

Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes

[Lance J. Hoffman](#)

[Karen A. Metivier Carreiro](#)

[Cyberspace Policy Institute, School of Engineering and Applied Science](#)

[The George Washington University](#)

Washington, DC 20052

1. Introduction

In addition to the generally accepted definition of privacy as "the right to be left alone", privacy has become a "broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behavior, including wiretapping, surreptitious physical surveillance, and mail interception. Individuals claim a right of privacy for an enormously wide range of issues from the right to practice contraception or have an abortion to the right to keep bank records confidential" [[Flaherty 1989](#)]. In recent years, these claims have expanded to include the right to keep one's trail of sites visited on the World Wide Web confidential.

In order to implement "privacy" in a computer system, we need a more precise definition. We have to decide when and under what conditions to give out personal information. Specifically, we must decide when to allow anonymous transactions and when to require accountability. If there are subgroups in society, or countries, with differing ideas about the answers to these questions, technology can, to a large extent, accommodate each group. There does not necessarily have to be only one privacy regime. Less law and more user choice is possible now; technology can provide every user with controls fine-tuned for the balance of privacy and accessibility that they prefer.

This paper first describes how accountability and anonymity can be balanced to allow user control as much as possible, community norms when the user desires conflict, and (finally) government regulation when the norms of the communities differ. It recognizes the possibility of "privacy royalties" and describes a few of the technological mechanisms available to implement these controls.

2. Anonymity vs. Accountability

Individuals sometimes choose to remain anonymous to safeguard their privacy, for example, when browsing in a department store or purchasing an "adult" magazine. Browsing the Web has also, to date, usually been an anonymous activity. Moving beyond the Web to the Internet in general, one can send anonymous messages using an *anonymous remailer* program. It is fairly easy today for a technically

sophisticated person to remain anonymous and avoid accountability on the Internet for actions which are questionable or illegal, e.g., sending advertising mail to numerous newsgroups (*spamming*), running a pornography server, or hacking the Web page of another person.

But technology can promote accountability as well as anonymity. If computer systems or applications require "proof" of identity before allowing use, we will have a much more accountable society. It would be as if cars would only start when driven by "authorized" drivers; mere keys would not work. On the other hand, usability and privacy would suffer -- imagine having to authenticate yourself to a pay phone or to a rental car!

Accountability should not always be required. Anonymous leafleting and other modes of expression are properly strongly protected by the U. S. Constitution. An appropriate balance must be struck by the community. Then the technology can enforce that balance.

3. Privacy Threats from Today's Computer Systems

The Privacy Act of 1974 [[Privacy 1974](#)] and data protection legislation in other countries has to some extent defused criticism and concern about potential government invasion of privacy. Indeed, medical, credit, and marketing databases appear to be as troublesome as governmental databases. Some private endeavors have already raised significant privacy concerns in the Internet community.

The Lotus MarketPlace: Households database was going to make names, addresses, demographic and prior purchase behavior data for 120 million U.S. consumers available on a CD-ROM in 1991. Consumers objected to the secondary use of identifiable personal information without their consent. Individual credit reports provided the basis of the MarketPlace data and, as a result, a fundamental privacy principle, that personal information collected for one purpose should not be used for other purposes without the consent of the individual, was violated.

The product was canceled based on the substantial, unexpected additional costs required to fully address consumer privacy issues. Much of the opposition to MarketPlace was mobilized, individual by individual, on the Internet. This grass-roots electronic movement flooded the mailbox of Lotus' chief executive officer with 30,000 electronic complaints, and could be characterized as the first "electronic sit-in".

More recently, in 1996, Lexis-Nexis offered a service which provided its 740,000 subscribers with 300 million names, previous and current addresses, maiden and assumed names, birth date, and telephone number. The wide availability of such information raised legal and other concerns and has triggered an investigation by the Federal Trade Commission, responding to congressional inquiries. Lexis-Nexis initially offered social security numbers as well, but changed the system after numerous complaints from Netizens.

There are ongoing court battles between advocates of electronic marketing like Sanford Wallace of CyberPromotions, Inc. and legions of users who say they have a right not to be bothered by him and other electronic marketers. CyberPromotions' messages (spam) have been barred by a number of online services, including America Online and Prodigy, and in some cases it has paid the provider in order to prevent further legal action.

Planning and sensitivity to user concerns about privacy could have greatly ameliorated the problems

above. Internet and computer users expect choices; from the minute they get their computer, they are asked whether they want a plain background or one of a number of screen-savers; what their printer is like; and a number of other things, all designed to configure the system to the preferences of the user. It is clear to them that making choices available is possible, and they consider it to be the norm. Thus, they expect to be given a choice about receiving unsolicited commercial e-mail. More and more, they also expect clear privacy statements when their data is being used. A number of leading firms already have privacy codes which deal with the privacy of their consumers' data [[P&AB 1994](#)].

4. Privacy niche markets, self-regulation, and fallbacks

One interesting thing here is that there is a demand by non-traditional players ("members" of the Internet community) for some say in defining the rules of the game. Where in the past business and government have obviously had a part in making the rules, now individual members of the online community are raising serious questions and refusing to play if these are not answered satisfactorily. In the three cases mentioned above, rapidly spreading, vocal, articulate protests by members of the Internet community have caused commercial firms to significantly change their plans; these cases are starting to define what is acceptable in Cyberspace.

A market is operating here, and the private sector can, as in most markets, strive to fill the market requirements. As an example, the Recreational Software Advisory Council (RSAC), an independent, non-profit organization was established in the fall of 1994 by a group of six trade organizations which created an objective content-labeling rating system for recreational software and other media, such as the Internet. RSAC uses the PICS (Platform for Internet Content Selection) technology system to allow third-parties or self-regulators to classify information directly, providing the ability to control information that can be received by a given user without censoring the network itself.

Most browsers are now or soon will be PICS-compatible. Thus, the technology can help niche markets in privacy develop. Privacy groups can label sites according to their information practices using PICS. A user can contract with an ISP or Web site owner to allow different amounts of information to "get out" about himself or herself depending on the fee paid by the user. This could include royalty (micro)payments to the user in return for the use of his or her data [[Laudon 1996](#)].

Thus, the first level of regulation will be the user and his or her ISP or Web content provider mutually agreeing on the appropriate level of privacy invasion and the compensation for the same. If some members of the online community don't accept user control (e.g., direct marketers like Mr. Wallace above), the Internet self-regulates. In the past, users who strayed beyond generally accepted norms of the net ("netiquette") have been subject to a variety of sanctions. These include "flaming", "mailbombing", warnings from their Internet service providers (ISPs), and termination of accounts (all of which Mr. Wallace has suffered).

Computer technology will not solve all privacy problems. Mr. Wallace, for example, has recently been promoting a scheme where he purchases excess capacity of some ISPs and they in turn allow him to send messages which look like they come from them, not from him (since America OnLine and other ISPs have programmed their firewalls to not let his messages through). Some would consider this a violation of federal law, or at least of ethics.

Ultimately, when self-regulation fails, the government is called upon to resolve problems or to adjudicate

contractual disputes. That will eventually happen in this case. Standards vary around the world, and each government will have its own domestic privacy standards. New York City has different privacy standards (and other standards) than Saudi Arabia. But just as the technology can today provide significantly more user choice than before, it can also allow nations to, if they wish, put their own designations on classes of Web pages. Citizens of a given geographical nation could be allowed, prohibited, taxed, or paid for visiting certain (types of) pages. Indeed, once governments figure out how to pull it off, the Web could produce a bonanza of "sin taxes". The technological tools are here today and can provide as much or as little privacy as desired, and can support an increasing variety of contractual mechanisms.

5. Technological safeguards

There are a number of technological mechanisms which enhance computer security and thus increase individual privacy in systems. This paper only highlights a few which are relevant to our topic. There is a wealth of computer security literature for the reader desiring additional information [[Pfleeger 1996](#), [Russell 1991](#)].

a. Authentication

There are typically three types of authentication mechanisms: something you know, something you have, or something you are. After individual recognition of a person, the most common mechanism is the password. For a variety of technical reasons, passwords alone will not be secure enough in the long run. Slowly we are going to evolve from these systems which only demand "something you know" (e.g., passwords) to those which also require "something you have" or "something you are". Thus, we will see more and more computers built with the capability to read an electronic card in the possession of the user, just like an automated teller machine at a bank. Sometimes this card will automatically transmit the password, and sometimes, for greater security, the user will have to enter his password separately, in addition to possessing the physical card.

We may also see the further development of biometrics (e.g., fingerprints, pronunciation, retinal patterns) as authentication mechanisms. These already exist, but their application has been limited, due to user acceptance problems. California and some other states now require fingerprints on their drivers licenses. Since most users won't want to carry several cards but would prefer one all-purpose card (in battles between utility and security, utility almost always prevails), additional privacy questions appear: why not have one central authority (a government?) issue a universal (money) card (and driver's license)? The advantages are less cards and account numbers, and more efficiency for the system and for its users. The disadvantages are the potential for nonresponsive bureaucracies to develop and for abuse of power by a rogue government. Society has to decide whether the (financial and social) costs of maintaining multiple separate identity regimes still worth the (privacy) benefits?

b. Cryptography

Manual encryption methods, using codebooks, letter and number substitutions, and transpositions can be found in writings of the Spartans, Julius Caesar, Thomas Jefferson, and Abraham Lincoln. Cryptography has often been used in wartime, and critical victories (such as that of the United States at the Battle of Midway in World War II) depended on successful analysis (codebreaking) of the German encryption

method.

There are two kinds of cryptographic systems -- secret key and public key. In secret key systems, a secret key -- a specially chosen number -- when combined with a set of mathematical operations, both "scrambles" and "unscrambles" hidden data. The key is shared among consenting users. In public key systems, each user has two numeric keys -- one public and one private. The public key allows anybody to read information hidden using the sender's private key, thus allowing authentication of messages (electronic signatures) in addition to confidentiality. The private key is kept secret by the user.

Many cryptographic systems today use a combination of public key and secret-key encryption: secret-key encryption is used to encrypt the actual message, and public key encryption is used for sender authentication, key distribution (sending secret keys to the recipient), and digital signatures. This hybrid combination of the two encryption technologies uses the best of each while simultaneously avoiding the worst. It is the basic method of sending secure messages and files from anywhere to anywhere over unsecured networks. As long as sender and recipient ensure that their private keys are exclusively in their possession, this process will work every time, yet thwart any would-be attacker. It can be used to send (and keep secret) a two-line message or a two-hour movie, and anything in between.

Today, cryptography also is often used to also prevent an intruder from substituting a modified message for the original one (to preserve *message integrity*) and to prevent a sender from falsely denying that he or she sent a message (to support *nonrepudiation*). If data is deemed to be "owned" by individuals, and royalties paid, then we can use encryption technology to digitally sign individual pieces of data, effectively placing taggants with the data. Thus one could always trace the data back to its source.

Cryptographic procedures, or *algorithms*, are (or can be) public in most cases; the security of the system depends on users keeping *keys*, which are used with the (public) algorithms, secret.

c. Firewalls / authorization

Increasing numbers of users and computers are being checked for authorization before being allowed to interact with internal corporate, university, or government systems and obtain information from them. Traditional operating system and data base management controls have been joined recently by firewalls which check that only properly authorized (and sometimes paid-up) users are allowed access.

d. Cookie cutters

Often, Web servers keep records of what a user has done ("cookies") in order to better serve the user when he or she visits the site again. This capability can be abused, and thus most browsers now allow users to refuse to give Web servers this information. Occasionally, this will result in a denial of service to the user. But it is the user's choice, not the system's.

6. Summary

Accountability and anonymity can be balanced to allow user control over privacy as much as possible, community norms when the user desires conflict, and (finally) government regulation when the norms of the communities differ. This paper has given examples of the choices to be made and then briefly described a few of the technological mechanisms available to implement these controls in computer systems.

7. References

[Cook 1996] Cook, J., "A Market Ecology for Electronic Commerce", <http://eco.eit.com/information/electron.html> <http://eco.eit.com/information/electron.html>, accessed January 2, 1997.

[Flaherty 1989] Flaherty, David H., *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill, NC, 1989.

[EC 1995] EC Directive on Data Protection (draft), available at http://www.cpsr.org/cpsr/privacy/privacy_international/international_laws/ec_data_protection_directive.html

[Flaherty 1989] Flaherty, David, *Protecting Privacy in Surveillance Societies*, University of North Carolina Press, Chapel Hill, NC, 1989.

[Froomkin 1996] Froomkin, A. Michael. 1995. "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases", available as of November 25, 1996, from <http://www.law.miami.edu/~froomkin/articles/ocean.htm>

[HEW 1973] Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Department of Health, Education, and Welfare, July 1973.

[Hoffman 1995] Hoffman, Lance J. (ed.), *Building in Big Brother*, Springer-Verlag, New York, N. Y., 1995.

[IITF 1995] Information Infrastructure Task Force, NII Security: The Federal Role, draft of June 5, 1995, available from iitf.doc.gov.

[Laudon 1996] Laudon, K., "Markets and Privacy", *Communications of the ACM*, Volume 39, No. 9 (September 1996), pp. 92-104.

[Ontario 1995] Privacy-Enhancing Technologies: The Path to Anonymity, Privacy Commissioner of Ontario, Canada, 1995.

[Pfleeger 1996] Pfleeger, Charles, *Security in Computing*, 2nd Ed., Prentice-Hall, Inc., Englewood Cliffs NJ, 1996.

[Privacy 1974] Privacy Act of 1974, as amended. P. L. 93-579, 5 USC 552a.

[P&AB 1994] Handbook of Company Privacy Codes, Volumes 1,2, and 3, Privacy & American Business, Hackensack, NJ, 1996.

[Resnick 1996] Resnick, P. and Miller, J., "PICS: Internet Access Controls Without Censorship", *Communications of the ACM*, Volume 39, No. 10 (October 1996), pp. 87-93.

[Russell 1991] *Computer Security Basics*, O'Reilly & Associates, Inc., Sebastopol, California, 1991.

[Rothfeder 1992] Rothfeder, J., *Privacy for Sale*, Simon & Schuster, New York, N. Y., 1992.

[von Solms 1992] von Solms, S. and David Naccache, "On Blind Signatures and Perfect Crimes", *Computers and Security*, Vol. 11, No. 6, 1992, Elsevier Science Publishers Ltd.

[Warren 1890] Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy", *Harvard Law Review* 4 (1890): 193-220.

[Westin 1967] Westin, Alan F., *Privacy and Freedom*, Atheneum, 1967.