ANONYMOUS COMMUNICATION POLICIES FOR THE INTERNET: RESULTS AND RECOMMENDATIONS OF THE AAAS CONFERENCE

Al Teich**, Mark S. Frankel**, Rob Kling*, Ya-ching Lee*

*Center for Social Informatics
Indiana University
Bloomington, IN 47405

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

Version 14/ January 27, 1999

For *The Information Society* 15(2)

ABSTRACT

The Internet offers new opportunities for anonymous and pseudonymous communications. Users can, for example, engage in political advocacy, receive counseling, and perform commercial transactions without disclosing their identities. The cloak of anonymity can also facilitate socially unacceptable or criminal activities because of the difficulty in holding anonymous users accountable. This paper reports the results of a conference on anonymous communication organized by the American Association for the Advancement of Science. Among the findings were that online anonymous communication is morally neutral; that it should be considered a strong human and constitutional right; that online communities should be allowed to set their own policies on the use of anonymous communication; and that individuals should be informed about the extent to which their identity is disclosed online. The paper discusses how anonymous communications can be shaped by the law, education, and public awareness, and highlights the importance of involving all affected interests in policy development.

I. INTRODUCTION

In less than a decade, the Internet has dramatically changed the way people communicate and live. In 1990, few people outside the research community had heard of the Internet. In 1998, it is estimated that nearly 113 million people in virtually every country in the world are using the Internet. More than half – some 62 million –are in the United States alone (Nua, 1998). There are several reasons for the phenomenally rapid growth of the Internet: It gives individuals the ability to communicate directly, easily, and inexpensively with each other across time and space. It allows people to transmit text,

voice, data, image, and video information from one point to another. It increases access to diverse information and entertainment resources that are delivered quickly and economically anywhere. And, most importantly, it facilitates interactive human communications.

The appeal of Internet communication depends in part on its capacity to support anonymity. Internet users can make political claims as well as non-political comments, engage in whistle-blowing, conduct commercial transactions, and consume sexual materials without apparently disclosing their identities. All of these examples illustrate improved freedom from detection, retribution, and embarrassment. As a result, people may feel more comfortable communicating with strangers and exchanging confidential information. In other words, anonymous communication encourages Internet communications, and the Internet in turn may encourage anonymous communication.

While many people believe that anonymous communication on the Internet is not only acceptable but has positive value, others see risk in it because anonymous users are not accountable for their behavior. Consequently, anonymity can mask or even encourage criminal or anti-social behavior.

To address the problem of how to foster socially-desirable uses of anonymous communication online while discouraging undesirable uses, the American Association for the Advancement of Science (AAAS), through its Program in Scientific Freedom, Responsibility and Law, held an invitational conference in Irvine, California, in November 1997.[1] This conference brought together experts from the computing industry,

the legal community, professional societies, academic institutions, human rights organizations, and law enforcement agencies in an effort to better understand the nuances of anonymous communication on the Internet and to develop ideas which can guide policy development in this area.

This paper reports the results of the AAAS conference. While the conference used no formal process for formulating recommendations or reaching consensus about policies, the discussions converged on many key ideas. In this paper we identify areas where there seemed to be a reasonable degree of consensus among the conference participants. The broad principles and practical suggestions discussed here are the authors' interpretations and do not necessarily reflect the views of *all* conference participants.

A companion paper in this issue of *The Information Society*, "Assessing Anonymous Communication on the Internet" (Kling et. al., 1999),[2] examines some of the fundamental ideas and controversies over anonymous communications that the participants discussed during the conference. It also describes a rich set of materials that Drs. Mark Frankel and Al Teich and their colleagues provided for the conference participants, including a survey, reports from focus groups of professionals, and specially commissioned background papers. That paper examines many of the details of anonymous communication, such as the extent to which people who use pseudonyms can be traced, and the nature of identity disclosure when using e-mail or browsing the World Wide Web.

In face-to-face interaction, we have visual and auditory clues about the person we encounter. In online interaction, however, the text-based content lacks many of the cues on which we normally rely, and our common-sense might mislead us (Sproull & Kiesler, 1992; Marx, 1999). Conference participants generally believe that people have legitimate reasons to engage in anonymous communication and to avoid the consequences of identity revelation. Yet the abuses of anonymity, including libel, impersonation, online fraud, spam, hate mail, and various criminal activities in the virtual environment, have led to calls for regulation.

The participants in the conference acknowledged the harmful consequences of abuses of anonymous communication. However, they concluded that the complexity of online anonymous communication makes the formulation of policy difficult in two ways. First, there is a need to mitigate the harm resulting from online anonymity while preserving its positive aspects. That is, how can we balance the benefits and costs? Second, there is a problem of effectively enforcing regulations on anonymous communication, since the originators of such messages are, by definition, anonymous.

The next section describes four principles that, in the view of conference participants, could provide a framework within which policy development might take place. The concluding section discusses the pros and cons of various practical steps that might be taken to deal with the issues raised by anonymous communication online.

II. PRINCIPLES FOR POLICIES ON ANONYMOUS COMMUNICATION ONLINE

A fundamental perspective that was shared by virtually all conference participants is that the ability to communicate anonymously is a particularly valuable feature of the Internet and that, as regulatory regimes and policies for Internet communication evolve, efforts should be made to preserve it.

Participants recognized that there are ways in which anonymous communication can be misused for harmful, unethical, immoral, or even criminal purposes. No one disagreed with the proposition that such uses should be discouraged and that perpetrators of such uses should be punished by means appropriate to the specific cases. Nonetheless, the consensus view of the conference was that the positive value of anonymous communication more than offsets these dangers. With this in mind, discussions coalesced around several principles that, in the view of conference participants, should help shape future policies on anonymous communication online.

A. Anonymous communication online is morally neutral.

It is important to distinguish among uses and types of anonymous communication so that the evils of one form do not serve as reasons for unnecessarily restricting others. Under some circumstances, anonymous communication can encourage people to be more forthcoming, to provide valuable information with which they might not wish to have their names associated (e.g., anonymous tips by whistleblowers), and to use resources they might not otherwise use (e.g., drug abuse, AIDS, or suicide hotlines). Nonetheless,

individuals can use anonymous communication to cause harm to others. As legitimate anonymity comes into wider use, illegitimate uses become more common and easier as well. Policies should seek to prevent harmful or destructive uses of anonymous communication while facilitating those that are socially desirable.

B. Anonymous communication should be regarded as a strong human right; in the United States it is also a constitutional right.

Participants at the AAAS Conference discussed frameworks for evaluating anonymous communication practices on the Internet. The Universal Declaration of Human Rights (UDHR), adopted by the General Assembly of the United Nations in December 1948, was proposed as a useful approach in that it is regarded as a common standard of achievement for all peoples and all nations to promote respect for the rights and freedoms that it enumerates.[3]

The UDHR contains several provisions that protect the ability of individuals to communicate anonymously. Key among these are Article 12, which governs freedom from interference with privacy, home, and correspondence[4], and Article 19, which provides for freedom of opinion and expression and the right "to seek, receive, and impart information and ideas through any media and regardless of frontiers." With regard to Internet communication, these articles suggest that recipients have the right to choose to accept or refuse anonymous messages and that individuals do not have the right to impose messages upon an unwilling recipient. At the same time, law enforcement agencies and commercial interests do not have the right to interfere with individual privacy in electronic communication, regardless of whether it is anonymous or not.

Closely related to these provisions of the UDHR is the First Amendment of the U.S. Constitution, which guarantees the right of free speech to all Americans. The First Amendment applies equally to communications in which the initiator is identified and to those that are sent anonymously. (*McIntyre v. Ohio Elections Commission*, 1995)

In view of these protections, participants in the AAAS conference considered the right to communicate anonymously to be a "strong right" that deserves priority over other rights in most cases. Nevertheless, no right is absolute. The "default condition" on the Internet should be free speech, and as such, there must be channels for anonymous communication. Any ban on online anonymous communication would affect freedom of speech and impinge on personal privacy and security. Therefore, any limitations on anonymity should not be more restrictive than rights to free speech outlined in the UDHR. Those who propose to restrict this right in any way must assume the burden of proof and must fulfill that burden to the highest level.

C. Online communities should be allowed to set their own policies regarding the use of anonymous communication.

Individuals and organizations, including online forums, online services, and Internet service providers, should, in general, be allowed to determine the circumstances under which anonymity is permitted in communications using their facilities. Forums for communication, such as newsgroups, chat rooms, as well as universities and corporations, should be encouraged to develop, adopt, and implement their own policies and practices regarding anonymity. Individuals (and organizations) should have available a full range of anonymous communication options and strategies and should be

free to determine the degree to which they wish to be identified or remain anonymous when they engage in voluntary interactions. A key condition is mutuality – that is, people should be treated like "consenting adults."

Those who do not wish to receive anonymous electronic communications should be protected. Such protection is currently available by technical means in limited ways, but each way has its costs. For example, users can manipulate their incoming messages by filtering out messages from anonymous remailers (Lee, 1995). When a message from an anonymous remailer is identified, the computer will automatically delete it (Long, 1994; Lee, 1995). Filtering software can block unwanted messages, but it may also accidentally block messages that the user might wish to receive. Under most circumstances, allowing individuals to make their own choices will be preferable to legislation that seeks to regulate anonymous communication.

D. Individuals should be informed about the ext+ent to which their identity is disclosed online.

Closely associated with the principles of self-determination and informed consent is the principle of "transparency." Internet users should be clearly informed about the degree of anonymity, privacy, or confidentiality available in any online community which they enter or join. Individuals should be fully informed about the conditions under which they are communicating in an informed consent provision upon subscribing to an online service and any time the policy changes. Policies should be clear and public. The conditions under which confidentiality applies and anonymity is allowed and/or

supported, and the conditions under which individual identity will be disclosed, should be made known to all who might be affected.

III. PRACTICAL MEASURES

A. Anonymity and the Law

1. Anonymity and cryptography

Probably the most vexing policy issues encountered by conference participants were those involving cryptography. Both legitimate and illegitimate users of anonymous communication (e.g., human rights activists and terrorists) use encryption in conjunction with remailers. Encrypting a message facilitates anonymous communication by protecting the contents of the message as well as the identity of the sender. Some conference participants argued, in fact, that without strong encryption, Internet communication cannot be truly anonymous.

Thus, many participants took the position that the federal government, which is currently seeking to regulate the availability of strong encryption technology, should desist from these efforts, thereby facilitating its general availability. Banning or limiting the use of strong cryptography not only produces chilling and harmful effects on freedom of speech and intrudes on privacy, according to this view, but it also opens the door to government surveillance and, in some cases, to political repression.

On the other hand, if strong encryption technology is available to legitimate users, it is also available to those who would use it to break the law – for example, drug dealers and money launderers. The Clinton Administration's response has been to propose a system

under which it would maintain, in escrow, a key that would allow it to break encrypted messages under carefully controlled (presumably court-sanctioned) conditions. Advocates of encryption technology regard this as an unacceptable limitation on anonymity and privacy in communications. Though the issue has remained unresolved, some conference participants favored a policy allowing people who use the Internet to have access to strong encryption to ensure as much communications security and anonymity as possible. Unless criminality is involved or the victims complain or decide to engage in legal action against the originator of an anonymous message, law enforcement authorities should be forbidden to crack any coded message. Under such an approach, only a court-issued search warrant or subpoena would permit the authorities to break encrypted messages and trace the initiator of the anonymous messages.

To our view, this is consistent with USACM's [5] long-held belief that promoting the widespread use of strong encryption would be in the best interests of the U.S. (Landau, et al., 1994a; Landau, et al., 1994b; USACM, 1994; USACM & IEEE/USA, 1996; USACM, 1997a; USACM, 1997b), because encryption protects the security and privacy of communications, data storing, and electronic commerce (USACM, 1997b), and it enables people to communicate in privacy (Landau, et al., 1994b).

2. Regulation of remailers

The role played by remailer operators is critical in sorting out the issues of online anonymous communication. One possible means of restricting the flow of harmful (e.g.,

harassing or threatening) messages would be hold remailer operators responsible for the content of the messages that they relay.

However, most remailer operators are volunteers or hobbyists who run their remailers as a public service. In general, they do not receive any compensation for providing their services. The prospect of remailer operators exercising control over the content of the messages that flow through their remailers, whether those messages are encrypted or not, seems remote (Froomkin, 1996). The volume of data is simply too great. The time and effort involved (and therefore the costs) and the delays that would result would undermine the viability of the remailers.[6] Moreover, from the point of view of conference participants, such a review would constitute surveillance and monitoring and impinge on user privacy.

Even if such monitoring were feasible and considerations of user privacy were set aside, it is unlikely that remailer operators could judge whether a given message was harmful in the absence of its full context. For example, in *Church of Spiritual Tech. v. Helsingius*, Erlich, a user, with an anonymous e-mail account at "anon.penet.fi," posted the contents of a file copyrighted by the Church of Scientology to a Usenet group named "alt.religion.scientology" (Edelsten, 1996; Lewis, 1996). Erlich's purpose for posting was to critique the church's teachings. In response, the Church of Scientology claimed copyright infringement, and the provider, Helsingius, had to choose to release the user's identity to Finnish police.

The notion of holding remailer operators liable for damages that might result from messages that pass through their servers was discussed, but dismissed by most participants as tantamount to closing down these operators. Some additional discussion was devoted to the idea of requiring remailer operators to maintain logs of incoming and outgoing messages as means of providing law enforcement officials (with appropriate search warrants or subpoenas) with the ability to trace illegal activity, but no consensus was reached on this idea.

3. Punishing the sender for violations

The rationales for protecting online anonymous communication and prohibiting abusive uses of anonymity are the same on the Internet as in physical settings. For example, in *Griset v. Fair Political Practices Comm'n*(1994), Griset had sent a pseudonymous mailing containing a false statement of support by a non-existent neighborhood association. The court decided that this deception was harmful to the state's interest and banned it. The same logic should apply in the case of Internet anonymity: when the effects of anonymous communication do harm to individuals, organizations, or the state, regulation of such communication is necessary.

The abusive use of online anonymous communication should not be tolerated because in addition to the harms it causes people, it also hinders the development of Internet communication which heavily depends on mutual trust and respect. Conference participants favored a narrowly-tailored regulation of online anonymous communication: the law should hold the initiator of a defamatory message accountable for any negative

consequences associated with it. That is, if anonymous communication is used for illegal purposes, the originators of the anonymous message should be punished.

4. International dimensions of the problem

As in many debates on policies relating to the Internet, discussions of policy prescriptions at the AAAS conference came up against the largely intractable problem of the Internet's global nature. All of the legal approaches discussed –from controlling the availability of cryptographic software to regulating the activities of remailer operators to holding the originators of harmful messages responsible for their actions –are limited in their effectiveness by question of jurisdiction. The very nature of the Internet makes it virtually impossible, except in the most totalitarian societies, to control the flow of messages. Thus, activities which are banned in the United States can often be conducted with impunity outside our borders and made available to U.S. Internet users with relatively little inconvenience. For example, federal regulations forbid the export of the strongest cryptographic software, but these products are freely available from Web sites in Norway and The Netherlands. Remailers operating in almost any country can be used by people in almost any other country.

Participants believed that some form of international agreement may be the ultimate solution to controlling crime and harmful activities on the Internet. They proposed that the United States urge other countries to adopt policies that strictly define standards as well as means used to disclose the sources of illegal messages transmitted via anonymous remailers once evidence is shown that a crime had been committed. (Edelsten, 1996).

Signatory nations should criminalize money laundering, data theft, online fraud, and electronic vandalism. Any international convention should recognize the importance of cryptography in ensuring online security and user privacy.

Dual criminality should not be required: the requesting nation should be able to ask for assistance from the host nation in the criminal investigation even when the host nation does not consider the act a crime. In order not to place inappropriate limits on political discourse, however, a principle for exceptions should be established. The identity of anonymous users should not be disclosed if the communication in which they engage is purely political in character. That is, democratic nations should not be compelled to reveal the identities of anonymous users for criticizing repressive regimes (Edelsten, 1996). Any convention should also provide that the originator of anonymous messages, not remailer operators, should be liable for criminal actions.

Most conference participants were realists, however, and saw the prospects for international adherence to such an agreement as relatively small. They noted that the law was neither the only remedy available for dealing with the problems raised by anonymous communication online, nor necessarily the best one. Discussion therefore turned to several complementary approaches.

B. Education and Public Awareness

1. Educating Internet users and the public

As the role of the Internet in modern society continues to grow, there is need for education to enhance public awareness about many aspects of online communication, including anonymity. The Internet is a complex medium, which was designed originally for use by scientists, not the general public. Most people who use the Internet routinely have little understanding of the workings of this medium, of how they appear to others when they send messages or surf the Web, and of the degree to which they convey information about themselves to the others when they interact via the Internet. Very often, people have a false sense of security about technology and place more trust in it than is warranted. In this way, they are blind to the fact that there exists no such thing as guaranteed anonymity or guaranteed security. Almost anything one does to conceal one's identity can be defeated.

It is essential for people who use the Internet to be informed much more fully than they currently are about the levels of confidentiality and security provided in various uses. The same is true for citizens who are not presently Internet users, but who should have some say in the further technical and legal structuring of a cyberspace to which they will likely have access in the future. Internet users should learn to be very skeptical of the credibility and trustworthiness of anonymous messages. The public should be aware that any message could be pseudonymous. Users also need to know both the technological limits and circumstances under which people might be forced to reveal their identities

Efforts should be made to inform all Internet users that there can be no absolute guarantee of anonymity in their communications. Also, efforts should be made to educate individuals about the kinds of technologies available for surveillance and anonymity. Education and training are very important to enable information receivers to feel secure, to receive the most valuable information and messages, and to evaluate the credibility of sources.

Conference participants did not propose specific means of increasing public awareness of the nuances of Internet communication. Ideas discussed centered on strategies for education and the wide dissemination of information about online anonymity. It was suggested that the development and distribution process for this kind of education can be established in the schools (at every education level), both public and private, and in other educational organizations. On a different scale, public interest organizations such as the Electronic Privacy Information Center, the Internet Privacy Coalition, the National Computer Security Association, eTRUST, Global Internet Liberty Campaign, the Parliamentary Human Rights Foundation, Human Rights Watch, and the American Civil Liberties Union can provide educational materials for public institutions and private companies, as well as educating the public by distributing information directly. Finally, Internet service providers, operators of Web portals and other major sites such as search engines, and remailers can use screens or banners to highlight information about online anonymity and educate people on the Internet.

2. Encouraging the development of codes of conduct

Several organizations have sought to develop and promote codes of conduct for computer users. For example, the Washington, D.C.-based Computer Ethics Institute has published "The Ten Commandments of Computer Ethics." While these cover the problems caused by the misuse of anonymous communication in a general way (e.g., "Thou shalt not use a computer to harm other people"), they are aimed mainly at computer professionals. Moreover, participants in the AAAS conference felt they do not deal specifically enough with the matter of anonymity. As a step toward developing such a code, or enhancing existing codes with more specific discussion of anonymity, some ideas on identifying conditions under which anonymity should be protected were presented and discussed.[7] These include:

- To facilitate the flow of information and communication on public issues.
- To obtain personal information for research in which the information is confidential, not open to the public.
- To encourage attention to the content of the message or behavior.
- To encourage reporting, information seeking and self-help for conditions that are stigmatizing and/or are very personal.
- To obtain a resource or discourage action involving illegality.
- To protect economic interests.
- To protect time and space from unwanted intrusions.
- To aid judgments and decision-making based on specified criteria, not on irrelevant personal characteristics.

- To avoid persecution.
- To serve as a factor in rituals, games, play and celebrations in which part of the fun and suspense of the game is not knowing the identity of others.
- To encourage experimentation and risk-taking without facing large consequences, risk of failure or embarrassment.
- For the protection of personhood.
- Other conditions in which anonymity is required or permitted; such conditions may be related to personal privacy (situations in which people want to be alone and not be intruded upon).

3. Institutional policies

Conference participants generally agreed that individuals and organizations (including online communities) should be free to determine the level of anonymity that they deem appropriate for those with whom they engage in voluntary interaction. Institutions (e.g., universities) should be encouraged to recognize the importance of anonymous communication online and to create their own policies and practices to govern it. Forms of and forums for communication should also be encouraged to develop and adopt institutional policies relevant to anonymity online. Communities should be free to choose guidelines most appropriate to their members, but policies should be explicit and communicated clearly to all those affected by them.

IV. CONCLUSION

Participants in the AAAS conference recognized that the problems they were discussing are complex and not susceptible either to quick and easy technological fixes or obvious policy solutions. These issues will continue to be the subject of discussion and debate as the importance of the Internet and its pervasiveness in all areas of society grow. This conference was but one step on the path toward addressing the issues raised by this revolutionary technology in a responsible and socially-productive fashion. It was not expected to yield definitive solutions. It did, however, persuade all those involved that anonymous communication is a key aspect of the Internet and that policies that seek to shape it should reflect a balance among the affected interests – including the users, the service providers, law enforcement agencies, and the continued growth and development of the Internet itself.

BIBLIOGRAPHY

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).

Edelsten, Jonathan. 1996. Anonymity and International Law Enforcement in Cyberspace. *Fordham International Property Media and Entertainment Law Journal* 7(1): 231-294.

Froomkin, A. Michael. 1996. Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Database. *Journal of Law and Commerce* 15(2): 395-507.

Griset v. Fair Political Practices Comm. 1994. 884 P.2d 116, 126.

Kling, Rob, Ya-ching Lee, Mark S. Frankel, and Al Teich. 1999. Assessing Anonymous Communication on the Internet. *The Information Society* 15(2).

Landau et al. 1994a. *Codes, Keys, and Conflicts: Issues in U.S. Crypto Policy. A report of a special panel of USACM* [online].Available from World Wide Web: < http://info.acm.org/ reports/acm_crypto_study.html> (last visited on 7 October 1998).

_____. 1994b. Crypto Policy Perspectives. *Communications of the ACM*, 37(8), 115-121.

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).

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

Long, George P., III. 1994. Comment, Who Are You?: Identity and Anonymity in Cyberspace. *University of Pittsburgh Law Review* 55: 1177-1213.

Marx, Gary T. 1999. What's in A Name? Some Reflections on The Sociology of Anonymity. Paper presented to the Anonymous Communications On the Internet, Irvine, California, American Association for the Advancement of Science. *The Information Society* 15(2).

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

Nua. 1998. Internet Surveys [online]. Available from World Wide Web: <http://www.nua.ie/ surveys/how_many_online/index.html> (last visited on 26 March 1998).

Sproull, Lee and Sara Kiesler. 1992. *Connections: New Ways of Working in the Networked Organization.* Cambridge, MA. MIT Press.

Universal Declaration of Human Rights. 1998a. Universal Declaration of Human Rights (Abbreviated). In *Universal Declaration of Human Rights* [online]. Available from World Wide Web: <http://www.umn.edu/humanrts/instree/bludhr.htm> (last visited on 27 April 1998).

_____. 1998b. Universal Declaration of Human Rights (Abbreviated). In *Universal Declaration of Human Rights* [online]. Available from World Wide Web: <http://134.84.205.236/udhrabbrev.htm> (last visited on 9 May 1998).

_____. 1998c. Universal Declaration of Human Rights 1948-1998. In *Universal Declaration of Human Rights* [online]. Available from World Wide Web:<http://www.udhr50.org/default.htm> (last visited on 11 May 1998).

USACM. 1998. USACM Homepage [online]. Available from World Wide Web: <http://www.acm.org/usacm/crypto/> (last visited on 7 October 1998).

_____. 1994. *USACM Statement on the Escrowed Encryption Standard* [online]. Available from World Wide Web:<http://www.acm.org/usacm/crypto/encrypt.html> (last visited on 7 October 1998).

_____. & IEEE/USA. 1996. A letter on export controls of encryption [online]. Available from World Wide Web:<http://www.acm.org/usacm/crypto/burns_letter.html> 2 April. (last visited on 7 October 1998).

_____. 1997a. *USACM Applauds California Legislature for Unanimously Endorsing Relaxed Export Controls on Encryption* (press release) [online]. Available from World Wide Web:< http://www.acm.org/usacm/crypto/usacm_cal_resolution.html> 8 September. (last visited on 7 October 1998).

_____. 1997b. *USACM comments on Digital Signatures to National Institute of Standards and Technology* [online]. Available from WorldWide Web:< http://www.acm.org/usacm/crypto/usacm_digsigs.html> 16 July. (last visited on 7 October 1998).

Notes:

[1] The American Association for the Advancement of Science (AAAS) Conference on Anonymous Communications on the Internet was held on November 21-23, 1997. It was hosted by the University c California at Irvine's Department of Information and Computer Sciences and Center for Research on Information Technology and Organizations. More information about the project can be found online a <http://www.aaas.org/spp/anon/>

[2] *See* Kling et al. (1999) in this issue.

[3] The idea of using the UDHR as a framework for consideration of anonymous communication practices on the Internet was suggested by the participants in one of the small group discussions that took place at the AAAS Conference. It was discussed relatively briefly in the concluding plenary session of the conference, where it received widespread support.

[4] Specifically, Article 12 states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor or reputation. Everyone has the right to the protection of the law against such interference or attacks." See UDHR 1998a. For additional information about the UDHR, see UDHR 1998b and 1998c.

[5] The ACM U.S. Public Policy Committee (USACM) is a committee of the Association for Computing, an international professional society (ACM). It promotes ACM's interaction with U.S. government organizations, the computing community, and the U.S. public issues related to information technology. The USACM provides information to the ACM and identifies "potentially significant technical and public policy issues and brings them to the attention of ACM and the community." See the USACM Homepage at http://www.acm.org.

[6] Some participants suggested, however, that operation of a remailer would provide an ideal "listening post" for a government agency that wished to exercise surveillance on its citizens.

[7] See the essay by Gary T. Marx in this issue.

To obtain a sample copy of The Information Society (TIS), choose one of the following:

Print the form below and mail to the Taylor & Francis Office nearest to you. In North America, send email to: sample-tis@taylorandfrancis.com Outside North America, fill out an electronic form that is available via Taylor & Francis' web site. Follow the path to "sample copy".

To purchase individual copies of The Information Society (TIS), visit the Taylor & Francis Journal Ordering Page.
Single back issues are available for each journal, the price being obtained by dividing the institutional subscription rate by the frequency + 10%, which is currently about US$42 (as of early 1999).

Contact Peggy Pagano, Journals Manager ppagano@taylorandfrancis.com OR1-800-821-8312 (EXT.117) OR

215-269-0400, OR FAX: 215-269-0363.

Taylor & Francis retain a 2 year back stock of journals. Older volumes are held by our official stockists: Dawson (UK)Ltd, Back Issues Division, Cannon House, Folkestone, Kent CT19 5EE, UK to whom all orders and inquiries should be addressed. Tel: +44 (0) 1303 850101; Fax: +44 (0) 1303 850440.

To subscribe, clip the following form and mail to the address below:

-- --

THE INFORMATION SOCIETY
Published quarterly, ISSN 0197-2243

___ Please enter my institutional subscription at US$140 (starting with vol 15)
___ Please enter my personal subscription at US$69 (starting with vol 15)
___ Please send me a free sample copy

Payment options:

___ Check/Money Order Enclosed
(please make checks payable to Taylor & Francis, US$ only)

___ Please charge my: ___ VISA __ MC ___ Amex
Card #_____ Exp date:_____
Signature:_____
Telephone:_____
(required for credit card purchases)

or BILL TO: (please print)

Name_____
Institution_____
Address_____
City_____
State_____ Zip_____

SHIP TO (if different):

Name_____
Institution_____
Address_____
City_____
State_____ Zip_____

Mail this form to:

Taylor & Francis Inc.
47 Runway Road
Levittown, PA 19057
Toll free- 1-800-821-8312 or
Phone- 215-269-0400
Fax- 215-269-0363

Outside the U.S. contact:

Taylor & Francis Ltd.
Rankine Road
Basingstoke, Hampshire
RG24 0PR, United Kingdom
tel: +44 (0) 256 840366
fax: +44 (0) 256 479438