Assessing Anonymous Communication on the Internet: Policy Deliberations

Rob Kling and Ya-ching Lee

Center for Social Informatics, Indiana University, Bloomington, Indiana, USA

Al Teich and Mark S. Frankel

American Association for the Advancement of Science, Washington, DC, USA

Anonymous communication on the Internet offers new opportunities but has ill-understood risks. This article helps to ground the policy debates by examining some fundamental aspects of anonymous social behavior and current controversies over anonymous communications. It is a companion to the article in this issue, "Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference." It examines the social character of anonymous communication and the ways that anonymous communication has played important roles for professionals such as journalists and the police. It also explains some of the new technological supports for anonymous communication on the Internet. The openness, decentralization, and transnational character of the Internet challenge the efficacy of traditional control mechanisms and have raised issues related to accountability, law enforcement, security and privacy, governmental empowerment, and e-commerce. Yet, to ban or restrict all anonymous communication online because of the harms it could bring would deny its benefits to those people who may legitimately gain from it. This article helps to understand how to balance these positions.

Keywords anonymity, CMC, email, encryption, information policy, Internet, privacy, professional communication

The Internet provides new opportunities for anonymous communication—opportunities to make political claims and non-political comments, engage in whistle-blowing, perform commercial transactions, and conduct personal correspondence without disclosing one's identity. At the same time, anonymity can facilitate socially unacceptable or even criminal activities because of the difficulties in holding anonymous users accountable. Because of the complex interaction of social conventions, legal traditions, and technological designs the policy issues associated with the regulation of anonymous communications on the Internet have some important nuances. This article examines some of the nuances behind the policy debates.

AAAS PROJECT ON ANONYMOUS COMMUNICATION ON THE INTERNET

The American Association for the Advancement of Science (AAAS), with funding by the National Science Foundation (NSF), conducted a project to examine online anonymity and identify criteria for judging the desirability of anonymous and pseudonymous communications.[1] The goals of the AAAS project were to develop an understanding of anonymous communication on the Internet, to determine if and how it might be possible to facilitate socially desirable uses of anonymous communication while limiting undesirable ones, and to develop policy recommendations for implementing these ideas.

The project consisted of four core activities:

1. AAAS conducted an **online survey** in the summer of 1997 to gather information from Internet users about their experiences with anonymity and pseudonymity online.[2]
2. Five **focus groups** were conducted in the summer of 1997 to examine experiences and views regarding the uses of anonymity in different settings off-line—law enforcement, journalism, counseling and support services, whistleblowing, human rights—and

Address correspondence to Rob Kling, Indiana University, School of Library and Information Science, Main Library, 10th and Jordan, Room 012, Bloomington, IN 47405-1801. E-mail: kling@indiana.edu

The Information Society, 15:79–90, 1999

0197-2243/99 $12.00 + .00

to see what lessons might be learned for use online.

3. In November 1997, AAAS convened an **invitational conference** in Irvine, CA. Participants were drawn from the computing industry, including Internet service providers, network administrators, and providers of "anonymizing" services; the legal community, including law enforcement; professional societies; academic institutions; and human rights groups, to discuss uses of anonymous communication on the Internet.[3] The meeting was organized in part around four commissioned papers that were intended to focus and foster conference discussions:

   - "Technical Dimensions," by Peter Wayner, Consulting Editor, BYTE Magazine;
   - "Ethical and Social Dimensions," by Gary Marx, Woodrow Wilson International Center for Scholars and Director of the Center for the Social Study of Information Technology, University of Colorado at Boulder;
   - "Legal Issues in Anonymity and Pseudonymity," by Michael Froomkin, Associate Professor of Law at the University of Miami Law School;
   - "Commercial Dimensions," by Donna Hoffman, Associate Professor of Management, and Co-Director of Project 2000 at the Owen Graduate School of Management, Vanderbilt University.

   Revised versions of these articles appear in this issue of *The Information Society*.

4. Following the conference, in the summer and fall of 1998, AAAS staff, in collaboration with several conference participants, developed and tested several **case scenarios** on anonymity/pseudonomity for educational use. The cases will soon be posted on the World Wide Web at http://www.aaas.org/spp/anon/

This article distills and elaborates on the discussions at the AAAS Conference, on data generated by the online survey, and on information gleaned from the project's focus groups. It begins by defining some key dimensions of anonymity and then describes the technologies that enable anonymous communication on the Internet. This is followed by an overview of the advantages and disadvantages of anonymous/pseudonymous communications, a summary of policy issues related to the regulation of such communications, a comparative look at the control of online versus offline communications, and a set of conclusions.

DIMENSIONS OF ANONYMOUS COMMUNICATION

Gary Marx (1999) enumerates seven elements of personal identification:

1. **Legal name**: A legal name involves a person's true identity and may be connected to biological, social, and other information.
2. **Locatability**: If a person's address is known, he or she can be located and reached.
3. **Traceable pseudonymity or pseudo-anonymity**: A person using a pseudonym that can be linked back to that person or his or her address under restricted conditions. In the case of Internet communications, online services act as an intermediary and allow participants to use pseudonyms in BBS or chat rooms. The online services retain a record of each person's identification.
4. **Untraceable pseudonymity**: A person using a pseudonym which cannot be linked back to that person or his or her address by intermediaries because of protective policies or the inability to trace. In the case of Internet communication, people using pseudonyms can make their identities untraceable through chain mailing and encryption remailer services (e.g., Mixmaster).
5. **Pattern knowledge**: A person can be identified by reference to his or her "appearance or behavior patterns." Persons making anonymous postings can be known by the content and style of their messages.
6. **Social categorization**: A person can be identified by social categories, such as gender, age, class, employment, and religion.
7. **Symbols of eligibility/non-eligibility**: A person can be identified by her possession of knowledge (passwords, codes) or artifacts (tattoos, uniforms) as an eligible or ineligible person.

Anonymous communication is a feature of social relationships and encompasses several dimensions:

1. **Relational**: Anonymous communication is relational as it involves at least two parties, sender(s) and receiver(s). There may or may not be an intermediary acting as a link between these two parties, and the intermediary may know or may not know the true identification of the sender (Marx, 1999).
2. **Confidentiality**: Anonymous communications, full or partial, can be confidential. Confidentiality involves the sharing of information with the expectation that it will not be revealed to third parties, or that it will be revealed only under restricted circumstances (Marx, 1999). Confidentiality is a form of anonymity. For example, it is common for journalists to use anonymous informants. The identities of

the informants are confidential, but are known to the journalists.

3. **Pseudonymity**: Pseudonymous communication involves the use of a pen name, symbol, or a nickname. People who use the Internet can have one or many pseudonyms that allow for the continuity of identity and the creation of an online personality (Froomkin, 1995a). Sometimes an individual can establish a reputation over time based on his or her communications without disclosing his or her actual identity (Froomkin, 1995a).
4. **Pseudo-anonymity**: Pseudo-anonymity results when a person opens an account with a remailer service provider and chooses or is assigned a pseudonym. Only the remailer operator can link the pseudonym to the individual. As long as the remailer operator protects a person's records and does not reveal his or her e-mail address(es), privacy is secured. For an individual wishing to send an e-mail message without disclosing his or her identity, pseudo-anonymity is a user-friendly means of doing so, but it provides less assurance of anonymity than use of an anonymous remailer, as described below (Bacard, 1996).

A person is not anonymous in any absolute sense. Anonymity and pseudonymity are features of specific relationships and communications. We will refer to all four of these as anonymous communication, unless we wish to distinguish explicitly between them.

INTERNET TECHNOLOGY AND ANONYMITY

Anonymous Remailers

Anonymous remailers were originally developed in 1988 to allow Internet users to post messages to certain Usenet newsgroups without disclosing their identities. Today, they allow Internet users, free of charge, to post anonymous messages to virtually all newsgroups or to send anonymous e-mail to anyone they wish (Edelsten, 1996).

In its simplest form, an anonymous remailer works by accepting an e-mail message from a sender, stripping off the headers that would serve to identify the sender, and then forwarding the message to the intended recipient. Anonymous remailers have several vulnerabilities. First, remailers can be compromised (e.g., the remailer server may be broken into, or its files may be subpoenaed). Users seeking a stronger guarantee of anonymity can avoid this vulnerability by **chaining remailers** (discussed below). To add further security, messages may be encrypted using public-key cryptographic techniques.

A second weakness is that remailers, even chains of remailers, are vulnerable to traffic analysis. Traffic analysis, the study of patterns of communication, is a technique used to glean information about network communications, even when the contents of the communications themselves are encrypted (Diffie & Landau, 1998, p. 35–38). For example, if a remailer is known to process incoming messages and send them on immediately, it is a simple matter to connect the source of a given incoming message with the destination of the next outgoing message. Also, because messages differ in size, they can be traced and distinguished by size (Cottrell, 1996a). Traffic analysis is particularly effective when the identity of the communicants, rather than the content of the communication, is desired. To counter these methods of detection, certain remailers (e.g., Mixmaster) reorder the packets of network traffic and make them all the same size.[4]

The advantage of using chained remailers is that each remailer only knows a small part of the entire message route, namely the preceding remailer and the next remailer to which the message is to be routed in the chain. Even if one remailer in the chain is compromised, it is unlikely that any given message can be connected with its sender (Cottrell, 1996a).

Varieties of Anonymous Communication on the Internet

There are at least four types of anonymous communications on the Internet:

Traceable Anonymous Communication. In Internet communication, people can use an intermediary to convey information or messages without revealing their true identities. The sender is only identifiable to the intermediary (Marx, 1999). Traceable anonymous communication occurs when Alice asks Bob (who operates an anonymous remailer) to forward an unencrypted message to Eric. Bob keeps a record of Alice's e-mail address and (perhaps) a copy of the forwarded message as well as Eric's address. When Eric receives the message, he has no way of knowing it is Alice who sent the message because Bob has removed Alice's identification and return address. However, if the content of the message violates a law, a judge may subpoena Bob and compel him to reveal Alice's identification.

"Untraceable" Anonymous Communication. There are instances in which an Internet user may wish to be more certain of remaining anonymous than a single remailer will allow. One way in which to accomplish this is by using "chained remailers" (Froomkin, 1995a). Imagine that Alice sends a message to Bob the Remailer, encrypted with Bob's public key (i.e., only Bob can decrypt the message). The content of the encrypted message sent to Bob is another encrypted message (this time encrypted with Charlie's public key), along with instructions to send the message on to Charlie.

When Charlie receives the message from Bob, he decrypts it. The contents of this decrypted message are yet another encrypted message (this time encrypted with David's public key), along with instructions to send the message on to David. When David receives the message from Charlie, he decrypts it, and finds the text of the original message intended for Eric, along with instructions for sending the message to Eric. Each remailer decrypts its portion of the message, follows the instructions, and sends the rest of the (still encrypted) message on to the next remailer (Cottrell, 1996b). No single remailer knows the full path of the other remailers handling the message. In other words, no single remailer can read the message to Eric and connect it to Alice. However, each remailer in the chain will know the identity of the remailer from which the message came, and the identify of the next remailer to which the message will be sent (Froomkin, 1995a). That means Alice can still be traced, albeit with difficulty. A judge can order David to disclose Charlie's identity, Charlie to reveal Bob's identity, and, finally, Bob to reveal Alice's identity.

An alternative way to achieve virtually untraceable anonymity is to open an account on one of the Web sites that gives away free e-mail addresses, such as Yahoo! Mail, MauiMail, 3Dmail, Busymail, Conk!mail, EMU Mail, Flashemail, Hotmail, and Mail City.[5] People who use the Internet can create an account without giving any personal information or by giving false information. Furthermore, ComputerMax Inc. now offers anonymous prepaid Internet service giving subscribers a randomly generated user name and password. The service is expected to attract people who are looking for secured privacy and who want to communicate anonymously because a customer's real name is not associated with the account. The free e-mail offering and anonymous services make traffic analysis more difficult and costly.

Traceable Pseudonymous Communication. Like anonymous communication, pseudonymous communication can be either traceable or untraceable. Suppose that Alice sends a message to Eric through remailer Bob using a pseudonym. Bob keeps a log and can link the pseudonym to Alice. Eric can directly send the reply message to the pseudonymous e-mail address appearing in the "From:" field of the message. The message sent by Eric will be received by the remailer operator, Bob, who will locate Alice and forward Eric's reply to her (Froomkin, 1995a). Many Internet service providers and online service providers (e.g., America Online) allow people to employ a pseudonym as their user ID (Froomkin, 1996a). The providers usually keep a record of customers' names, e-mail addresses, and other personal information and can trace them if necessary.

Untraceable Pseudonymity. Untraceable pseudonymity works much like untraceable anonymity (Froomkin, 1995a). The difference lies in the sender signing his or her name with a pseudonym. Alice can even sign with a digital signature to prevent any counterfeit (Froomkin, 1995a). Alice can use multiple encryption to make herself unidentifiable, just as described above. At the same time, Alice can maintain the continuity of her pseudonym. The ultimate recipient, Eric, cannot identify the originator of the message unless he is able to trace back through all remailers in the chain. (Froomkin, 1995a).

Anonymous communication also results when remailer operators make no effort to verify the identify of individuals who use their services. Users who rely on this for anonymity may still be identified through traffic analysis. Even those who send anonymous mail from a free e-mail account can be traced with the aid of local or regional Internet service providers, unless they log into an open access computer, such as in a public library or university lab.

BENEFICIAL AND HARMFUL ASPECTS OF ANONYMOUS COMMUNICATION

People say or write things under the cloak of anonymity that they might not otherwise say or write. Since anonymity typically frees the sender of a message from fear of retaliation or confrontation, it may encourage either honesty or dishonesty in communication, depending on circumstances (Levmore, 1996). Because anonymity permits communication without retribution, it raises issues of accountability and reliability, and when and why identification should be revealed or concealed. What are the conditions under which people who communicate over the Internet should be encouraged (or perhaps compelled) to disclose their identities, and when should they be allowed (or encouraged) to remain anonymous?

Benefits

Most respondents to the AAAS online survey and focus groups indicated that they had had very positive experiences in communicating anonymously. They identified several positive aspects of anonymous communication, both on- and off-line. Some, in fact, regarded the ability to communicate anonymously as essential to their work.

Investigative Journalism. Journalists frequently use anonymous sources to help investigate news stories. While the journalists participating in the AAAS focus group expressed some discomfort with anonymous tips, they nevertheless reported using them and quoting informants who were unwilling to reveal their identities as an "anonymous sources." Double-checking with other sources and verifying information received anonymously are essential in such cases, however.

Whistleblowing. Conference participants pointed out that, before the advent of the Internet, employees of an organization wishing to "blow the whistle" on colleagues or superiors while remaining anonymous could simply send a letter without including any identifying information, such as a name and return addresses. Telephones and fax machines provide alternative channels for doing this. Now, individuals can also register anonymous complaints by e-mail. Government agencies, including the Department of Veterans Affairs (http://www.va.gov/oig/hotline/hotline.htm) and the General Accounting Office (http://www.gao.gov/fraudnet/fraudnet.htm) have established anonymous hotlines on the Internet. A government employee who believes, for example, that his boss is taking bribes can use anonymous e-mail services to send evidence to his agency's inspector general's Internet hot line.

Law Enforcement. Police rely on anonymous informants to obtain information about criminal activities, although they are sometimes overloaded with misleading anonymous tips on high-visibility cases. In cyberspace, several sites offer access to anonymous e-mail to help police capture suspected criminals by offering rewards and anonymity to citizens for information about crimes. The web site of the Chicago Police Department (http://www.ci.chi.il.us/CommunityPolicing/FightCrime/Forms/Narcotics.html), for example, includes an "Online Drug Activity Form" for people who want to provide anonymous information about drug sales and related activity. Another example is the establishment of a special e-mail address—*uce@ftc.gov*—for the Federal Trade Commission. Consumers can, without identifying themselves, forward unsolicited commercial e-mail that they believe may be fraudulent or deceptive while remaining anonymous if they wish (Clausing, 1998).

Self-Help. Conference and focus group participants identified a number of instances where anonymity may facilitate self-help regarding such matters as alcohol, drug, and family abuse, sexual abuse, sexual identity, AIDS and other diseases, and mental and physical illness (Froomkin, 1996a; Froomkin, 1997; Marx, 1999). People might be shy or feel uncomfortable seeking help or information in a face-to-face interaction, telephone conversation (even though they can communicate anonymously or pseudonymously), by mail (a person has to attach a return address in order to receive a response), or by seeking information in libraries (others might accidentally see what one is reading). Searching for, sharing, and consuming the information on the Internet, preferably in the privacy of one's home, might be the optimal way to gain knowledge without disclosing one's identity. The proliferation of Internet discussion groups focusing on such topics offers evidence of the value of anonymous communication in this realm (Lewis, 1994; Lee, 1995).

Personal Privacy Protection. Anonymous communication is one of the most powerful means people have for ensuring privacy. Anonymity offers protection against being tracked and receiving unwanted advertisements as well as junk e-mail. People may also use pseudonyms to hide their true identities when requesting information. Women may prefer using a neutral or male pseudonym to communicate on the Internet in order to avoid gender discrimination, differentiation, or harassment. Men can also use female pseudonyms to mingle with female communicators or to experience the intimacy of female friendship. Such deception may, of course, have harmful as well as beneficial effects.

Avoiding Persecution. Individuals subject to human rights violations by repressive regimes sometimes communicate anonymously to avoid persecution (Froomkin, 1996a; Froomkin, 1997; Marx, 1999), and human rights organizations use it to ensure private communication with those who may be at risk. In many countries, criticizing the government or exposing human rights abuses is illegal. With anonymous online postings, such information can be brought into the open without exposing the informants to the risk of retaliation.

Harms

Experience with anonymity off- and on-line demonstrates that it can also lead to unwanted communication that can range from annoying to dangerous (Froomkin, 1995a).

Spamming. Anonymous "spam" is perhaps the most common abuse of anonymous communication. Spam is electronic junk mail—messages that are posted to multiple newsgroups or mailing lists as well as bulk e-mail advertisements sent simultaneously to many individuals (Bernstein, 1995; Arar, 1994). Spamming newsgroups or individual e-mail addresses with thousands of commercial messages is attractive to some advertisers because of the low cost (Edelsten, 1996; Foner, 1996). Hackers may send messages to disrupt or damage services. Online spamming, generally an annoyance for individuals, has occasionally become a serious problem for ISPs and system operators. For example, in 1997, spam from firms calling themselves "LCGM" and "Web Promo" caused traffic congestion on America Online. The companies used false header information to make it appear that the messages came from AOL itself (Seminerio, 1997). A similar situation occurred on CompuServe, also in 1997

(*CompuServe Inc. vs. CyberPromotions*, 1997). The junk e-mail sent by these companies slowed down or jammed the service providers' servers.

Deception. Anonymity facilitates deception. In 1994, a subscriber to Prodigy made allegedly libelous statements on an electronic bulletin board claiming that an investment bank, Stratton Oakmont, was assisting a public offering for a firm whose president had been involved in criminal activities (Kansas City Star, 1994). Because the message was posted with a pseudonym, readers could neither assess the credibility of the assertions nor contact the sender for evidence of the charges. Nevertheless, the libelous assertions caused a steep fall in the value of stock and damaged the bank's business.

Hate Mail. Individuals may say things anonymously that they would not say if they believed they could be identified and held responsible for their statements. Messages that threaten or harass are generally sent anonymously. In one well-known example, in September 1996, Richard Machado, a former student at the University of California at Irvine, sent a number of e-mail messages threatening to "hunt down and kill" Asian students at the university. The message, signed "Asian hater," warned that all Asians should leave UC Irvine (Maharaj, 1997). Machado was eventually caught and convicted on civil rights violations.

Impersonation and Misrepresentation. While impersonating others may be socially acceptable in certain contexts, such as a costume ball or theatrical event, such behavior is illegal in many other circumstances where it could cause financial loss, physical or emotional harm. Online impersonation may deceive whole groups, such as the participants in a self-help newsgroup. Or an individual may gain access to someone else's account, and send hate mail, spread rumors, or engage in various illegal activities in that person's name.

People can also misrepresent themselves by using a fake identity (pseudonym). For example, a teenage girl calling herself "Kim" posted a series of fabricated messages to a newsgroup about her experience associated with the death of her premature baby. "Kim" misrepresented herself to gain sympathy, and members of the newsgroup responded with nurturing, care, and concern. Eventually, she was tripped up by her own lies and vanished. "Kim's" behavior had a negative effect on members of the group because she violated their trust. Members experienced hurt, anger, embarrassment, and suspicion of one another (Grady, 1998).

Van Gelder (1996) discusses a similar way in which the Internet enabled some people to develop unusually intimate friendships under false pretenses. In Van Gelder's account, a man by the name of Alex impersonated a disabled woman (whom he called "Joan") on CompuServe's "CB" channel. Many people trusted "Joan" and "she" developed relationships with several participants. The ease of online access to a special group of people aided Alex in perpetrating his fraud. His intentions were manipulative and largely self-serving. When participants discovered that they had been deceived, some experienced a strong sense of what has been termed "identity rape."

Online Financial Fraud. With the advent of electronic cash (e-cash), individuals can conduct online commercial transactions anonymously. Any individual or organization can set up a virtual commercial site to run a fraudulent business on the Internet, sell merchandise and/or information, and satisfy customers who are also virtual players (Froomkin, 1995a, 1996a, 1997). For example, Kevin Jay Lipsitz sold magazine subscriptions over the Internet but failed to deliver them to his customers. He was eventually found guilty of violating New York state consumer fraud laws (Swartz, 1997).

Other Illegal Activities. Conference participants identified several other types of illegal activities that could be conducted online with the aid of technologies that facilitate anonymity or pseudonymity. These included money laundering, illegal arms transactions, drug deals, criminal organizational recruitment, and theft of intellectual property. Since the nature of the Internet does not materially affect the criminality of such activities they were not the subject of much discussion at the meeting.

NEW CONTROVERSIAL ISSUES

The nature of the Internet poses huge barriers to the regulation of individual behavior, including anonymous communication. The openness, decentralization, and transnational character of the Internet all challenge the efficacy of traditional control mechanisms, including physical surveillance. As a result of its challenges to traditional means of regulation, the Internet has raised several new controversial issues.

Anonymity vs. Accountability

Societies have different practices related to anonymity and accountability in daily life. In Germany, citizens have to register with the police if they move, even within the same region. In the United States, such registration would be regarded as an infringement on individual rights under the Constitution. Even when Americans pay taxes, they do not have to reveal their true addresses—a post office box is perfectly acceptable. Many of the tensions between anonymity and accountability have been examined under the rubric of personal privacy and social control (see Kling, 1996b).

The link between anonymity and accountability raises special concerns. Because of the difficulty in holding individuals accountable for their statements and actions, anonymity can lead to the spread of conspiracy theories, encourage financial fraud, and make it possible to smear or victimize others sexually (Mossberg, 1995). Consider, for instance, using a computer in a public library, school, or Internet café where anyone can sit down at a computer and access the Internet without providing identification. An individual could create one or more free e-mail accounts from services such as Hotmail that operate on the World Wide Web. They could then send harassing or noxious mail in a manner that is virtually untraceable.

On the other hand, there are clearly circumstances in which anonymous communication can play a more positive role. For example, in a study of people providing evaluations, David Antonioni (1994) found that those who were required to identify themselves gave more positive evaluations than those whose who were allowed to give their responses anonymously. The not-too-startling implication is that anonymity produces more candid (and presumably more useful) evaluations.

Law Enforcement vs. the Nature of the Internet

In the physical world, anonymity can serve either as a "shield" or as a "sword." The law protects and sometimes encourages anonymity when it is used as a "shield" to guard individuals against abuse—for example in the federal witness protection program. If, however, anonymity is used as a "sword" to abet illegal or otherwise socially unacceptable activity, then the law may be used to regulate it. Issues raised by certain activities on the Internet, such as fraud, data theft, child pornography, privacy invasion, and copyright infringement, take on heightened importance because of the difficulties authorities face in trying to regulate online activities. These difficulties are often attributed to the characteristics of the Internet that serve to impede local and national as well as international efforts to stop criminal activities (Lee, 1998):

1. There are very low barriers to entry. Anyone with a computer, certain easily-obtainable software, a telephone line, and a modem can access the Internet.
2. The Internet provides many-to-many communication that the traditional media do not routinely offer.
3. Communication on the Internet was designed to be decentralized and free of direct human control. In other words, the Internet provides an arena for people to communicate and transmit messages with minimal, if any, constraints.
4. Information on the Internet is delivered quickly and at very low cost.
5. The Internet connects vast numbers of linked computer networks. The connections are not just national, but international as well. It is, as has often been said, a network of networks.
6. People can request or consume whatever they want and, with appropriate security, can do so with a relatively high degree of privacy.
7. In the absence of special measures, the Internet allows one easily and inexpensively to make an unlimited number of perfect copies of anything that can be digitized.
8. The Internet provides a nearly ideal setting for anonymous and pseudonymous communication.

The very nature of the Internet makes it virtually impossible to set up barriers among the computers that are connected to it and very difficult to trace true identities (Edelsten, 1996). As a result, governments are limited in their ability to identify and locate those responsible for illegal behavior and to impose punishment and compensate victims (Post, 1995). Remailers pose a special dilemma for law enforcement. If the number of remailers is relatively small, it might be possible for law enforcement authorities to analyze the traffic in and out of them and determine "who sent what to whom" (Froomkin, 1996a). (Some conference participants suggested that one strategy for law enforcement officials wishing to track anonymous messages might be to operate one or more remailers of their own. Others observed that there was no way of knowing whether this practice was not already in use.) Increasingly powerful encryption technology, however, will make it even harder to locate remailers and senders of anonymous messages.

Many conference participants noted that in a global society where the Internet knows no geographic borders, technology is very quickly outpacing any jurisdiction's ability to keep up with it. New technologies like Iridium, a satellite system that will permit high quality global wireless communication (Iridium LLC, 1997) and Teledesic satellite systems, a wireless networking company that operates a satellite that will offer high-bandwidth Internet services (Teledesic, 1998) make it very hard to control traffic going in and out of a country.

Some U.S. authorities have suggested that anonymous communication might be controlled by holding operators of remailers liable for any harm that might result from messages transmitted through their servers. The recently enacted Digital Millenium Copyright Act of 1998 includes provisions for such liability for online service providers, but also provides for a number of ways that service providers can avoid or limit their exposure to liability (Public Law No. 105-304, October 28, 1998). With easy Internet access through satellite systems, however, remailers could simply move offshore. Indeed, one of the earliest and best-known remailers (no longer in operation) was located in Finland. Even if the law breaker is located with the aid of remailer services and the courts, the violator may not be reachable if he or she is outside the jurisdiction of the court (Froomkin, 1995a; Edelsten, 1996). It may be difficult, if not impossible, to regulate the use of online anonymity on such an open and interactive system. Nevertheless, Froomkin (1996a) has suggested that bilateral or multilateral agreements between countries may be good national strategies to regulate the abuse of anonymity.[6] Differences among nations' legal systems will need to be dealt with if such approaches are going to work.

Security and Privacy

Remailer technologies and cryptography increase the security of anonymous e-mail and enhance personal privacy in online communication, as described above. Nevertheless, security and privacy of individual messages depend critically on the willingness and ability of remailer operators to protect the confidentiality of their records (Levy, 1994; Froomkin, 1995a).

An example of dependence on a trusted intermediary (in this case, a service provider), and the consequences of its violation is demonstrated by the case of Timothy McVeigh (no relation to the individual convicted of the bombing of the Oklahoma City federal building). In fall 1997, a female Navy employee discovered an America Online member listing for McVeigh, a member of the U.S. Navy who posted his marital status as "gay" in his online autobiographical sketch. She reported it to Navy officials who pressed AOL to reveal McVeigh's identity. Without a warrant, subpoena, or court order, AOL revealed the identity of Timothy McVeigh, a 36-year-old sailor. McVeigh was subsequently discharged (Abate, 1998; Napoli, 1998a; Rich, 1998). While the court eventually ruled that McVeigh should be allowed to return to his duty station in Hawaii (Napoli, 1998b), his case became a symbol for online privacy.

In a legal sense, privacy is the "right to be let alone" (Liu, 1997, pp. 294–295),[7] a "right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures" (Liu, 1997, pp. 297),[8] and a right of individual interest in avoiding disclosure of personal matters (*Whalen v. Roe*, 1997). As the Internet evolves into a mass medium, users are finding it increasingly difficult to preserve the right of autonomous choice in concealing or disclosing personal information, and may have to live with the erosion of their informational privacy.

Anonymous Communication and Encryption: Governmental Empowerment

Encryption technologies are used to provide several crucial functions in online communication. Most often, encryption is used to ensure confidentiality of transmitted information, allowing a message to be scrambled such that only the intended recipient can easily unscramble it (Post, 1995). It enhances privacy by ensuring the confidentiality of personal records, such as medical information, personal financial data, and electronic mail (Madsen, 1998). Cryptographic techniques can also be used to provide authentication of the identity of a message originator (i.e., a recipient of a message can verify that the person who claims to have sent a document really is the sender—this is often called a *digital signature*) and to verify data integrity (i.e., that the message received is the same as the message that was sent, and thus that the message was not accidentally or intentionally changed in transit). Finally, encryption can be used to ensure the non-reputability of messages. This means that the sender of an electronic message (a purchase order, a contract, a threat) cannot deny having been the sender (Certicom, 1997). The primary implication of cryptography for anonymous communications is that encryption can be used to hide both message content and the sender's identifying information, preventing an eavesdropper from determining the message content and/or the sender's identity.

Disputes have arisen between the law enforcement and intelligence communities' interests and the interests of privacy advocates with respect to the use of and regulation of encryption technologies. The Clinton administration has argued that unregulated use of encryption can lead to the widespread exploitation of the Internet for criminal activity, and thus supports the regulation of encryption technologies through export controls (Suro & Corcoran, 1998). A coalition of privacy, commercial, and human rights groups have contested the Administration's proposals (Corcoran 1998a). Toward the end of 1998, the administration scored a victory in its efforts to limit the use of encryption technology abroad when the United States and 32 other countries reached an understanding that would restrict exports of such technologies from their countries (Corcoran, 1998b).

E-commerce

The picture with respect to the role of anonymity in online commerce is mixed. The Internet allows people to conduct commercial transactions without disclosing their identities, as they might by paying cash in a retail store in which they are not known to the salesclerk. However, relatively few Internet users employ such means, and those who use credit cards and otherwise do not seek to disguise their identities are subject to various kinds of surveillance by service providers, content providers, sellers, and public and private organizations. By collecting data from a variety of sources they are able to discern buying patterns and viewing habits of Internet users. "Data owners" can manipulate the collected data, sorting, for example, by income, address, age, purchasing habits and preference, gender, and interests, and sell the databases in the market. As a result, the buying habits and personal characteristics of Internet users are increasingly being studied and used by marketers, and individuals whose names are included in such databases are being targeted for junk mail and other unwanted information.

Anonymous communication technologies may serve as tools through which people can combat the compilation and analysis of their personal information by others (Froomkin, 1996a). The availability of anonymous e-cash enables people to conduct transactions without revealing their actual identities,[9] thereby reducing opportunities for others to maintain dossiers on their identity, buying preferences, and habits (Froomkin, 1996a and 1997; McDevitt, 1997).

The widespread use of encryption technology also offers new opportunities for criminal activity. Not only do innocent people enjoy the privacy that digital currency offers, but criminals also benefit. For example, a kidnapper could ask the victim's family to issue anonymous digital cash and pick up the ransom without being revealed. Or an organization or person could establish a web site to sell goods, collect digital cash, and disappear without delivering the goods to buyers. Anonymity clearly threatens the enforcement capability of national authorities. It is not surprising, therefore, that many governments wish to ban anonymous digital cash. However, any restriction on anonymous e-cash may also place a chilling effect on anonymous speech (Froomkin, 1996a) and impinge on personal privacy. Consider the possibility that customers have to pay with e-cash in order to participate in a newsgroup, view pornographic materials, or read fee-based text. If e-cash is not used anonymously, records of their participation and reading habits could be compiled and sold by service content providers. Imagine that customers must reveal their identity (or part of their identity) whenever they ask the bank to issue digital cash and whenever they spend the cash. Their records would be readily subject to manipulation. Balancing the use of anonymity to protect personal privacy with the government's mandate to prevent crime is one of the challenges heightened by the relatively easy use of anonymous communication on the Internet.

ONLINE AND OFFLINE ANONYMOUS COMMUNICATION

One major issue that arises frequently in discussions of anonymous communication on the Internet is the extent to which the social conventions and legal traditions that govern anonymity/pseudonymity in other areas of life can serve as models for online anonymity. The right to communicate anonymously is closely associated with freedom of speech, freedom of assembly, and right to privacy. Some anonymous speech has been protected under the roof of the First Amendment for years (Froomkin, 1996a and 1997). In the United States, both political and non-political speech receive First Amendment protection, with political speech usually receiving the highest constitutional protection (Froomkin, 1995b; 1996b; 1997).[10] A recent Supreme Court decision (*McIntyre v. Ohio Elections Commission,* 1995, at 1516) has confirmed that "an author's decision to remain anonymous... is an aspect of the freedom of speech protected by the First Amendment."

There are at least two important differences between online anonymity and offline anonymity: (1) Mass dissemination—the Internet raises the stakes because it is much easier and less expensive to reach large numbers of people online than it is by more conventional media; and (2) Persistence—electronic messages may remain undetected in many locations on the Internet far longer than the sender (or anyone else) expects. Even if a user deletes a message, it can often be found through a log and rebroadcast.

Concerned about possible abuses of anonymity on the Internet, some observers support a policy that prohibits or strictly regulates anonymity on the grounds that it empowers people who use the Internet to do substantial harm to others. People holding this view might advocate that remailers be forced to discontinue their services if their operators cannot guarantee that no harmful messages will be transmitted and if they are unable or unwilling to provide recipients with the identities of the originators of messages they forward. Such a policy would make Internet communication more restrictive than other common, everyday forms of communication. Telephone operators do not monitor calls, nor are they required by law to reveal information without a warrant about where calls originated. Postal workers deliver mail without having to guarantee that the content of the mail is not harmful. The Postal Service does not make any attempt to authenticate return addresses. Why, then, should authentication always be required on the Internet? In the physical world, if the authorities have done nothing to prevent the fraud or deception conducted in other media, especially print media, why should they do so with Internet communication?

Participants at the AAAS conference debated the extent to which the social conventions and legal traditions that govern anonymity and pseudonymity in non-Internet life should be used as guidelines for the Internet. Some participants argued that computer-mediated communication washes out many cues, clues, and indicators of authenticity that are routinely available in face-to-face settings (or even telephone interactions). It puts trustworthiness at risk. Others argued that the sheer volume of communication via the Internet is too overwhelming to sift through it all, and that fine-grained surveillance tools radically reduce privacy. However, participants agreed that people have higher expectations for electronic communication than they do for other forms of communication. The "default" for online anonymity policy, most agreed, should be free speech. Limitations on anonymous communication should be no more restrictive than the provisions of the Universal Declaration of Human Rights (UDHR) that apply to free speech.[11] Some conference participants also argued that policy should reflect the views and experience of those who would be most harmed or threatened by reductions in anonymous communication (e.g., human rights groups).

CONCLUSION

Anonymous communication on the Internet offers opportunities and risks related to how people exchange information and communication. The deliberations at the AAAS conference helped to clarify important concepts of anonymous communication and explain how technologies work to conceal identity on the Internet. Controversial issues that the Internet has raised were discussed by comparing them to anonymous communications in the offline world.

Anonymous communication is neither intrinsically bad nor intrinsically good. There are situations in which anonymity is to be encouraged, desired, or at least tolerated. Anonymous communication may help or encourage people to determine the truth or falsity of allegations (in the case of journalism, for example); blow the whistle on illegal or unethical behavior in an organization by reporting problems, violations, and actions; obtain help from social service providers; protect their personal privacy; and avoid persecution by oppressive regimes. Anonymity also carries risks. Because accountability is diminished, it can be abused to send electronic junk mail; to deceive, as well as impersonate others; to send hate mail; and to engage in illegal activities. Organizations and on-line groups have the right to insist that their participants' electronic communications are not anonymous. In practice, some on-line groups insist that their members be personally identifiable, while others encourage anonymous communications.

However, governments are challenged to enforce laws on the Internet and regulate online anonymous communication. Yet, to ban or restrict *all* anonymous communication online because of the harms it could bring would deny its benefits to those people who may legitimately gain from it.

Although there was an unresolved debate at the AAAS conference about the extent to which the social conventions and legal traditions that govern anonymity and pseudonymity in the physical world should be used as guidelines for the Internet, participants generally seemed to favor policies related to online anonymity in accordance with internationally developed principles of human rights.[12] Although no formal polls or votes were taken, it was evident that most felt it was premature, unnecessary, probably harmful from the standpoint of individual rights, and perhaps fruitless for governments to attempt to impose restrictions on anonymous communications. The presumption underlying this consensus was that anonymous communication on the Internet should be permitted to the extent that technology allows and that the burden of proof rests with those who would seek to limit it.

NOTES

1. See AAAS's Web site for the detailed information about the project *http://www.aaas.org/spp/anon/project.htm*. See Teich, et al. (1999), "Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference," in this issue for policy recommendations drawn from the AAAS project.

2. The survey form is avialable at <http://shr.aaas.org/anonsrv1.nsf/$defaultform>

3. American Association for the Advancement of Science (AAAS) Conference on Anonymous Communications on the Internet was held on November 21–23, 1997. This invitational conference was workshop-style and was hosted by the University of California at Irvine's Department of Information and Computer Sciences and the Center for Research on Information Technology and Organizations.

4. Even these techniques are not perfect, however. See Cottrell (1996b) for more information about the vulnerabilities and intended future enhancements to the Mixmaster service.

5. Anyone online can set up an e-mail account with a pseudonym or several accounts with different pseudonyms.

6. INTERPOL is an example of multilateral agreement that includes 177 member countries. In the case of *Church of Spiritual Tech. v. Helsingius* (1996), the Church claimed that its copyrighted work was posted through Helsingius' anonymous remailer server. The FBI requested the Finnish police to obtain a search warrant, and retrieved the name of the originator through INTERPOL.

7. Liu, Ching-Yi, quoting from Warren & Brandeis. (1890).

8. Liu, Ching-Yi, quoting from U.S. Constitution, Amendment IV.

9. Most of the ventures that have proposed e-cash have worked on designs that support (one-way) anonymous transactions. There is some debate about the extent to which e-cash is necessarily anonymous or even that the protections of one-way anonymity are realizable in practice (Phillips, 1996). Online shoppers could use anonymous e-cash from a virtual bank to make purchases with a digital signature. For details about technologies of digital cash and digital signatures, see Certicom (1997) and Cobb (1996).

10. Froomkin (1997) develops an exhaustive analysis of several legal cases and their implications for the regulation of anonymity. He concludes that even though political speech receives the highest constitutional protection, the misuse of anonymity is still subject to regulation.

11. See the discussion about using Universal Declaration of Human Rights as a foundation for policy relating to anonymous communication in the article. See Teich, et al. (1999), "Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference," in this issue.

12. See Teich, et al. (1999), "Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS conference," in this issue.

REFERENCES

Abate, Tom. 1998. Online privacy on stage. *San Francisco Chronicle*, 20 January, B3.

American Civil Liberties Union of Georgia v. Zell Miller. 1997. Civil Action 1:96-cv-2475-MHS [online]. Available from World Wide Web: <http://www.aclu.org/court/aclugavmiller.html> (last visited on 4 February 1998).

Antonioni, David. 1994. The effect of feedback accountability on upward appraisal ratings. *Personnel Psychology* 47(2):349–357.

Arar, Yardena. 1994. Techno-babble spotlighting the computer world "most hated" couple beefs up online "spamming," *L.A. Daily News*, 28 November, at L5.

Bacard, Andre. 1996. Anonymous Remailer. In *Computer Privacy Handbook* [online]. Available from World Wide Web: <http://www.well.com/user/abacard/remail.html> (last visited on 17 January 1998).

Bernstein, Judith H. 1995. Attack of the killer spam—been spammed? It likely won't be the last time so be prepared. *Netguide*, 11 November, at 91.

Certicom. 1997. An introduction to information security. In *ECC Whitepapers* [online]. Available from World Wide Web: <http://www.certicom.com/ecc/wecc1.html> (last visited on 29 January 1998).

Church of Spiritual Tech. v. Helsingius [online]. 1996. Available from World Wide Web: <http://www.cybercom.net/~ rnewman/Scientology/home.html#PENET> (last visited on 2 February 1998).

Clausing, Jeri. 1998. U. S. puts junk e-mailers on notice. In *New York Times Interactive* [online]. Available from World Wide Web: <http://www.nytimes.com/library/cyber/week/020698spam.html> (last visited on 6 February 1998).

Cobb, Chey. 1996. Security issues in internet commerce. In *NCSA White Paper on Internet Commerce* [online]. Available from World Wide Web: <http://www.monopoly.org/library/inetsec2.html> (last visited on 29 January 1998).

CompuServe Inc. vs. CyberPromotions. 1997. C.S. No. C2-96-1070.

Corcoran, Elizabeth. 1998a. Ads to target encryption curbs. *Washington Post*, 4 March, C15.

———. 1998b. Encryption curbs backed by 33 nations. *Washington Post*, 4 December, D1.

Cottrell, Lance. 1996a. *Mixmaster and Remailer Attacks* [online]. Available from World Wide Web: <www.obscura.com/~ loki/remailer/remailer-essay.html> (last visited on 17 January 1998).

———. 1996b. *Frequently Asked Questions about Mixmaster Remailers* [online]. Available from World Wide Web: <www.obscura.com/~ loki/remailer/mixmaster-fap.html> (last visited on 17 January 1998).

Diffie, Whitefield, and Susan Landau. 1998. *Privacy on the Line: The Politics of Wiretapping and Encryption*. Cambridge, MA: Massachusetts Institute of Technology.

Edelsten, Jonathan I. 1996. Anonymity and International Law Enforcement in Cyberspace. Fordhan Intellectual Property, Media and Entertainment Law Journal. 7:231.

Foner, Lenny. 1996. *Anonymity and Pseudonymity* [online]. Available from World Wide Web: <http://foner.www.media.mit.edu/peo...-Theory-and-the-Net/anonymity.html> (last visited on 17 January 1998).

Froomkin, A. Michael. 1995a. Anonymity and its enmities. *Journal of Online Law* 4:1–27.

———. 1995b. The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution. *University of Pennsylvania Law Review* 143:709–810.

———. 1996a. Flood control on the information ocean: Living with anonymity, digital cash, and distributed database. *Journal of Law and Commerce* 15(2):395–507.

———. 1996b. It Came from Planet Clipper: The Battle over Cryptographic Key Escrow. *Law of Cyberspace Issue of the University of Chicago Legal Forum* [online]. Available from World Wide Web: <http://www.law.miami.edu/~ froomkin/articles/clipper.htm> (last visited on 8 February 1998).

———. 1997. *Legal Issues in Anonymity and Pseudonymity.* Paper presented to AAAS Conference on Anonymous Communications On the Internet, Irvine, California.

Grady, Denise. 1998. Faking pain and suffering in internet support groups. *New York Times*, D1.

Iridium LLC. (1997). IRIDIUM, LLC announced launch of the first five IRIDIUM satellites. In *PR News Wire via Dow Jones* [online]. Available on the World Wide Web: <http://www.mot.com/General/Press/PR970506.html> (last visited on 9 April 1998).

Kansas City Star. 1994. Business in Brief. In *Kansas City Star*, 11 November, B2.

Kling, Rob (Ed.). 1996a. *Computerization and Controversy: Value Conflicts and Social Choices* (2nd ed.). San Diego: Academic Press. (See *http://www-slis.lib.indiana.edu/kling/cc/index.html*).

Kling, Rob. 1996b. Information technologies and the shifting balance between privacy and social control. In Kling, Rob, (Ed.), *Computerization and Controversy: Value Conflicts and Social Choices* (2nd ed.). San Diego: Academic Press.

Lee, Gia B. 1995. *Addressing Anonymous Messages in Cyberspace* [online]. Available from World Wide Web: <http://www.ascusc.org/jcmc/vol2/issue1/anon.html> (last visited on 18 January 1998).

Lee, Ya-Ching. 1998. Toward a more balanced online copyright policy. *Communications and the Law* 20(1):37–59.

Levmore, Saul. 1996. The Anonymity Tool. *University of Pennsylvania Law Review* 144(5):2191–2236.

Levy, Steve. 1994. Anonymously yours—Part 2 how to launder your e-mail. In *Wired Magazine* [online], 2.06. Available from World Wide Web: <www.hotwired.com/wired/2.06...nts/electrosphere/anonymous.2.html> (last visited on 17 January 1998).

Lewis, Peter H. 1994. Computer jokes and threats ignite debate on anonymity. *New York Times*, 31 December, D1.

———. 1996. Behind an Internet Message Service's Close. *New York Times*, 6 September, D2.

Liu, Ching-Yi. 1997. *The Regulation of Cyberspace: Computer Technology, Law, and Self-regulation on the Internet.* Ph.D. Dissertation. The University of Chicago: Chicago, IL.

Madsen, Wayne. 1998. Cryptography and liberty: An international survey of encryption policy. In *A Report for the Global Internet Liberty Campaign* [online]. Available from World Wide Web: <http://www.glic.org/crypto/crypto-survey.html> (last visited on 15 February 1998).

Maharaj, Davan. 1997. UCI Internet Hate Mail Case Ruled a Mistrial. Los Angeles Times, 22 November, A1.

Marx, Gary T. 1999. What's in A Name? Some Reflections on The Sociology of Anonymity. *The Information Society* 15(2):99–112.

McDevitt, Gavin. 1997. Legal regulation and internet commerce: An analysis of anonymous digital currency. In *Computer Law* [online]. Available from World Wide Web: <http://www.law.stetson.edu/courses/gmcdevitt.htm>(Last visited on 1 February 1998).

McIntyre v. Ohio Elections Commission. 1995. 115 S. Ct.

Mossberg, Waler S. 1995. Personal technology: Accountability is key to democracy in the online world. *Wall Street Journal*, 26 January, B1.

Napoli, Lisa. 1998a. AOL admits error in sailor's case. In *New York Times Interactive* [online]. Available from World Wide Web: <http:// www.nytimes.com/ library/ cyber/ wek/ 012198navy.html> (last visited on 22 January 1998).

———. 1998b. Federal judge halts sailor's discharge case. In *New York Times Interactive* [online]. Available from World Wide Web: <http://www.nytimes.com/ library/ cyber/ week/ 012698navy.html> (last visited on 26 January 1998).

Phillips, David. 1996. "The Construction of Routine Surveillance Practice in the Electronic Marketplace—Socio-technical Negotiations Around Digital Cash Systems" Communication Technology Policy Section of the 20th AIERI/IAMCR/AIECS Conference & General Assembly, Sydney, Australia, August 18–22,1996 (at http://www.komdat.sbg.ac.at/ectp/PHIL_P.HTM).

Post, David. 1995. *Knock Knock, Who's There?: Anonymity and Pseudonymity in Cyberspace* [online]. Available from World Wide Web: <http://www.cli.org/DPost/X0012_KNOCK.html> (last visited 17 January 1998).

Rich, Frank. 1998. The 2 Tim McVeighs. *New York Times*, 17 January, A13.

Seminerio, Michael. 1997. AOL Slams Two More Spammers. In *MSNBC* [online]. Available from World Wide Web: <http://www.msnbc.com/news/139959.asp>(last visited on 1 February 1998).

Suro, Roberto, and Elizabeth Corcoran. 1998. U.S. law enforcement wants keys to high-tech cover. *Washington Post*, 30 March, A4.

Swartz, Jon. 1997. Scam artists thriving on the internet. *The San Francisco Chronicle*, 20 December, E1.

Teich, Al, Mark S. Frankel, Rob Kling, and Ya-Ching Lee. 1999. Anonymous Communication Policies for the Internet: Results and Recommendations of a AAAS Conference. *The Information Society* 15(2):71–77.

Teledesic. 1998. Visualizations of the teledesic network. In *Teledesic Home Page* [online]. Available on the World Wide Web: <http://www.teledesic.com/technology.html>(last visited on 21 May 1998).

Van Gelder, Lindsy. 1996. "The Strange Case of the Electronic Lover: A Real-Life Story of Deception, Seduction, and Technology." In Kling, Rob (Ed.), *Computerization and Controversy: Value Conflicts and Social Choices* (2nd ed.). San Diego: Academic Press.

Warren, Samuel, and Louis Brandeis. 1890. The Right to Privacy. *Harvard Law Review* 4:193–211.

Whalen v. Roe. 1977. 429 U.S. 589.