses its own cookies for a number of purposes, including to:

- Access your information when you "sign in," so that we can provide you with customized content, such as my thisCompany.
- Keep track of preferences you specify while you are using thisCompany's services -- for example, the local zip code you want to use in thisCompany Yellow Pages or thisCompany Movies.
- Display the most appropriate advertising banners, based on your interests and activity on thisCompany.
- Assist merchants in thisCompany Stores and thisCompany Shopping to process the items in your shopping cart.
- Estimate and report our total audience size and traffic.
- Conduct research to improve thisCompany's content and services.

- Require you to re-enter your thisCompany password after a certain period of time has elapsed to protect you against others accidentally accessing your account contents.

Other Companies' Cookies on ThisCompany

- Please note that thisCompany allows other companies that are presenting advertisements or researching users' response to advertisements on some of our pages to set and access their cookies on your computer.
- Advertisers' and researchers' use of cookies is subject to their own privacy policies, not the thisCompany Privacy Policy

thisCompany Family Accounts

thisCompany Family Accounts allows a parent or legal guardian to give consent before their child creates an account with thisCompany. A child is someone who indicates to us that they are under the age of 13. Family Accounts also allows the parent to access and maintain information about their child's account.

Information Collection and Use Practices

- Before a parent can give consent for their child to register with thisCompany through a thisCompany Family Account, the parent must register and create their own thisCompany account.
- In addition to information requested at registration, thisCompany Family Accounts asks for the parent's name and credit card information. The credit card will not be charged; it is used for real-time verification purposes only.
- The credit card information is archived in a secure fashion as evidence that parental consent was received.

Other

- When you use thisCompany Family Accounts, you are subject to the thisCompany Terms of Service.
- Please see thisCompany Family Accounts Help if you have questions about this service.

This page describes current thisCompany practices with respect to this particular service. This information may change as thisCompany revises this service by adding or removing features or using different service providers. To find out how thisCompany treats your personal information, please visit our Privacy Policy.

Network Advertisers and Third-Party Ad Servers
thisCompany sends to your web browser most of the advertisements you see when you use the thisCompany network of web sites. However, we also allow other companies, called third-party ad servers or ad networks, to serve advertisements within our web pages.

Because your web browser must request these advertising banners from the ad network web site, these companies can send their own cookies to your cookie file, just as if you had requested a web page from the site.

Please note that if an advertiser asks thisCompany to show an advertisement to a certain audience (for example, men ages 18-34) and you respond to that ad, the advertiser or ad-server may conclude that you fit the description of the audience they are trying to reach.

Opting Out of Third-Party Ad Servers
If you want to prevent a third-party ad server from sending and reading cookies on your computer, currently you must visit each ad network's web site individually and opt out (if they offer this capability).

- Currently, thisCompany has relationships with the following third-party ad networks (click to visit their site):
    - (List of partners)

Web Beacons
Web pages may contain electronic images (called a "single-pixel GIF" or "web beacon") that allow a web site to count users who have visited that page or to access certain cookies. thisCompany uses web beacons in the following ways

Within the thisCompany Network

- thisCompany uses web beacons within the thisCompany network of web sites in order to count users and to recognize users by accessing thisCompany cookies.
- Being able to access thisCompany cookies allows us to personalize your experience when you visit thisCompany web sites that are located both on

and off of the thisCompany.com domain. For example, thisCompany *Special* pages are mostly located on the special.com domain.

Outside the thisCompany Network

- thisCompany uses web beacons to conduct research on behalf of certain partners on their web sites and also for auditing purposes.
- Information recorded through these web beacons is used to report aggregate information about thisCompany users to our partners. This aggregate information may include demographic and usage information. No personally identifiable information about you is shared with partners from this research.
- When conducting research thisCompany practice is to require our partners to disclose the presence of these web beacons on their pages in their privacy policies and state what choices are available to users regarding the collection and use of this information. You may choose to opt-out of thisCompany using this information for this research. Please click here to opt-out.

  Note: This opt-out applies to a specific browser rather than a specific user. Therefore you will have to opt-out separately from each computer or browser that you use.

HTML Mail

- ThisCompany's practice is to include web beacons in HTML-formatted email messages (messages that include graphics) that thisCompany, or its agents, sends in order to determine which email messages were opened and to note whether a message was acted upon.

In general, any electronic image viewed as part of a web page, including an ad banner, can act as a web beacon. Advertising networks that serve ads onto thisCompany may use web beacons in their advertisements

Data Storage
Account Information

- When you register with thisCompany or submit information to thisCompany, a temporary copy of that information is routinely made to prevent accidental loss of your information through a computer malfunction or human error.
- thisCompany keeps your account information active in our user registration databases in order to provide immediate access to your personalization preferences each time you visit thisCompany.

- If you ask thisCompany to delete your thisCompany account, in most cases your account will be deactivated and then deleted from our user registration database in approximately 90 days. This delay is necessary to discourage users from engaging in fraudulent activity.
- Please note that any information that we have copied may remain in back-up storage for some period of time after your deletion request. This may be the case even though no information about your account remains in our active user databases.

Servers

- The thisCompany computers (called "servers") that send your web pages and advertising banners process and store an enormous amount of information every day. These computer records are called "log files."
- Log files are used for analysis, research, auditing, and other purposes, as described above. After this information has been used, it is stored and is inaccessible. Until the information is stored, your thisCompany ID may remain in our active server log files.

Products & Services

thisCompany Mail
thisCompany *Mail* is a free web-based email service. In order to use thisCompany *Mail*, you must be a registered thisCompany user. You may also purchase premium services such as extra mailbox storage for a fee.

Information Collection and Use Practices

If you have previously registered with thisCompany, the first time you access thisCompany *Mail*, you will be asked for the first and last name you would like to display on all outgoing mail messages. You can choose the name you would like your account to reflect. If you register with thisCompany through thisCompany *Mail*, this information will be collected during the registration process.

- thisCompany practice is not to use addressing information or the content of messages stored in your thisCompany *Mail* account for marketing purposes.
- Additional mailbox storage, POP/forwarding and other premium services are available for a fee. When you sign up for premium services, you will be asked to create a thisCompany security key and establish a thisCompany *wallet* in order to make payment.
- If you sign up for *subscriptions* we ask you to specify the email address where you want to receive the newsletters or reminders that you specify.

- If you sign up for *reminders*, we ask you to specify your email address and information you want to include in the *reminder*.

Information Sharing and Disclosure Practices

- thisCompany *Mail* includes IP addresses in outgoing mail message headers, as specified by standard Internet protocol.
- The thisCompany *Mail* Personal Address service provides domain registration through Internet Names Company. We ask you to supply the personal information of the registrant and administrative contact such as their name, address, telephone number, and email address. This information is transmitted to Internet Names Company or "INCC" for the purpose of registering your web address (domain name). By registering a web address, the personal information that you indicate as registrant and administrative contact will be made publicly available by INCC as required by the Internet's governing organization, ICANN.
- thisCompany *Mail* works with faxCo to make it easy for you to sign up for their free fax service. For your convenience, thisCompany will pre-populate a form with information you supplied in your account information. If you do not wish to send the information to faxCo, you can close the window and no information will be sent.

Practices Regarding Your Ability to Update or Delete Information

- You can modify your settings and preferences in your thisCompany *Mail* account by accessing "Options" or your thisCompany account information.
- You can cancel your *subscriptions* and edit or remove your *reminders* at any time.

Other

- When you use thisCompany *Mail*, you are subject to the ThisCompany Terms of Service and to the thisCompany *Mail* Guidelines.
- If you subscribe to a thisCompany *Mail* premium services, your use of that service will be subject to additional Terms of Service or guidelines you agree to, specific to those services.
- Please see thisCompany Mail Help if you have questions about this service.

This page describes current thisCompany practices with respect to this particular service. This information may change as thisCompany revises this service by adding or removing features or using different service providers. To find out how thisCompany treats your personal information, please visit our Privacy Policy.

thisCompany *Messenger*
thisCompany *Messenger* allows you to exchange instant messages with your online friends. You must be a registered thisCompany user in order to use thisCompany *Messenger*. thisCompany *Messenger* establishes a connection to the Internet when it is active -- much like a browser does -- in order for communications to be received and transmitted.

Information Collection and Use Practices

- In addition to registration information, you can establish a friend list within your *Messenger* and be added as a friend to others' lists.
- Unless you log in to *Messenger* using the "invisible mode," your online status will be visible to other thisCompany Messenger users who have you on their friends list. You can turn this off in your Profile Settings.
- Other users may also see your online status on web pages throughout thisCompany. You can edit your preferences so that others do not see you online at any time.
- You have certain choices about whether to add friends, be added as a friend, or ignore other users. When you invite someone to use thisCompany *Messenger* (as opposed to add someone as a friend to your friend list), you will be sent to a web page that asks for that person's email address, your thisCompany ID or alias, your real name, and a message (these last two are optional). thisCompany will not use your friend's email address for any marketing purpose and will only use this information to transmit your invitation.
- thisCompany does not save your messages, but we do make some functionality, such as archiving and the ability to print and save messages, available to users so that they may retain records of their instant messaging communications. Please be aware that even if you choose not to save your message history, users you correspond with may opt to use the functionality available in their version of *Messenger* to save the communications.

Information Sharing and Disclosure Practices

- thisCompany works with PhoneCo, thisCompany's phone service provider, to provide PC to phone calling through thisCompany *Messenger*. When you place a call through *Messenger*, thisCompany and PhoneCo record usage information, including the phone number that you dial, frequency of use and call duration. In addition, thisCompany and PhoneCo may use aggregate usage information for future product enhancements and for research purposes.
- By using thisCompany *Messenger*, you may choose to make some of your personal information public or you may choose to share some of your personal information with others.

- If you post personal information online that is accessible to the public, you may receive unsolicited messages from other parties in return.
- thisCompany *Messenger* sometimes uses a peer-to-peer connection during its operation, including times when you may be using it for instant messaging (text conversations), file sharing and webcam streaming. Peer-to-peer means that your computer connects directly to the other user's computer in the conversation without needing to go through thisCompany servers. As such, your IP address is available to users you share a peer-to-peer connection with.

Practices Regarding Your Ability to Update or Delete Information

- You can edit your thisCompany *Messenger* settings and preferences through the Edit menu.
- thisCompany *Messenger* automatically stores past phone numbers that you dialed through the Call Center. You may delete phone numbers from the Call Center at any time.

Other

- When you use thisCompany *Messenger*, you are subject to the thisCompany Terms of Service and to the thisCompany Community Guidelines.
- Please see thisCompany Messenger Help if you have questions about this service.

This page describes current thisCompany practices with respect to this particular service. This information may change as thisCompany revises this service by adding or removing features or using different service providers. To find out how thisCompany treats your personal information, please visit our Privacy Policy.