Anonymity Tools for the Internet

Brian Kim, Chris Laas, Shelly O'Gilvie, Alexander Yip
{kimb, golem, shelly_o, yipal}@mit.edu

May 17, 2001

Contents

1 Overview

The Internet, once hailed as a super-egalitarian forum for the masses, is increasingly dominated by powerful corporations and governments. Unfortunately, the architecture of the Internet makes it easy for such entities to covertly monitor users' behavior; so, as the imbalance of power increases, it will become more difficult for individuals to say what they feel, read what they want, and do as they please without fear of repercussions.

Anonymity is an enabler than can help to counter this influence: when a person can make statements unlinked to his own identity, his power to speak freely expands. In this paper, we first discuss a set of potential threats to anonymity. We then present an array of tools an Internet user could use to protect himself against these threats, and divide them into two categories: the nonfunctional, and the nonexistent. We cautiously suggest that the currently available suite of privacy tools may be adequate for a casual speaker, but would be ineffective against a determined and powerful adversary. In the next section of our paper, we lay out the legal framework for anonymity in the United States, and conclude that, while U.S. law protects anonymous speakers from governmental intrusions, there is no such assurance with respect to private entities.

In the final section of this paper, we present a corpus of situations in which anonymity might help preserve the rights of individuals. For each situation, we detail the risks and threats the Internet user faces, and suggest means by which the user could overcome those threats. In some cases, there currently are no good options available; for these, we outline the technologies that we believe would be necessary to provide an adequate level of protection. We hope that our corpus of threats and case studies will serve the dual purpose of helping individuals to secure their privacy in a way appropriate to their situation, and of guiding the creators of future anonymity tools, laying out the needs and constraints of their potential users.

2 Threat Model

2.1 The Person You're Talking To

Applications such as email, chat rooms, and message boards involve interacting with other people, some of whom might decide they want to know who you are. If you tell them your name, no amount of technology can protect your anonymity. More subtly, it is difficult for technology to filter out identifying information such as a "From:" header in email.

2.2 Local Threats

An oft-overlooked threat to anonymity is other people with physical access to the home node or computer, such as one's spouse or co-workers. For example, a person looking over your shoulder can often glimpse what you are reading or typing and potentially expose your identity, either knowingly or inadvertently. More generally, a technically competent person with physical access to your computer can install invisible tracking software which records every keystroke and action on the computer; the only way to counter this is to be careful with your passwords, and in extreme situations to use old-fashioned locks and keys to protect your computer.

2.3 Web Site Operators

Unlike reading a newspaper, browsing the Web involves making a specific request for every item of information retrieved. Logging the pages retrieved by users is standard practice for Web site

operators, and rarely are users, who often take for granted the greater level of privacy offered by print media, notified of this practice. Analysis of these logs, which is also aided by the existence of "cookies", allows operators to determine how long users view a particular page, how often they visit, and what they actually look at.

There is a whole industry hawking techniques for extracting information from unwitting Web browsers, but often the simplest methods give the best results. Some Web sites simply prompt users for personal information before allowing them to proceed onto the site. Others insert into their pages active code (such as Java or Java-script) which automatically transmits personal information to the Web site without asking for approval from the user.

Obviously, there is a wide range of information that can be gathered by website operators, depending on the means used. Usually, the information is used to build user profiles, which can then be sold or used to improve marketing strategies.

2.4 ISPs and other Network Providers

Everyone that uses the Internet must access it through some service provider; for most people, this is either their workplace, their school, or a commercial Internet Service Provider. Service providers have tremendous capability to monitor a user's activities online; simple logging mechanisms can record all in-bound and out-bound user traffic, such as email and Web page requests. This data can then be analyzed to determine what Web sites a user is visiting, who he or she is sending email to and receiving it from, and what he or she is saying. In a workplace setting, such information can lead to disciplinary measures; in a repressive regime, it could lead to jail time.

2.5 Network Infrastructure

The companies which form the backbone of the Internet have broad monitoring capabilities, much greater than a single ISP. This is tempered by the fact that they are unlikely to care about the content of the data piped over their wires and fibers, and it is inconvenient for them to wiretap or tamper with communications without significantly disrupting service. However, if pressed by law enforcement or the government (or perhaps by a suitable bribe), they can prove a powerful adversary, since together they can monitor virtually all traffic on the Internet.

2.6 System Crackers

System crackers (or, as they are often called, "hackers") pose another threat to online anonymity. Current computer systems are riddled with holes, and commonly available "rootkits" allow even marginally competent criminals to break into a significant fraction of computers on the Internet; many systems storing highly private or confidential information are poorly secured. While a hacker's main purpose may not be exposing the identity of a user, it is quite possible that they will publish or leak information that can be used for such purposes. More importantly, a system cracker in the employ of an adversarial company or government may uncover information outside the reach of bribes or governmental jurisdiction.

2.7 Network Attackers

Sophisticated attackers with significant technical ability can launch attacks on the network itself in order to determine more information on who is sending and receiving data. By eavesdropping on data, manipulating its flow by inserting or dropping data, and sometimes overwhelming links by

flooding them, it is possible to squeeze information (using techniques collectively known as "traffic analysis") out of even the most carefully-designed anonymity systems.

2.8 Number Cruncher

The most effective tools for protecting privacy and anonymity online are based on encryption, a set of mathematical techniques for obscuring information from everyone but its intended recipient. Encryption schemes in common use are generally safe from an average person with a PC, but their guarantees of security are not quite as iron-clad against an opponent with tremendous computing power. For example, the widely-used DES cipher can be broken by any organization willing to spend $100,000 on a custom DES-cracking machine. It's generally believed that strong, published ciphers with sufficiently long key lengths, such as Triple-DES, will withstand attacks by any computers currently in existence. However, we never know what the NSA has up its sleeve.

2.9 Powerful Corporation

In some industries, such as oil and tobacco, there are big companies with secrets to keep; the threat of whistleblowing might be sufficient to induce them to invest in heavy iron (big number crunchers), mercenary system crackers, and bribed network operators. Thus, even if what you have to say isn't likely to be interesting to script kiddies or sysops, you may still want to protect against a combined attack from these sources.

2.10 Nosy Law Enforcement

Law enforcement is often in the business of tracing identities. Through court orders, subpoenas, and warrants [1], the FBI can enjoy the benefits of cracking systems, without going to the trouble of learning how to do so. Wiretapping systems, such as Carnivore, give law enforcement network monitoring capabilities comparable to the network infrastructure providers themselves, with a willingness to use those capabilities not shared by the networking companies.

However, there is a positive side. While many Web sites, ISPs, and other system administrators have the ability to identify a particular user, they often do not do so unless they are obligated to under the law; in more liberal jurisdictions, there are restrictions on what information can be subpoenaed by law enforcement. In addition, cross-jurisdiction redundancy helps to protect anonymity systems from subpoenas and warrants.

2.11 Repressive Government

In a regime with little respect for human rights, there may be little restriction on what enforcers can do to extract information, nor on what information they can legally extract. This makes computers within that jurisdiction very vulnerable. For this reason, to protect one's anonymity in the face of such opposition, it is vitally important to distribute trust over computers which reside in multiple jurisdictions, at least some of which are not repressive.

3 Basic Anonymity Technology

Although the methods employed by anonymity tools range from the simple-minded to the bewildering, a few basic technologies — proxies, cryptography, and MIX-nets — form the basis of the majority of these tools.

Table 1: Threats to Anonymity. This table shows the threats included in our threat model, and names ways to protect against those threats.

Threat and Examples	Capabilities	Approaches and Tools
Recipient of communications (e.g. chat room participant)	Hears what you tell him	Be careful what you leak; there is no technological solution
One with access to your computer (e.g. spouse)	Physical access	Be careful who you trust; use passwords and old-fashioned locks and keys
Corporate Web sites (e.g. DoubleClick)	Access logs, cookies	Proxying, relaying: Anonymizer.com, Rewebber, Freedom, Crowds, Onion Routing Anonymous payment: Digicash, "InternetCash"
ISP or network provider (e.g. AOL, MIT, your workplace)	Eavesdrops on all in-bound and outbound data; can tamper, if inclined	Encrypt communications and use proxying and relaying (see above); also PGP and remailers.
Network infrastructure (e.g. VBNS, "The Internet Cabal")	Eavesdrops on and tampers with the entire Internet. "Traffic analysis"	Mix-nets: remailers, Rewebber, Freedom. Crowds, Onion Routing.
System Crackers (e.g. network vandals, professional hackers)	Breaks into machines	Maintain tight systems; distribute trust over multiple, diverse third parties.
Network Attackers (e.g. IRC hosers, network terrorists)	Network flooding, cutoff. Dropping or replaying data.	Type 2 remailers, redundancy (e.g. Publius, Freenet, Freehaven).
Number Cruncher (e.g. NSA, companies)	Slowly breaking encryption	Use stronger encryption and longer key lengths
Powerful Corporation (e.g. Big Oil, Big Tobacco)	Buy number crunchers, hire crackers, bribe network operators	Must guard against all of those threats
Nosy Law Enforcement (e.g. FBI)	Subpoenas and warrants — political "cracking". Wiretaps (Carnivore).	See above. Cross-jurisdiction redundancy helps; e.g. Freehaven, Freenet.
Repressive Government (e.g. China, USA tomorrow)	Compulsion, within jurisdiction	As with law enforcement, but it is vitally important to distribute trust over machines in other jurisdictions.

3.1 Proxies and Proxy Chains

The fundamental technology for anonymous communications is the proxy. Essentially, a proxy is a computer on the network (a *node*) which, if sent a message by another computer A, will forward the message on to a designated computer B on A's behalf.

A proxy is the most simple embodiment of an anonymizer, one that is not unusual in "the real world." Consider what Alice might do if she wants to tell Bob that Carol is plotting to kill him, but doesn't want Bob to know she told him. Alice might find Trent and say, "Hi, Trent. Could you please tell Bob that Carol is plotting to kill him?" Trent will then relay this message to Bob, without telling him the source of the message.

Such a technique has also been used on the Internet, but suffers from several shortcomings. One is that if Bob, or anyone else, overhears Alice speaking to Trent, Alice's anonymity is compromised. Another is that if Trent was not trustworthy or reliable, he might let slip that Alice was the original source of the message. In particular, Bob (or someone who overheard Trent speaking to Bob) might come back at Trent with a subpoena, or, if he's less civilized, a rubber hose.

This last concern can be mitigated via the use of proxy chains. Let's say that, instead of directly passing the message on to Bob, Trent passes the message on to Trudy, who passes it on to Ted, who finally passes it on to Bob. In this case, Ted doesn't know where the message originated, unless he overheard Alice talking to Trent; if Bob comes after Ted, Ted can at most tell him that the message came from Trudy. Likewise, Trudy can only point Bob to Trent. This improves Alice's anonymity, since now, to find Alice's identity, Bob has to get past three trusted parties rather than only one.

Unfortunately, this improvement still does not address the other concern: anyone who can eavesdrop on Trent can trace the message back to Alice. In practice, eavesdropping on digital communications is very easy, and so this is a real concern. To solve this problem, we must turn to cryptography.

3.2 30-Second Introduction to Cryptography

In general, cryptography is the use of mathematical tools to enforce trust relations between mutually distrustful parties. While this includes a broad range of esoteric protocols (such as the "digital cash" protocols discussed later in this paper), the most basic use of cryptography is to encode information such that it can only be decoded by the intended party. The "intended party" is distinguished by the fact that he knows a particular secret unique to himself, known as his "key".

The two forms of encryption in which we will be primarily interested are known as *symmetric cryptography* and *public-key cryptography*. In the public-key cryptography scenario, each individual generates a "key pair" consisting of a *public key* PK and a *secret key* SK, and releases the public key for all the world to know. If anyone wants to send a secret message M (called the "plaintext") to Alice, for example, they first encrypt M under Alice's public key PK_A, producing the "ciphertext" C:

$$C = PK_A(M)$$

They then send the ciphertext C over the network to Alice. Since Alice knows her secret key SK_A, she can retrieve the plaintext:

$$M = SK_A(C)$$

However, although anyone who eavesdrops on the conversation can learn C, they cannot learn M, since they do not know Alice's secret key.

In the symmetric cryptography scenario, there is only one key, used for both encryption and decryption. This key must be kept secret from everyone except the sender and the receiver.

3.3 Mixnets

Mixnets, first devised by David Chaum in 1981 [2], are the fundamental technology providing anonymity in Internet communications. While several advances have been made in mixnet technology since 1981, the basic concepts embodied by the Chaum's first mixnet design still prevail. The fundamental unit of the mixnet is what Chaum called a "MIX", a proxy which accepts messages encrypted in its public key, decrypts them, reorders them randomly, and passes them along to their destination, eliminating all evidence of their origin. Chaum also pointed out how to use chains of such MIXes to eliminate the reliance on a universally trusted third party.

A mixnet is a collection of nodes, usually individual computers on a network. All nodes have a public-key/secret-key pair whose public key is easily accessible and known to everyone. A node in the mixnet listens for encrypted messages; once it receives one, it decrypts the message using its secret key. The decrypted message reveals a chunk of ciphertext and instructions regarding to whom the node should forward the ciphertext. This process is followed at every node until the message is finally forwarded on to its final destination.

To clarify how this works, we'll use an example. Suppose there are two users, Alice and Bob, both with public-key/secret-key pairs. Alice wants to send anonymously a message, M, to Bob. First, Alice chooses a "chain length" N and selects a random set of N nodes from the mixnet; Alice is hoping that at least one of these nodes will turn out to be trustworthy. She then encrypts her message M with Bob's public key:

$$C_B = PK_B(M)$$

She then takes the newly-created ciphertext C_B, prepends the instructions "Please send this to Bob," and encrypts the result with the public key of the Nth mixnet node, M_N, in her chain. She now has produced the ciphertext:

$$C_N = PK_{M_N}(\text{"Please send this to Bob"} + PK_B(M))$$

Alice then prepends the instructions "Please send this to M_N" to the newly created ciphertext and encrypts *that* with the public key of the $(N-1)$th node:

$$\begin{aligned} C_{N-1} &= PK_{M_{N-1}}(\text{"Please send this to } M_N\text{"} + C_N) \\ &= PK_{M_{N-1}}(\text{"Please send this to } M_N\text{"} + PK_{M_N}(\text{"Please send this to Bob"} + PK_B(M))) \end{aligned}$$

She then continues this process of adding routing instructions and re-encrypting until she has gone through all the nodes in the list she has selected. The final result is a piece of ciphertext whose structure looks like this:

$$\begin{aligned} C_1 = PK_{M_1}(&\text{"Please send this to } M_2\text{"} + PK_{M_2}(\text{"Please send this to } M_3\text{"} + \ldots \\ &+PK_{M_N}(\text{"Please send this to Bob"} + PK_B(M))\ldots)) \end{aligned}$$

Note, of course, that to anyone except node M_1, this ciphertext is as unintelligible as a string of random data.

Alice now sends this encrypted chunk of data to node M_1, which decrypts the message using its secret key SK_{M_1}, reads the instructions "Please send this to M_2", and obediently forwards the enclosed ciphertext to node M_2. Node M_2 then decrypts the message and, likewise, forwards the enclosed ciphertext to node M_3, and the process continues. When the message reaches the final node M_N, it forwards the ciphertext on to Bob, who then decrypts the message (using his secret key SK_B) and reads it.

When a message is sent through the mixnet in this fashion, any given node in the chain knows the previous node and next node in the chain: it knows the previous node since it received the message from the previous node, and it knows the subsequent node because its name is encoded into the forwarding instructions. However, since the message is successively encrypted with the public key of each node, each node can only read what was meant for it to read, at that particular layer of encryption. It cannot predict, or even determine after the fact, to which node the next node forwards the message, since the next node will peel off another layer of encryption before forwarding it along.

Mixnets allow us to fully realize the promise of proxy chains: even if an adversary compromises all but one of the nodes in the chain, and has the ability to read every message on the network, he still cannot link incoming messages with outgoing messages for the uncompromised node. This unlinkability, afforded us by the use of public-key cryptography, ensures that Alice's identity is secure so long as any one of the nodes in her chosen proxy chain is trustworthy. Thus, the mixnet chain is as strong as its strongest link, in terms of security.

The robustness of mixnets leaves something to be desired, however. In terms of robustness, a mixnet chain is as weak as its weakest link — if one node in the chain fails to forward the message, it will get lost. Since Alice has no way to determine whether Bob received her message, short of sending him a message *outside of* the mixnet, this poor robustness leads to a security shortcoming as well.

Furthermore, mixnets do not seem to scale well in practice. When the set of nodes expands beyond a small set of administrators who know each other personally, there tend to be problems with reliability and free-loading, and there is no authority ensuring that mixnet nodes behave according to the protocol. In general, mixnet nodes do not have good uptimes [3].

Finally, there exists a rather difficult trade-off between security and performance in the case of traffic analysis. More sophisticated mixnets incorporate random delays in the forwarding algorithm; without these delays, traffic analysis by an eavesdropper can rather trivially restore the linkage between sender and receiver, simply by following a message through the network. (If the delay through a node is one second, then simply match up the incoming message with the outgoing message one second later.) However, adding random delays at each hop results in a significant end-to-end delay; for some applications, it can take hours or even days for a message to propagate through the mixnet. This makes such highly-secure mixnets rather impractical for use in interactive applications such as Web browsing or online chat rooms.

3.4 Mixnet Reply Blocks (Brian)

As described above, mixnets solve a fundamental problem of anonymity: how does A send a message to B without B's figuring out who sent the message? However, now that that problem's solved, we are left with a new problem: how can B reply to A's message, given that he doesn't know how to reach her?

Let's take again our situation with two users, Alice and Bob. Alice has sent a message anonymously to Bob using a mixnet chain. If Alice wants to be able to receive a reply back from Bob

without revealing her identity, she can include what is called a *reply block* in the body of her message.

To create a reply block, Alice again chooses a chain length N, and randomly selects a set of N nodes from the mixnet. Suppose, in this case, N is three. Alice first encrypts her real address and a randomly generated symmetric-encryption key K_1 with the public key of the first remailer. She now has the following:

$$C_1 = PK_{M_1}(\text{“send to Alice”}, K_1)$$

She then prepends the address of M_1 and another symmetric key, K_2, to the above cyphertext and encrypts that with the public key of second remailer:

$$C_2 = PK_{M_2}(\text{“send to } M_1\text{”}, K_2, PK_{M_1}(\text{“send to Alice”}, K_1))$$

Alice then prepends the address of the second remailer and a new symmetric key, K_3, and encrypts *that* with the public key of the third remailer.

$$\begin{aligned} C_3 &= PK_{M_3}(\text{“send to } M_2\text{”}, K_3, C_2) \\ &= PK_{M_3}(\text{“send to } M_2\text{”}, K_3, PK_{M_2}(\text{“send to } M_1\text{”}, K_2, PK_{M_1}(\text{“send to Alice”}, K_1))) \end{aligned}$$

Alice finally constructs her reply block:

$$RP_A = (\text{“send to } M_3\text{”}, C_3, PK_A)$$

Alice can attach this reply block to any anonymous message she sends out; anyone who gets the block will be able to send messages to her using it, despite the fact that they need not know her true address. The procedure for doing so is as follows.

Let's say Bob wants to send Alice a reply message using the reply block RP_A he received in the message from Alice. He first encrypts his message M in Alice's public key:

$$C_A = PK_A(M)$$

He then prepends the value C_3 to the ciphertext, giving the pair (C_3, C_A), and sends it to M_3 as per the instructions in the reply block.

When the third mixnet node receives the above message, it decrypts it using its secret key SK_{M_3}, getting an address M_2 and a symmetric key K_3. It cannot read the message, because it has been encrypted in Alice's public key, and it cannot read the rest of the reply block, because it has been encrypted in M_2's public key.

$$SK_{M_3}(C_3) = (\text{“send to } M_2\text{”}, K_3, C_2)$$

M_3 encrypts the body of the message, $PK_A(M)$, using the symmetric key K_3, resulting in the following message pair:

$$(C_2, K_3(PK_A(M)))$$

It forwards this pair to M_2, as per its instructions. Upon receipt, M_2 decrypts C_2 using its secret key, getting:

Table 2: Summary of Internet anonymity tools. This table shows the basic technology behind the tool, its target audience, benefits and drawbacks.

Tool	Technology	Audience	Benefits	Drawbacks
Remailers	Strip/forward email chains	Internet savvy users interested in very anonymous communication	Good anonymity if many remailers used	Unreliable, Difficult to configure
ZKS Freedom	Packaged privacy solution	Basic web user	Easy to use, Provides basic anonymity	Single point of weakness: ZKS
Freehaven	Peer to peer anonymous publication	Internet savvy users interested in very anonymous publication	Persistent storage, anonymity for writer, server, reader	not implemented
Digicash	Blinded coins	Anyone interested in fast, anonymous, online payment	Fast, Anonymity for payor	Not widely accepted
InternetCash	Prepaid debit cards	Anyone interested in fast, anonymous, online payment	Fast, Basic anonymity for payor	Not widely accepted, Geographic and card linkable

$$SK_{M_2}(C_2) = (\text{“send to } M_1\text{”}, K_2, C_1)$$

M_2 then further encrypts the body of the message using K_2, and forwards the result on to M_1:

$$(C_1, K_2(K_3(PK_A(M))))$$

Like the others, M_1 decrypts the reply block, giving it Alice's address and the last symmetric key K_1, and encrypts the body of the message with K_1. M_1 sends the following to Alice:

$$K_1(K_2(K_3(PK_A(M))))$$

Since Alice originally generated K_1, K_2, K_3, and PK_A, she can decrypt this message to retrieve M. Our final result, as we hoped, is that Bob can send a message to Alice despite his lack of knowledge regarding her true identity and address.

4 Anonymity Tools

In this section we will describe a number of existing and theoretical anonymity tools. We evaluate them according to how they work, who they are targeted towards, what their benefits are, and what their drawbacks are.

4.1 Remailers

4.1.1 Technology

Proxying tools used for anonymizing email are known as "remailers". The first remailers, now called Type 0 remailers, were simple proxies: users simply sent mail to the remailer, which would strip off the mail's headers and forward the message on to the intendend recipient. Reply functionality was implemented in terms of pseudonyms. The remailer stored a fixed mapping from pseudonyms (such as "an024601@anon.penet.fi") to real addresses (such as "alice@mit.edu"); if a message was sent to the anonymizer with an envelope address like "an024601@anon.penet.fi", the anonymizer would translate the address using its secret mapping, and then forward the message on to the real address.

This type of remailer system, which uses only one proxy, suffers from a single point of failure: users must trust that the remailers won't be compromised, and won't divulge any information from its secret table of pseudonyms. The original Type 0 remailer, `anon.penet.fi`, was compromised in 1995 when the Church of Scientology succeeded in convincing a Finnish court to order the remailer's operator to expose the true email address of a user.[4] When this happened again, Julf Helsingius, the operator of the remailer, decided to shut it down rather than continue to jeopardize the anonymity of his users.

To address this issue, the denizens of the *cypherpunks* mailing list designed a new type of remailer, commonly called Type 1 remailers or simply cypherpunk-style remailers. Type 1 remailers implement a standard mixnet: remailer chains prevent the single point of failure, and the use of cryptography prevents eavesdroppers from linking incoming and outgoing messages.

Although there's been no publicized compromise of Type 1 remailers, they suffer from weaknesses that could allow an eavesdropper to link incoming and outgoing messages. For example, since there is no delay between the time a Type 1 remailer receives a message and the time it forwards it on, an eavesdropper who can listen in on the connections between remailers could easily follow a message through the network, bypassing the encryption entirely. The Type 2 remailer, or "mixmaster" remailer, attempts to counter this and other "traffic analysis" in several ways [5]:

- To prevent the attack outlined above, Type 2 remailers add a random delay in between receiving and forwarding messages.
- To prevent eavesdroppers from linking messages by observing their size, Type 2 remailers only forward messages of a fixed size.
- To prevent eavesdroppers from linking messages simply by the order in which they arrive and leave, Type 2 remailers collect batches of messages, randomly reorder them, and then forward them on.
- Finally, another possible attack for an active adversary is to store an overheard, targeted message and replay it to the remailer. To determine what outgoing message corresponded to that incoming message, the adversary need only note which message is repeated on the output. To counter this attack, Type 2 remailers detect when a message is repeated, and will only forward it once.

Type 1 and Type 2 remailers support replies and persistent pseudonyms through the use of reply blocks[6]. In particular, systems such as `nym.alias.net` store a mapping between pseudonyms (addresses like "foo@nym.alias.net") and reply blocks; mail sent to the psuedonym is automatically sent through the mixnet using the reply block. This is a significant improvement over the Type 0

Table 3: Remailer Types and Characteristics.

Type	Characteristics
Type 0: anon.penet.fi	Keeps table of nyms and real email addresses Single point of failure/exposure
Type 1: cypherpunks	Have public keys used to encrypt incoming messages Message can be sent through chain of remailers Can provides anonymous email address through use of reply blocks
Type 2: mixmaster	Has all the features of Type 1, plus: Fixed size messages Batching and reordering Replay detection User-specified random delays through each hop

pseudonym design, because if `nym.alias.net`'s list of reply blocks is compromised, it is still not possible to link a pseudonym with a real address without compromising every remailer in the reply block chain.

4.1.2 Audience

The potential audience for remailers is vast, since email remains one of the most popular Internet services; also, email can be interfaced to other services, such as Internet newsgroups (or bulletin boards). However, depending on the type of remailer, some degree of technical competance may be a prerequisite for use.

Type 0 remailers are attractive to novices because they are very easy to use: a single command sets up a pseudonym, and sending and receiving anonymous email is as simple as sending mail to the proxy. However, Type 0 remailers' security flaws make them a poor choice, in general.

Type 1 and Type 2 remailers are somewhat more difficult to use: the instructions for creating remailer chains and reply blocks may seem esoteric to novices, require knowledge of the current state of the remailer network, and require mastery of PGP. There exist software tools, such as "premail" and "Private Idaho", to make the process of using remailers more convenient, but they are in general poorly supported and maintained. This state of affairs is slowly improving, however.

4.1.3 Benefits

When used correctly, Type 2 remailers are probably currently secure against all but the most determined adversaries. Casual correspondants and most corporations are unlikely to have the resources to mount a traffic analysis attack on many remailers. Likewise, since the incoming and outgoing messages are encrypted, one's network provider can't easily trace one's messages. Probably most importantly, the compromise of a small number of remailers does not compromise any users' anonymity; this gives remailers a fair bit of immunity against subpoenas, bribes, and hackers.

4.1.4 Drawbacks

Type 0 remailers, although the easiest to use, are generally considered fairly useless: there have been demonstrated legal and network attacks against Type 0 remailers. Unfortunately, the more secure Type 1 and Type 2 remailers also require more sophistication on the part of the user, and have also been generally less reliable, due to the poor uptimes of some remailers[1].

Type 1 and Type 2 remailers remain subject to several potential attacks; although they have not been demonstrated yet in real life, there is little doubt that they pose a serious threat to users of these systems. Type 1 remailers are susceptible to attacks by the network infrastructure providers, or anyone who can convince, bribe, or compel the operators of the network to cooperate to reveal a user. A system such as Carnivore, if widely deployed, could allow the government to trace the identity of a person sending an anonymous message through a Type 1 remailer chain. Although Type 2 remailers mitigate this problem somewhat, it is very difficult and inconvenient to use them; since one's level of anonymity is, essentially, inversely related to the number of people using the service, this negatively impacts the security of Type 2 remailers. In addition, Type 2 remailers remain vulnerable to active attacks. Although such active attacks would be unlikely to be used by, for example, the FBI in today's United States, it's not very difficult to imagine them being used by China or Texaco.

Finally, all proxy chains are susceptible to a social attack: if all the nodes in a chain can be compromised, the chain can be traced. This is not as farfetched as it may seem. If all remailers in someone's reply block reside in the United States, as is not unlikely, it would not be overly difficult for the FBI to subpoena each remailer, one after another. Likewise, remailers are generally run by poor grad students; if each one can be bought for $10,000, a company may be able to buy a chain of three to five remailers more cheaply than it can buy a number-crunching machine or pay for a lawsuit. In general, there currently exist no good solutions to this issue; for maximum anonymity, users should use long mixnet chains consisting of machines in different jurisdictions and maintained by reliable operators.

4.2 Zero Knowledge Systems Freedom 2.x

Zero Knowledge Systems, a company seeking to become the leader in privacy solutions for the Internet, is currently marketing a general-purpose Internet anonymity software suite named Freedom. Services anonymized by Freedom include email, Web browsing, chat rooms (e.g. IRC), monetary transactions, and remote logins (e.g. telnet and SSH). Freedom 2, unlike the first version, attempts to sacrifice quality of anonymity protection in exchange for scalability, efficiency, reliability, and speed, a tradeoff which ZKS plans to justify via an analysis of their threat model in an as of yet unpublished white paper[7]. In this section, we explain the difference between the levels of anonymity offered by the previous and current versions of the system, assuming equal weighting of stress on all components of the system. We also discuss the vulnerabilities posed by the current system's almost complete dependence on the anonymity of the "nym". As further background, we outline the ideas behind the anonymity of the "nym". We also explain to what extent the system, given its capabilities, meets the threats outlined in our model.

4.2.1 Technology

The key elements of Freedom 2 are Anonymous Internet Proxies (herein referred to as AIPs), which perform relaying services to transport data anonymously, and the Freedom Core Servers, which

[1] However, some systems, such as nym.alias.net, are currently attempting to address the issue of reliability.

provide basic services. Each of the nodes are administrated by ZKS or by various ZKS-approved third parties, such as ISPs. The key server software running on a node is the AIP daemon, the NIQS daemon, and various administration and management utilities. The node operator generates a public-key/private-key pair and submits the public part to ZKS for distribution; due to this structure, only the appropriate nodes can decrypt the layers of encryption intended for them. ZKS never sees the secret keys; this becomes important later, when we discuss clients' options for traffic routing and nym anonymity. AIPs forward packets amongst themselves until an exit node is reached; Web sites and other hosts can only see that queries come from the system, and cannot determine their origin.

The Freedom client-side software allows applications to access the Internet through the Freedom System. It consists of: a graphical user interface, a network access layer, traffic filters, application filters, and a set of libraries responsible for anonymous computing functions (routing, encryption, etc.). Freedom 2 currently supports the following application protocols: SMTP, HTTP, POP, SSL (although it cannot decrypt the communications to filter them), IRC (although not DCC), Telnet, SSH, and NNTP (although only for posting; reading on the Usenet currently has to be done on the web). By "support", it is meant that the traffic and application filters allow these to function as if there were nothing between it and the user. For example, protocols such as SMTP and HTTP often implicitly reveal information about the user, and the filters fix this without interfering with the function of the protocol. It is also important to note that the system itself comes with a premium package as opposed to a mainstream one. The prior allows for traffic to flow through an authenticated route signed by the nym, the AIP retrieves the public key and then verifies the request. The difference between this and the latter unauthenticated route is that authenticated users have access to the entire system whereas the unauthenticated nym has access only to main nodes.

The Freedom 2.x system is a replacement, rather than an upgrade, of Freedom 1.x. Some of the key differences compromise anonymity for usability and scalability. In the previous system the AIPs used fixed size packets and cover traffic to counter traffic analysis. In the current system both of these features were excluded, in order to reduce wasted resources and improve efficiency. The obvious problem here is the improved capability for those doing traffic analysis. As it exists it is already possible for an eavesdropper to monitor a node and see whether or not someone is using the Freedom network and based on the size and spacing of the packets, draw conclusions as to what the system is being used for at that point. This information would most likely be of use only for investigative purposes by law enforcement or national intelligence and is at any rate a difficult problem to solve. In the previous system the AIP was not capable of transporting ICMP traffic and now support is available for some. This adds to the list of things that would cause a problem if the system were somehow compromised. As it is it does not pose a direct threat and the user has the added bonus of being able to ping anonymously. The Freedom 1.x network was also more distributed than Freedom 2.x. Freedom 2.x has a single network and a single domain for nyms. The purpose of this is to make the network scalable to larger numbers of customers. This requires more user trust in ZKS instead of distributed trust. Someone is more likely to collaborate with himself than with others. Also, in the process of creating a next generation mail handler, Freedom's reply-block system has been replaced by a POP box-based mail system in order to provide faster and more efficient e-mail. The POP has not improved or compromised security. The reply-block system required passing mail amongst servers, which could cause problems if a node in the chain was not functioning properly. For the purposes of browsing, this is matter of re-querying, but it can be a frustratingly slow process for e-mail. Among the plusses for this new system are that it is free from the threat of law enforcement, that is to say, it is un-subpoenable because mail is

not stored in ISP accounts; this also helps reduce the ISP threat[8]. However, users must interact separately with each nym to avoid the possibility of tracking by ZKS. Another minus is that it is possible for ZKS to learn who (what nym) sent mail to whom and when.

Due to the changes in the system, maintaining the anonymity of the nym, especially from ZKS itself, is even more important than before. The anonymous creation of a nym is facilitated by a system consisting of a credit card or cash payment mechanism, an untraceable currency subsystem, and a nym purchasing subsystem [9]. The inherent flaw in paying for ZKS product with a credit card is that it leaves identifiable information lying around somewhere in the hope that no one is capable or will desire to uncover it. Exchanging encrypted codes online and of course getting the cash to ZKS facilitate cash transactions. Activation codes (analogous to traveler's cheques), as well as encrypted nym tokens, make up the untraceable currency system eventually used to purchase the nyms. The nym tokens are then exchanged for nyms. The inherent weakness in this is that ZKS must be trusted not to do several things: store IP addresses (although this can be mitigated by using a public computer, such as at a library, to establish payment codes), intercept your cash payment envelope (if paying by cash) and do a DNA analysis on the spit used to seal the envelope, or record any association between activation codes and nym tokens. Nyms can also be deactivated by simply canceling the private keys' ability to communicate with Freedom servers; thus, connection and disconnection can be accomplished without knowing anything about the user except for the nym.

4.2.2 Threats that ZKS meets

Corresponding party: As far as protecting user identity for correspondences online the Freedom system salable point is in the "untraceable" nyms that users are provided with. With each nym it is up to the user to fill in their false profiles and so the real threat in this situation comes from the user themselves and their decision on whether or not to disclose real or personal information during online correspondence.

Local Threat: Because ZKS offers no means of blocking non-account holding users of the same computer from viewing files and information it is up to the user to protect their nyms and data from other users of their computer.

Website operators: One of the free features of the Freedom 2.x system is a cookie manager. The Cookie Manager allows you to keep track of your cookies and separate them into separate folders that send your nym's info out when necessary. In order to prevent unnecessary tracking that does nothing to enhance to browsing the experience, for example by an ad server like DoubleClick.net, the Ad Manager, also standard, blocks all HTTP requests to ad servers so that they neither receive requests nor cookie information. This prevents web-based tracking and improves download time[10]. ZKS currently has no effective means of addressing the problem of Javascript data collection but this option can be turned off on a user's browser.

ISPs and Sysadmins: Mail under the Freedom system is protected from ISPs and sysadmins because it is not stored on their accounts. Also, because Freedom works on top of the Internet ISPs would have to employ active attacks on users to analyze fully their usage. Although they can see that a user is using Freedom and can make general assumptions through traffic analysis. Assuming the anonymity of the nym is not compromised, the ISP or sysadmin should not be able to identify users on the network, but there are ways for users to blow their cover, namely: changing nyms while browsing, and forwarding e-mail from one nym to another (this makes it extremely difficult to say that the two nyms are unrelated).

Hackers: having nyms that provide websites with false information is the method that Freedom

provides to protect against required information falling into the wrong hands.

Network Attacker: The threat of a network attacker is still a problem for Freedom in that the few protections against traffic analysis have been removed for efficiency and scalability's sake.

Computational Attackers: considering the fact that increasing the bits in an encryption key exponentially guards against cracking at least by brute force method, it seems highly improbable the Freedom would not be able to add bits to its encryption codes faster than decryption technology advances.

Law enforcement: the threat posed by law enforcement is covered in the same way as the threat by ISPs and sysadmins since these are the routes that law enforcement agents go through to gather information.

4.2.3 Audience

The target audiences of this product are businesses and individuals seeking one-stop anonymity shopping. Due to the small flaws in the system's ability to offer complete and reliable coverage, the user would have to be looking to compromise on things like less security for more speed and an all-in-one package for having to trust a third party with some information.

4.2.4 Benefits

This tool overcomes some of the basic threats to anonymity. It overcomes the threat of someone a client might send e-mail messages to, and to websites but not necessarily to online retailers if the clients purchase on the site because online transactions are not anonymous at least not with this tool alone.

4.2.5 Drawbacks

In some ways Freedom is susceptible to statistical traffic analysis, but in general network eavesdroppers cannot glean personal information from traffic analysis. Freedom addresses the threat from law enforcement in that the Freedom Network is fairly distributed enough in that individual ISPs cannot track a person down. This is not foolproof, however, because of the fact that somewhere along the line client information was taken by a third party to issue ZKS tokens and both this third party and Zero-Knowledge had to be trusted to not be logging IP information during these transactions. As for the threat from someone who could factor large primes the encryption on e-mail and web communications are strong enough, assuming that their computing technology is not years and years ahead, it would not likely be worth the trouble. The user is still vulnerable to a few things. The tool by itself does not protect the user from someone who has access to his or her computer at home. Also, there remains the small threat of law-enforcement, the third-party billing agent and Zero-Knowledge all teaming up together to track down the client.

4.3 Freehaven

Freehaven is an anonymous publishing system which was intended to provide "low profile", permanent, anonymous storage.[4] [11] The agents involved in the system are the publisher, the server, and the reader. The community of servers that compose Freehaven are referred to as the "servnet". Freehaven was designed to protect anonymity of the author, publisher, reader, server, document, and query.[2]

[2]Query anonymity means that a server does not know the identity of a document that it is serving.

4.3.1 Technology

Each server in the servnet has a public key and at least one reply block. All communication in Freehaven, between users and servers and between actual servers themselves, is done through mixnets, via reply blocks.

When a user wants to publish a document on Freehaven, he must first find a server that is willing to store it. When a server receives a new file to store, it first uses Rabin's information dispersal algorithm (IDA) to break the file into n shares, where only k shares are necessary to recreate the document. The selections of the numbers n and k can be determined by the user; a large value of k relative to n makes the file more "brittle", meaning that only a few pieces can be lost before the file is unrecoverable. However, a small value of k means that the shares will be larger and additional storage will be needed. Once the document is broken up into shares, the server that has agreed to store it generates a public-key/secret-key pair for the document and digitally signs each share. The shares are then stored on the server as new data. Attributes of each share include a timestamp, expiration date, public key, information about share numbers, and a signature of the document.

When a user wants to retrieve a document from Freehaven, she must first discover the public key that was used to sign the document, because Freehaven indexes documents by the hash of the document's public key. The reader then generates a one-time-use public-key/secret-key pair and a reply block for the request. The server requesting the document on the behalf of the user then broadcasts the request, which is composed of the hash of the document's public key, the user's public key, and the user's reply block, to all other servers that it knows. All recipients of the request then check their shares to see if they have any documents signed with the appropriate secret key. If they do, they encrypt the share with the user's public key, and send it back to the user via the reply block that was received in the request. Once enough shares have been received by the user, the document can be recreated.

An important aspect of Freehaven is the trading of shares. While there are several reasons why this is done, two of them are relevant to anonymity, while the rest mainly concern system robustness. The first aspect that helps anonymity is that trading helps cover publishing. It cannot be assumed that a server trading a share is also the publisher of the share. Second, it helps obscure where the shares for a document are stored. This means there is never a static target to attack in order to remove a document from Freehaven. The other reasons for trading, mainly concerning system design, are to better allow for servers joining and leaving the servnet, to accommodate operator concerns for storing documents, and to help allow for longer expiration dates.

The frequency of trades is a parameter set by the server operator. The cost of trades is measured using a "size $\times$ duration" metric: if a server had a 2 megabyte file that had to be stored for 2 weeks, it would consider trading it for another share that was 4 megabytes and had to be stored for 1 week. A four-way protocol involving "receipts" is used to perform the transaction of trades, but this is not relevant here.

All shares have an expiration date that is chosen by the publisher at creation time. While the publisher has the ability to set an expiration date very far into the future, he must also consider that doing so will make it more difficult to find a server willing to store the document. In addition, there is no ability to revoke documents in Freehaven once they have been published; this was a conscious design decision, made to avoid people being coerced into revoking the document. Both of these measures add to the permanence of document storage on Freehaven.

One important aspect of the permanence of documents on the servnet is called the "buddy system." When shares are created by the publisher, pairs of shares are associated together. Each

member of a pair is kept updated with the location of the other pair, particularly through trades. While this helps increase the robustness of document lifetime, it also helps provide a mechanism for server accountability which can be used to determine whether a server is abiding by its Freehaven agreements.

The last significant aspect of Freehaven is its "reputation system" for accountability. Each server maintains ratings for all other servers that it has transacted with or "heard" about, through broadcast messages sent after transactions have been completed. Ratings are computed and stored that attempt to measure a server's reputation and credibility. While this technology is still highly experimental, it is still important to acknowledge that it is a part of the Freehaven design.

4.3.2 Audience

Freehaven was designed to provide anonymous, long term storage. Due to efficiency issues that arise from the use of remailer chains as the primary means of communication, the system is not intended to handle the same volume of requests as a typical Web server. Once a request for a document has been sent out, it may be hours, or even days, before the document is received. [3] Second, Freehaven is designed for storing content that would not otherwise survive on other systems, which preserve documents based on popularity. Systems such as Freenet and Mojo Nation would quickly drop an unpopular document, whereas Freehaven would guarantee storage up until the document's expiration date[12] [13]. This fact makes Freehaven a valuable tool for people who are worried about having their document somehow flushed out of the system.

4.3.3 Benefits

The careful design of the Freehaven system makes the list of benefits fairly long. We will only list the relevant ones here. First of all, because the IDA algorithm is used to break documents into shares, very concerned users can store documents with fairly high reliability by selecting a small value for k. This provides protection against several system failures or anomalies at the server level because it would require several servers to be lost before the document is no longer available.

Freehaven also provides "plausible deniability" for server administrators. Since documents are not stored in a readable form on the machine, due to the fact that they are only encrypted shares, administrators have no way of knowing what is being stored on their machine. Being able to avoid legal issues gives people more incentive to run a Freehaven node.

Freehaven also provides many mechanisms for protecting against rogue servers. The buddy system coupled with the reputation system helps servers keep track of who is misbehaving in the system and thus limiting the damage that can be done.

4.3.4 Drawbacks

There are several drawbacks to Freehaven. First, it is not a deployed system. The current implementation only suffices as a "proof of concept" and cannot be used at this time. Second, there are several inefficiencies that need to be addressed in order to make the system more reliable and useable. The use of remailer chains for communication has been found to be very slow and also unreliable. While the slowness can considered acceptable for a system that attempts to provide anonymity for all agents, the unreliability isn't. In addition, the use of broadcasts when performing queries is also a source of inefficiency that needs to be addressed before the system can be widely deployed.

[3] Reply blocks may specify a random delay at each hop.

It is also important to consider that Freehaven does not guarantee anonymity. It does an admirable job in protecting anonymity and foiling most attacks, but there are still some very sophisticated custom attacks to which it remains susceptible. However, these attacks are so sophisticated and require great enough control over the network that very few people or agencies could perpetrate them.

4.4 Digicash

Digicash is a system based on the David Chaum's blinded digital coin[14]. It allows for digital payments issued by a supporting bank. Coins are issued to payors and can be used to pay other parties. The payee can then redeem these coins for real currency without revealing who the payor was. This section will outline the technology behind the Digicash system and the audience it is targeted towards. It also explain some of its benefits and drawbacks.[15]

4.4.1 Technology

Suppose Alice would like to buy digital coins from her bank. She chooses a denomination and n large random serial numbers. She then combines the denomination with the random numbers to create the n serial numbers. She then multiplies each by a blinding factor to create the n blinded numbers and then sends all n blinded numbers to her bank.

Her bank chooses one of these blinded numbers, and asks Alice to surrender the serial numbers for the other $n-1$ blinded numbers. She does this, and the bank exposes the denominations hidden in these blinded numbers. If all of the denominations match, the bank can assume Alice is being honest about the denomination of coin she is buying.

Her bank signs the unexposed blinded number with the bank's secret key and returns it to Alice. At this point, Alice has a number which has been signed by the bank, and the bank knows that Alice purchased a coin of a certain denomination, and the blinded number Alice gave to the bank.

Now, Alice can perform a special mathematical operation on the coin and remove the blinding factor. The operation is designed so that after the blinding factor has been removed, the signature is still intact for the original serial number chosen by Alice. Alice can now pay someone with her signed coin.

Alice pays Bob with her new digital coin. Bob takes the coin to the bank, and the bank authenticates the coin. The bank then checks to see if this coin's serial number has been redeemed in the past. If the coin has not been encountered before, it is added to the redeemed coin list, and Bob gets a credit to his account. If the bank *has* seen this coin before, it rejects the coin as being double spent. The bank can also analyze the two spent coins, and discover who tried to spend it twice. If Bob has tried to redeem the coin twice, the bank will discover this. Also, if Alice tried to spend this coin twice, the bank will discover Alice's identity. With this ability to expose double spenders, blinded coins are a viable solution for anonymous spending.[16]

Note that Bob does not need to take the coin to the bank right away. He can wait until the end of the day, or the end of the week and deposit all of his coins at once. Batching these transactions makes it possible to cut down on transaction overhead. This is made possible because if Alice tries to double spend, her identity will be exposed, and she can be punished for double spending. Reducing single transaction overhead makes it possible for digital cash to be used for micro-transactions for values less than a cent.

4.4.2 Audience

Digicash's target audience consists of just about anyone who would like to speed up monetary transactions. Not only do blinded coins give payors anonymity, but it also makes it easier and faster for anyone to exchange currency. The anonymous aspect of digicash appeals to consumers who would like to protect their identities. It would also to appeal to retailers who might increase sales by selling to these concerned customers.

4.4.3 Benefits

The benefits of this system are pretty clear. Payors are given an anonymous payment method that can be executed over the Internet. The bank cannot track what consumers are purchasing, and sellers cannot discover their customers identities. In addition, transactions can be completed automatically, and instantaneously.

Another benefit is that digital cash can be for normal monetary transactions or can be used to transfer very small amounts on the order of a fraction of a cent. The properties of Digicash that make these micro-transactions possible is the automation of the transaction, and the possibility of offline clearing. Such a technology may prove very useful in the future if pay-per-view websites or small licensing fees become popular. Digital cash would enable users to pay for such things without exposing their identity.

If digital cash is built and used for the same transactions credit cards are used for, the technology should scale very well. Current credit card companies already perform online clearing; the only additional processing would be the issuing of digital coins. Digital cash issuers could encourage or force users to buy coins in batch, so that they do not cause over burden on the system by asking for one coin at a time. The additional load of issuing coins should not be a problem in the scaling of digital cash.

With respect to anonymity and the threats in Table 2, Digicash performs quite well. Corresponding parties, the website operators, ISPs, law enforcement officials, and network attackers should not be able to identify a spender.

4.4.4 Drawbacks

One particular drawback of the Digicash solution is that large transactions may become very difficult to detect. In addition, these transactions would protect the identity of the payor. These properties make it a good medium to conduct illegal business with. Crimes such as money laundering and tax evasion could become much easier with the widespread use of blinded coins. Obviously, government and law enforcement agencies may attempt to limit or ban the use of Digicash for this reason.

Another drawback is that payees need to change their systems to support digital cash payments. This will take a lot of effort, and will take time. Currently, very few, if any merchants accept any kind of digital cash solution.

With respect to anonymity and our threat model, Digicash cannot protect against very strong opponents or local threats. The hacker or computational attacker may be able to identify the spender by somehow uncovering the blinding factor. They could accomplish this by infiltrating the spender's computer system or by some kind of brute force key attack. The local threat is also a vulnerability in this case, but it would be difficult and maybe impossible for a digital cash system to protect a user against people looking over his shoulder.

4.5 InternetCash.com

InternetCash.com is company that sells anonymous debit cards. The cards can be purchased in convenience stores, and can be redeemed at various online retailers. Their goal is to provide a means for anonymous payment.

4.5.1 Technology

The technology for InternetCash cards is very simple. The cards act much like prepaid phone cards. Each card represents a balance, and every time a customer uses the card to buy something, the account is debited.

4.5.2 Audience

InternetCash is targeting consumers who are concerned with their anonymity when they purchase things on the web. Another party who may find this technology useful is people who are purchasing things for illegal means. Although this group may not be the targeted audience, the option will arise for criminal use of these debit cards.

4.5.3 Benefits

Some of InternetCash's benefits are that it is anonymous, and easy to use. Ease of use is probably the most important aspect of a tool targeted toward the every day consumer. They might not be willing to go through the trouble of setting up special bank accounts or subscribing to extra services to use a system like Digicash.

Another benefit is that these prepaid cards allow consumers to buy goods and services online without the need for credit cards or bank accounts. This is a great benefit for people who do not have the resources to have these financial accounts.

From a technical point of view, the debit card model is quite scalable to many users. The system is a very similar to prepaid telephone cards. The only difference is that card providers need to connect debit accounts to supporting retailers; this last step should be quite feasible. Since we know that prepaid phone cards are in widespread use, the use of Internet debit cards should be equally scalable.

As far as anonymity goes, InternetCash is very strong. Assuming a consumer uses cash to buy his InternetCash cards, he is protected against corresponding parties, website operators, ISPs, network hackers, and computational attackers. These adversaries would have no way of linking an identity to purchases made on the card because he bought the card without exposing his identity. For the most part, he is protected from law enforcement because it would be very difficult to find a careful buyer of a debit card, even if you knew where the card was purchased. Unless the consumer could be tied to some kind of pattern linking him to the cards, he is well protected.

4.5.4 Drawbacks

Some of the drawbacks are that InternetCash requires the consumer to purchase the debit card out of band. Also, transactions can be linked to a given card, and can also be linked to where that card was purchased. This information may not seem important to the average user because their identities have been masked, but users who are very serious about protecting their identity may want to suppress even regional and linking information.

With respect to our threats, the most viable danger to anonymity comes from a local threat. As in the Digicash case, it would be very difficult to prevent a consumer from exposing himself at his own computer terminal. Just about anyone could peek at his computer screen and discover what he was buying or doing.

5 Legal Framework

One of the first questions we need to ask before we think about Internet anonymity tools is whether or not we have the right to do things anonymously at all. We will look at anonymity from two different perspectives. First we will explore the right to speak anonymously, and second, the right to read anonymously. For each, we will describe case law that shows where the US Courts stands on the matter.

5.1 Anonymous Reading on the Internet

5.1.1 Protection from the State

In the US, reading anonymously is well protected by the First Amendment. We will see this in four cases regarding communication and anonymity: *Lamont v. Postmaster General, Denver Area Educational Telecommunications Consortium v. FCC, Fabulous Associates v. Penn Public Utility Commission,* and *NAACP v. Alabama*. In these cases, the right to receive communication and associate is protected against threats of obstruction and inhibition. Although these protections do not explicitly apply to anonymous reading, they seem to protect anonymous reading in most cases.

Lamont v. Postmaster General In *Lamont v. Postmaster General*, the issue at hand was the Constitutionality of a 1963 postal regulation requiring people to take special action to receive "Communist propaganda" through the mail. The postal service channeled mail coming from flagged countries through one of several check points. At these checkpoints, unsealed mail was screened for Communist propaganda. If a piece was found to be propaganda, it was held and a postcard was sent to the recipient of the mail. If the recipient desired the message forwarded to him, he needed to check a box on the postcard verifying that he wanted this and future messages held by the checkpoint. His name was then added to a list of willing recipients. The Constitutionality of the regulation was questioned in both New York and California District Courts. In New York, the postal regulation was upheld because mail recipients need only check one box and send a postcard to receive their mail. That amount of effort was not considered burdensome and thus communication was not being stifled. In California, the District Court came to a very different conclusion. Use of the reply postcard was found to be too burdensome. Furthermore, potential readers may be discouraged from receiving reading material for fear of being exposed, should the forwarding lists ever be leaked. By the time this case reached the Supreme Court, the regulation had changed such that a mail recipient needed to reply by postcard for every single piece of mail being held for him. The lists of willing recipients were eliminated. The Supreme Court ruling was very similar to the California District Court ruling. It was held that asking a reader to send a postcard for every piece of mail was enough burden to stifle speech. In addition, the fear of being exposed as a willing recipient of Communist propaganda might scare away potential readers. In *Lamont* we see that the courts are willing to protect the right to receive communication against unnecessary burdens and inhibitions. We will see this reasoning used again in several other cases.

Denver Area Educational Telecommunications Consortium v. FCC In *Denver Area Educational Telecommunications Consortium v. FCC*, the issue was a 1996 FCC regulation that required cable television companies to place all of their indecent programming on separate channels in the interest of protecting minors. Viewers would need to send a written request to the cable company to gain access to these channels. When brought to the Supreme Court, the regulation was found be overly restrictive for its intended use. The case cited *Lamont* and said that users might be too concerned about their reputations, should the subscription records ever be disclosed even inadvertently. The reasoning for *Denver* shows that the courts are willing to protect speech against threats of inhibition. The fear of having these lists exposed is enough to chill free speech, even if the disclosure were by accident.

Fabulous Associates v. Pennsylvania Public Utility Commission Another similar case is *Fabulous Associates v. Pennsylvania Public Utility Commission*. In this case, the issue was the constitutionality of a Pennsylvania regulation. It required each dial-a-porn user to register for an access code before he could use the service. The Third Circuit Court found that the regulation was unconstitutional because of its effect on free speech. The case clarified the notion that requiring users to identify themselves would cause an inhibitory effect.

NAACP v. Alabama In the fourth case, *NAACP v. Alabama*(1957), the Alabama State Attorney General brought an equity suit against the NAACP for not following proper state corporation statutes. As part of the suit, Alabama acquired a court order requiring the NAACP to disclose their membership lists as part of the case. The NAACP refused to comply, arguing that their Fourteenth Amendment rights were being violated. After reviewing the case, the Supreme Court found that the court order asked for information that was not directly relevant to the case. In the past, revealing the identities of NAACP members were subjected to "economic reprisal, loss of employment, threat of physical coercion, and other manifestations of public hostility"[**?**]. Forcing disclosure of these member-rank lists in the *NAACP* case could intimidate potential members and prevent their affiliation with the NAACP; this would intrude on the right to freely associate. The finding of this case protects the right to associate from threats of intimidation.

Protections In these four cases, we have seen that the courts will protect the right to receive communication and associate from any unnessecary burden and intimidation. These cases do not explicitly mention protection for anonymous reading or anonymous association. The protection for anonymity comes from this reasoning: if a government entity requires readers to identify themselves before they can receive some kind of communication, then potential readers who fear being exposed for willingly receiving this material may shy away from receiving it. If the identity of the receiver is required for the communication to occur, then it would be unnecessarily inhibitory for a potential reader. This inhibition is particularly important when the communication is controversial or personally sensitive, and in most cases, this is when a reader would most want to remain anonymous.

In the context of anonymity tools, these cases suggest that a government agency could not shut down any of these tools for the anonymity they provide. They also suggest that a government agency would not be able to coerce the proprietors of these tools to exposing the identities of their users without a very good and specific reason. Without some kind of law enforcement or security reason, it is unlikely that an agency would be able to gather information about a particular user. Gathering system wide information(like logs) is even less likely because of its inhibitory nature. Through now, we have only considered the protections afforded by the Constitution and how it

limits the authority of government agencies. We will now consider how private companies handle the anonymity of their users.

5.1.2 Protection from Private Parties

In cyberspace, many companies collect personal data about their clients. The can choose to use this information for many different purposes, including internal marketing and sale to direct marking firms. In both cases, the identities of their users can be protected or they may be used directly. Companies usually publish how they use personal information they collect about their users in their privacy policies, including whether or not the data is identifiable, and if it is sold to outsiders. In general, web sites are not required by law to disclose their privacy policies although the current convention is a self-policing strategy to follow guidelines drawn by the Federal Trade Commission. The only solid government regulation is the Children's Online Privacy Protection Act(1999), which prevents companies from using information collected from minors under 13 years old without parental consent. In general though, web sites do publish their privacy policies, and they are easily accessible.

One might ask what happens when a company violates their own privacy policy. One case that involved a primary user of this collected data is *Judnick v. Doubleclick*. Doubleclick is an online advertising firm that collects usage information from its client web-sites. Their privacy policy stated that they would only use personal data in its anonymous form for its business. In 1999, Doubleclick acquired Abacus, a direct marketing company. By combining the Abacus and Doubleclick databases, Doubleclick could possibly identify web-surfers by name rather than anonymously. Judnick accused Doubleclick of doing this, which violates their privacy policy. If this were the case, Doubleclick would be vulnerable under the FTC Act Section 5(15 U.S.C. 45) which prohibits "deceptive acts". Although this case is still pending, In March 2000 Doubleclick has issued a statement saying that they made a mistake by planning the database merge, but will not implement it.

Overall, companies can do almost anything with the information they collect from users as long as they describe it in their privacy policy. The policy is actually an agreement between the user and the service, outlining what the user needs to abide by in order to use the service. Since the privacy policy defines the information that a service may release about its users, the real question becomes: how well are users notified about these privacy policies?

The notification issue has materialized as the opt-in opt-out argument. Opt-in means that users would need to explicitly agree to the terms of a service's privacy policy. In an opt-out situation, the service automatically assumes that the users agree to the terms in the policy if they choose to use the service. A user who does not agree to the privacy policy of a service would need to take extra action to opt-out of any personal information practices used by the service. Unfortunately, there is no standard for using an opt-in or opt-out strategy; no laws have been passed enforcing either of the options. From a privacy point of view, opt-in would be the ideal choice. Users would have a better chance at understanding how their personal information would be used, and would have more control. Most services would rather adopt an opt-out strategy, because their customers' information has value for them, whether it before internal or market uses.

5.2 Anonymous Speech on the Internet

Nowhere in the Constitution is the right to anonymity enumerated, but because of the interpretation of the Constitution it is held to be a "penumbra right", and thus demands protection under our laws. Yet, how this affects online anonymous speech is quite complicated. While the Constitution

protects our rights from the abuses of a heavy-handed government its jurisdiction falls short to some of the more pressing threats to free speech within our virtual borders such as malicious or criminal hackers and the government. If the few but very important cases heard by the Supreme Court provide adequate precedent then the development of technology designed to conceal unauthorized information about net citizens will be able to legally continue. This would provide a check against private as well as governmental threat. At the present, the opposition to online anonymity mainly comes from the government and law enforcement who do not wish there to exist an un-policeable haven for criminal activity hiding behind the pretense of freedom of speech. Those who seek to profit from the lack of legal protections of online personal information would rather maintain the status quo than call attention to the nakedness of the net citizen. The current reality of electronic tracking is manifested in ways from collecting consumer information to finding a user's precise physical location. Fortunately, governmental use of real world to virtual world analogies to justify compromising constitutional rights will serve as a precedent to making similar corollaries between real world protections on anonymity to those online.

5.2.1 McIntyre v. Ohio Elections Commission

One landmark case for privacy advocates was McIntyre v. Ohio Elections Commission (1995). What was being decided was whether or not distributing anonymous campaign literature is a constitutional right. Although this case specifically deals with campaign literature it stands to reason that it is possible to interpret this as asserting that leaflets constitute speech. If leafleting can be defined as advertising an idea, statement, or position on a given issue in a form meant for mass distribution, this can definitely encompass analogous forms of leafleting on the Internet. Whether or not a document is in tangible or digital format should not relegate it to a different set of laws or protections. As was the case, the court decided that the First Amendment anonymously protects publishing. With the words publishing and publisher being so freely used in cases involving regulation of the Internet[4], this decision stands to directly impact the way we interact online.

5.2.2 ACLU-GA v. Miller

Another case that has directly decided the fate of anonymous communication over the Internet is ACLU-GA v. Miller. In this case the American Civil Liberties Union filed suit against Zell Miller[5] in order to challenge the constitutionality of a law passed in Georgia that would make it illegal for a person to falsely represent themselves or other in online communications. The issue at stake was not only anonymous publishing but also all anonymous communications on the Internet. The importance of protecting anonymous communications can be seen in examples such as those who use newsgroups to post questions about sensitive, personal or potentially damaging information, or reporting on government abuses without fear of retaliation, or being able to use the Internet as an extension of anonymous services used offline like anonymous crime reporting to police departments. The court held that anonymous online communications are protected because government law is not applicable to them but only to fraudulent misrepresentations of identity[6]. The law that came into question in this case, Act No. 1029, Ga. Laws 1996, p. 1505, codified at O.C.G.A. §16-9-93.1, did not specify this and hence censored protected speech.

Subsequently, there have been laws proposed and passed that further hinder anonymous communications. Michigan Internet Minimal Identifiers Act would require all free ISP's operating in

[4]For example Cubby v. CompuServe (1991)
[5]ACLU-GA v. Zell Miller (1997); Civil Action
[6]Ibid.

that state such as BlueLight and NetZero to provide traceable information on all of its account holders. The sentiment behind this bill, proposed by State Rep. Bob Brown, D-Dearborn Heights is that being able to track down people will enable law enforcement to crack down on those using Internet services illegally. The constitutional pitfalls of this are extremely evident and it remains to be seen what type of litigation will ensue to correct this or if this law would serve as a tool to those seeking to censor others.

In the same vein, there have been recent federal court rulings that reaffirm the right to anonymous communications. In the case of ACLU-WA v. 2TheMart.com, the defendants were seeking to uncover the identity of a newsgroup user who posted negative comments about the Internet start up which failed later on. In a quest to find the identity of a person who made allegedly financially damaging reports to a newsgroup about the company, 2TheMart.com was also treading a thin line between the violation of people's rights and protecting the personal interests of the company by seeking the identities of suspected newsgroup users from their ISP's. The court held that it is not allowable for this private entity to seek information about someone who has not committed a crime but merely was speaking his or her opinion. If this or other companies or private entities were so easily to be allowed access to the personal information of those who they suspect are speaking out against them it would cripple free speech.

A general border between acceptable and unacceptable levels of anonymous communication on the Internet under current Constitutional interpretation can be drawn as this: Anonymous publication is protected speech. If the anonymity of an author in print can be maintained the same standard should apply to all forms of the author's documents. Not having the ability to communicate under a pseudonym for the purpose of e-mail, posting to forums, chat rooms, etc. abridges constitutionally guaranteed rights. Many laws come directly into conflict with these facts and so maintaining anonymity in communications on the Internet, while it is protected, in some cases it is still unlawful. This impacts developing technologies in that until over-broad laws are repealed anonymity tools will become necessary to protect individuals where the government fails to in an efficient manner.

Due to the fact that the number of cases where the identity of anonymous Internet users is being sought and that service providers are permitted under the ECPA to give out user information to non-governmental seekers of such information, the user must rely on anonymity providing tools until the public outcry becomes enough to change these things. Also, the fact that private companies can subpoena information about Internet users can in itself be found to violate First Amendment rights if the right case comes at the right time to the Supreme Court. This is envisionable in a case where a private entity is seeking information about an Internet user that interferes with their rights to free speech. Given the rate at which companies seek and are granted information about users who may be "bad-mouthing" them in chat rooms and message boards, it is not difficult to see the opportunity for government using private sector ties to gain information that is otherwise restricted to their access.

6 User Scenarios

6.1 Political Dissident

6.1.1 User Goals

In this scenario, suppose you have a political dissident in a country where free speech is not protected. Thus, you have a delicate situation where everyone must watch what they say lest the government might imprison them for harboring thoughts of political change.

In this case, there are many users to consider. First, there is the actual dissident who would like to suggest his plans for reform or criticism of the government. Second, there are other people living in the country that would like to read the opinions of the dissident without being associated with the dissident. Third, there are system administrators who do not want to be held accountable for what their users are doing. Lastly, there is a usually a global audience that is trying to be reached by the dissident to bring attention to what is wrong with the government he or she is opposing.

6.1.2 Adversary's Goals

The adversary in this scenario is the government of the foreign nation. In the case of the dissident, the government would like to suppress speech and uncover the identity of the individual. In addition, the government would like to obtain the identities of the readers as well. Lastly, the government would like to block any and all news surrounding this affair from reaching the outside world.

6.1.3 Threats

A strong government is one of the most powerful adversaries an individual seeking to be anonymous can face. In a nation where certain rights such as freedom of speech and freedom of assembly are not protected, political dissidence can be considered a serious crime. It is not farfetched to assume that the government has complete "legal" power which they can exert over anybody including all ISPs. Using this power, they can force system administrators to give up whatever information they have on users and clients. The government can also use this power to force ISPs to shut off connectivity to the outside world. The government may also have the ability factor large primes which would largely decrease the effectiveness of cryptographic technologies. Lastly, it can also be assumed that the government can have Carnivore-like machines installed throughout much of the network, giving them tremendous ability to monitor and affect traffic at the network layer [17].

6.1.4 Tools

For the political dissident, there are several steps can be taken to increase anonymity.

First, use of a reliable remailer system is highly recommended for transporting illegal documents to publishing sites. This would ensure that the documents are multiply encrypted throughout transit which would make the job of decrypting that much harder for the government. Use of type-2 remailers would also help foil traffic analysis by the government by using fixed sized packets and message reordering. In addition, the reply-block used by the dissident should point back to a public newsgroup that is widely read so the government cannot determine the true recipient by simply keeping track of everyone that's read the message. Lastly, the user should take great care when mailing the message to the first hop in the remailer chain. Our recommendation is to send the mail from a network site or ISP that is known for extremely high traffic and to use some sort of time delay so that it is difficult to correlate users logged on and to mail sent.

Now there is the issue of actually publishing the document. This can be performed in many ways. Systems such as FreeHaven, Publius, or Rewebber would suffice for this given a significantly large deployment that is beyond the foreign government's control. Some technological glue may be required so that users can simply email documents that they would like to have published but this is technically feasible.

When it comes to readers who would like to remain anonymous, there are several technologies that attempt to make web browsing anonymous. Unfortunately, most of these technologies are susceptible to traffic analysis. However, modifying the closely related technology of "onion routing"

(which uses proxy chains similar to mixnets) may provide a better solution. While vanilla onion routing is also susceptible to traffic analysis, running additional software that would maintain a constant amount of traffic between the nodes in the onion network would greatly increase the systems susceptibility to this type of attack. At that point, users could then use onion routing to perform their http "GET"s in order to retreive web documents.

When considering system administrators, of ISPs, remailers, and anonymous publishing systems, the main precaution that they can take are to minimize the amount of logging that their system performs. This would help minimize their liability when users perform illegal actions because they would have little or no means to monitor and control such actions.

6.1.5 Remaining Vulnerability

The remaining vulnerability of the users is difficult to determine. A great deal depends on how powerful the government is, both computationally and from a law enforcement perspective. By forcing collaboration of all system administrators, it is feasible for the government to ascertain the identity of the individuals involved. With the added help of powerful encryption breaking technologies, even administrators that refuse to help cannot stand in the government's way.

6.2 Online Leaflets

The adversaries to online leafleting can be any entity or individual opposed to the content of the leaflet in question an in an effort to quash the distribution of a message, are seeking to uncover the identity of the author and publisher of the leaflet. This threat can come from law enforcement, government, or private citizens or corporations making opportunistic use of over broad laws.

The main tools of these adversaries are the current technology standards which make little provision for Internet users to maintain their privacy as well as laws drafted in a way that compromise constitutional rights in the name of making other laws more effective.

In the instance that some entity or individual acts on their ability to curtail a leafletter's activity through the enforcement of faulty laws, they can very effectively do so because legal action to rectify these problems take significant amounts of time. In the instance that some entity or individual acts on their ability to curtail a leafletter's activity through the implementation of tools to uncover the identity of Internet users, the proponents of unpopular or controversial ideas face impending retaliation in a way that would be much more difficult to take place in the real world and thus hindering freedom of speech as has been demonstrated in Supreme Court cases[7]. Aside from discouraging free discourse, the leafletter may also face fines or censorship.

6.2.1 Legal Situation

The legal and Constitutional protection offered to online leafletters can be inferred from their real world counterparts. Specifically in McIntyre v. Ohio Elections Commission 1995, it was held by the Supreme Court that the distribution of anonymous campaign literature is constitutionally protected speech[8]. The Supreme Court in ACLU of GA v. Miller that anonymous publishing online itself is constitutionally protected speech also held it two years later.

As for the possible adversaries of a particular leafletter's activity like an ISP suing for libel, a law enforcement agency attempting to conduct an investigation that is constitutionally in the grey area, enemies on the Usenet, as well as network and computational attacker employed by

[7]McIntyre v. Ohio Elections Commission (1995), United States Supreme Court
[8]Ibid.

any of the above; they would need to demonstrate that their rights are somehow being infringed upon by a leaflet or that the person publishing them is doing something that is illegal on order to proceed on a legal basis but this is not necessary to successfully achieve their ends as they are facilitated by technology. In that case the legal protections for the person are non-existent and both law and technology would be weighted in favor of the adversaries. Assuming the leafletter to be doing nothing illegal, the adversaries may still have a legal playing card. Many laws are still being enacted in an effort to thwart anonymity on the Internet. If The Michigan Internet Minimal Identifiers Act is passed for example, ISP's running in Michigan like NetZero and BlueLight to identify their subscribers by verifying customers phone numbers or credit card information[18]. In addition to laws that will probably be deemed unconstitutional in the future but are now in place, adversaries are able to take advantage of these things to do what amounts to censorship of constitutionally protected speech.

In this sense, until privacy protections become standard in Internet products and services, those who would seek to oppose a person doing the equivalent of leafleting online have not only technology on their side but the law is also tilted in their favor.

6.2.2 Tools

In the real world, a leafletter has basically two options of ways to distribute his material. On the one hand leaflets can be either placed on personal property like the crack in a front door or pinned underneath a windshield wiper. On the other hand leaflets can be placed and/or distributed in a public place like being handed out in front of 77 Mass. Ave. or posted on one of the bulletin boards in the hallway. The obvious online counterparts to these activities would be sending bulk e-mail and posting information in public forums respectively.

In the case of bulk e-mail one tool that could be considered for protecting anonymity are re-mailers. They are feasible to use but the decentralized nature of their operation leads to slowness of propagation. If the message is an urgent one this may be a problem but in most cases the additional time would have to be planned for as in the real world if anonymity is more valuable than instantaneous distribution. On another note of feasibility, as built in anonymization tools become more canonical, so do tools to reduce spam. This again is not a problem if the leafletter is sending e-mail to people who want to receive it because they have subscribed to certain mailing lists or have opted-in to receive mail from this person. As for the way this type of distribution is affected by law, privacy advocates are not only fighting for the anonymity that protects free speech but also the anonymity that protect people from being stalked by marketers and others interested in stereotyping them and then flooding them with unwanted mail. Currently, however analogous laws should apply to the leafletter's situation online and off[9].

If the leafletter wanted to obscure his identity using a tool such as Freedom from ZeroKnowledge Systems, they would gain the benefit of having encrypted e-mail but wouldn't be able to capitalize on it for these purposes because of the fact that ZeroKnowledge restricts the amount of e-mail subscribers can send in a day in order to serve the interests of all their customers[10]. The up side comes in that with an untraceable pseudonym, and advertised feature of their product, publishing in web forums, on bulletin boards, the Usenet, and purportedly on IRC becomes a safe activity. As for legality, it has already been discussed that anonymous publishing has been ruled protected constitutional speech.

[9] ACLU-GA v. Zell Miller (1997) decided that political leafletting is protected speech

[10] http://www.freedom.net/ one of the features is that it protects users from and prevents users from spamming by enforcing a limit on the number of e-mails that can be sent in a day.

With a conceptually operational FreeHaven, someone who wanted to distribute anonymous literature about a topic that would also warrant hiding his identity would be able to do so, providing that the information is useful or desirable by others[4]. If it were not, there would be no adversary to hide from and no reason to cloak his identity. Thus, this type of system also provides useful feedback. Critics of FreeHaven could claim, as is the case in The Michigan Internet Minimal Identifiers Act that the tool also serves to cloak illegal activities.

With speed not being a critical issue, a combination of a re-mailer service and a pseudonym provider such as ZeroKnowledge should be sufficient protection for someone wishing to anonymously publish their ideas.

6.3 Anonymous Shopping

One scenario many people can relate to is that of the anonymous shopper. Many consumers would like to avoid the intrusions of consumer profiling and extensive spending records, but the current Internet shopping scenario is the exact opposite. Most online retailers use credit cards to collect payment, and thus know the identity of their customers. The customer's, purchase data, billing address and shipping address are freely available to the retailer. In addition, the credit-card company is privy to how much money is spent and at what online store.

In contrast, at a brick and mortar retailer, a consumer can walk in, purchase something with cash, and walk out. Most retailers do not require names from their consumers, and even if they did, a consumer could provide an alias. By using cash, a consumer can purchase something and leave no record of who they were, what they bought, and how much they spent. This is completely different from current online purchases.

6.3.1 User Goals

In the anonymous shopping scenario, a consumer aims to purchase a product from an online retailer without exposing his identity, and without creating a record of the transaction linked to him. He is not planning anything illegal or dangerous; he is only trying to protect his privacy.

The consequences of exposure are not very great. The likely result of the adversaries discovering the user's identity is just more directed marketing. This is something we already encounter frequently.

We will assume that the anonymous shopper is not an expert computer user. He is an everyday person who does not care to understand the details of the systems he uses, and does not want to be burdened with excessive computer setup. He may use a packaged solution, but is not willing to do more than install an application on his computer.

6.3.2 Adversary Goals

The adversaries in this scenario are the retailer, the financial institution used to facilitate the monetary transaction, and the shipping company used to transport the purchased items.

The retailer, financial institution and the shipping company all have the same objective in this scenario. They would like to collect purchasing data for internal marketing purpose and for possible sale to professional marketing firms.

Any particular bit of data is not very valuable because marketing data is worth more in quantity. The minute importance of any particular transaction is very small, so the adversaries would not be willing to devote lots of resources for the discovery of protected data.

6.3.3 Threats

The threats controlled by the retailer include the correspondent. Obviously, because the retailer is the correspondent, it is privy to all of the information the consumer gives to them. Likewise, the financial institution can gather whatever information they can from account records and transaction details. The shipping company has information linking the retailer and the recipient address.

In addition to these individual threats, the three adversaries can collude in pairs or all together to combine all of the information available to them. They may also collude with ISPs to gather IP information about their users.

6.3.4 Tools

The anonymous shopper's most reasonable defense is to only hide his monetary transactions. He can accomplish this by surfing the website though an anonymous web proxy such as Anonymizer.com[19] or Zero Knowledge Freedom[20] and using blinded Digicash[21] or internetcash.com[22] for the transaction.

If Digicash is used, financial institutions(bank) cannot directly gather consumer data from his transaction. They only know that they issued digicash to the shopper, and the retailer is depositing digicash. The bank cannot link the two transactions and find out where the shopper spent his money.

Another advantage that Digicash gives the consumer is that the retailer does not need to know the identity of the consumer to collect payment. This is another property of the blinded coin structure of Digicash.

If the InternetCash card is used, internetcash.com knows that the purchase occurred, but it cannot link a buyer to the purchase. This is because the buyer purchased the debit card in person using untraceable paper money. The most that internetcash.com could know is that the card was purchased in a particular geographic location, and where the money was spent. It cannot know who exactly executed the transaction unless the consumer used a traceable payment to buy the card.

The drawback in this solution is that the retailer will know where the product will be shipped. Unlike the brick and mortar shop, the online consumer does not go and pick up his purchase; he usually has it shipped to himself. If the consumer has the product shipped to his home, and uses his name on the address, he has exposed his identity, and the retailer can use this information. If he uses his own address, but leaves off his name, the retailer can likely lookup his address and a directory to find a matching name. It is plain that this solution is not perfect. The retailer can find the name and address of the recipient, although the buyer's identity can be hidden. In many cases, these are the same person.

If the consumer wants a bit more protection, he can have the delivery made to a P.O. box instead of a real address and omit his name. Luckily, the Post Office does not release the owners of P.O. boxes so the consumers real address seems safe. Private services such as www.investigatorsonline.com[23] offer to search for the owner of the P.O. box, but the cost of the search is $75. The retailer is not likely to invest this much to find their customer identity, because the returns gained for such information is probably less than $75.

6.3.5 Remaining Vulnerability

One drawback of this system is that neither Digicash nor InternetCash is widely accepted at retailers. This is an obvious problem, because without Digicash (or an equivalent) the consumer must

pay via something like a credit card. Consequently, he would be forced to expose his identity.

Another drawback, is that assuming the consumer had an anonymous payment method, the he would still need to use a P.O. box to mask his address. Most consumers would not go as far as to rent a P.O. box for the occasional online purchase.

6.3.6 Recommendations

As a recommendation, we first need a widely accepted form of digital payment. Without this, there is very little chance for anonymous shopping. Credit-card payment is probably the easiest way for a retailer to verifiably identify the purchaser.

In addition to the payment problem, the shipping problem needs a solution. For anonymous shopping to be widely used, the P.O. box solution needs to be simplified. A casual consumer should not need to rent a P.O. box just to buy things in cyberspace.

One possible solution to this problem was presented by anon2u.com[24]. This service acts something like a shipping proxy, where the retailer sends packages to an alias at anon2u.com and anon2u.com then forwards the packages to the customer using that alias. To solve the payment problem, anon2u.com pays the retailer, and then bills the customer. The problem with this solution is that full trust is placed in anon2u.com, shipping time is increased dramatically and anon2u.com was not widely accepted . Furthermore, anon2u.com has gone out of business due to business problems.

In conclusion, for anonymous shopping to become reality, we first need a widely accepted anonymous payment method, and a viable anonymous shipping solution.

7 Conclusion

In the preceding sections, we evaluated the feasibility of online anonymity in several different usage scenarios. We began by defining specific threats to an Internet user's anonymity. Those threats come from all over, spanning from family members, to law enforcement officials. From there, we took a careful look at a number of Internet anonymity tools; these tools are either available today, or will be available in the near future. For each tool, we examined how well the tool protected against the threats we listed along with its benefits and drawbacks. We also evaluated the legal notion of anonymity and how users are, or are not, protected by US law and the Constitution. After describing all of this background, we went on to explore scenarios in detail where a user might desire anonymity.

We chose several user scenarios that represent most of the anonymity issues facing the Internet users of today. The breadth of our scenarios covers situations from anonymous whistle-blowing to anonymous shopping. For each scenario, we attempted to construct an anonymity solution, by combining the anonymity tools at our disposal. Our results from this study were encouraging, but not ideal. In most of our scenarios, a casual user could achieve acceptable identity protection, but for extremely sensitive users, these tools fall short. In most cases, a strong adversary with enough resources can discover a user's indetity. Unfortunately, anonymity is most important when the adversary *is* so strong.

For these reasons, we conclude that anonymity exists for the casual user. It can even come in an off-the-shelf product. For the more sensitive user, anonymity tools can help, but may not offer adequate protection against the strongest of adversaries. The current offering of anonymity tools is encouraging, but we would like to see what the next generation of tools can accomplish.

References

[1] D. Sobel, "The process that "John Doe" is due: Addressing the legal challenge to internet anonymity." http://www.vjolt.net/symp2000/johndoe.html.

[2] D. Chaum, "Untraceable electronic mail, return addresses, and digital pseudonyms," *Communications of the ACM*, Feb 1981.

[3] P. A. Strassman and W. Marlow, "Risk-free access into the global information infrastructure via anonymous remailers.," in *Symposium on the Global Information Infrastructure*, January 1996.

[4] R. Dingledine, "The Free Haven project: Design and deployment of an anonymous secure data haven," Master's thesis, Massachusetts Institute of Technology, 2000.

[5] L. Cotrell, "Mixmaster and remailer attacks," 1995. http://www.obscura.com/ loki/remailer/remailer-essay.html.

[6] D. Mazires and M. F. Kaashoek, "The design, implementation and operation of an email pseudonym server," in *5th ACM Conference on Computer and Communications Security*, 1998.

[7] P. Boucher, A. Shostack, and I. Goldberg, "Freedom systems 2.0 architecture," May 2001. http://www.freedom.net/info/whitepapers/Freedom_System_2_Architecture.pdf.

[8] R. McFarlane, A. Back, G. Hoare, S. Chevarie-Pelletier, B. Heelan, C. Paquin, and D. Sarikaya, "Freedom 2.0 mail system," May 2001. http://www.freedom.net/info/whitepapers/Freedom_2_Mail_System.pdf.

[9] "Untraceable nym creation on the freedom 2.0 network," May 2001. http://www.freedom.net/info/whitepapers/Freedom-NymCreation.pdf.

[10] G. Showman, J. Svatek, and P. Branchaud, "Freedom 2.0 ad manager," May 2001. http://www.freedom.net/info/whitepapers/Freedom_2_Ad_Manager.pdf.

[11] D. M. Roger Dingledine, Michael Freedman, "The Free Haven project: Distributed anonymous storage service," in *Proceedings of the Workshop on Design Issues in Anonymity and Unobservability*, July 2000.

[12] "Freenet," 2001. http://freenet.sourceforge.net/.

[13] "Mojo Nation," 2001. http://www.mojonation.net/.

[14] D. Chaum, A. Fiat, and M. Naor, "Untraceable electronic cash (extended abstract)," in *Advances in Cryptology—CRYPTO '88* (S. Goldwasser, ed.), vol. 403, pp. 319–327, Springer-Verlag, 1990, 21–25 Aug. 1988.

[15] A. M. Froomkin, "Flood control on the information ocean: Living with anonymity, digital cash, and distributed data bases," in *U. Pittsburgh J. of Law and Commerce, vol. 15, no. 395*, 1996.

[16] N. Usha Rani, "Privacy issues on the internet," in *Tata Infotech Research Group: Indian Institute of Technology*, 2000.

[17] "Carnivore FOIA documents," 2001. http://www.epic.org/privacy/carnivore/foia_documents.html.

[18] M. Wendland, "Proposed law would erase free web users' anonymity," Feb. 2001. http://www.freep.com/money/tech/mwend8_20010208.htm.

[19] "Anonymizer.com," May 2001. http://www.anonymizer.com.

[20] "Zero Knowledge Systems," May 2001. http://www.zeroknowledge.com.

[21] "Digicash," May 2001. http://www.digicash.com.

[22] "internetcash.com," May 2001. http://www.internetcash.com.

[23] "Investigators online," May 2001. http://www.investigatorsonline.com.

[24] "Anon2u.com," May 2001. http://www.anon2u.com.