National Telecommunications and Information Administration

United States Department of Commerce

Home

Chapter 5: Technology and Privacy Policy

Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes[(1)]

Lance J. Hoffman
Karen A. Metivier Carreiro
Cyberspace Policy Institute, School of Engineering and Applied Science
The George Washington University
Washington, DC 20052

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, accomodate 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 accessibilty 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.

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.

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 cancelled 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 marketeers. 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].

PRIVACY NICHE MARKETS, SELF-REGULATION, AND FALLBACKS

One interesting thing 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, 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 Internet Service Provider (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 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 On Line 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.

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].

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, pronounciation, 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 are worth the (privacy) benefits?

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 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.

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.

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.

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 has described briefly a few of the technological mechanisms available to implement these controls in computer systems.

REFERENCES

[Cook 1996] Cook, J., "A Market Ecology for Electronic Commerce," 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) (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_ 1995.txt**

[Flaherty 1989] Flaherty, *Supra*

[Froomkin 1996] Froomkin, A. Michael, "Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases," (1995), 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 http://iitf.doc.gov.

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

[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, 1-3 Privacy & American Business (Hackensack, NJ), (1966).

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

[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," 11 *Computers and Security*, at 6 (Elsevier Science Publishers Ltd) (1992).

[Warren 1890] Warren, Samuel D. and Brandeis, Louis D., "The Right to Privacy," 4 Harv. L. Rev. 193, 220 (1890).

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

The Role of Technology in Self-Regulatory Privacy Regimes

Lorrie Faith Cranor
Public Policy Research
AT&T Labs-Research[(2)]
lorrie@research.att.com

Individuals frequently reveal personal information in the course of doing business in order to gain benefits such as home delivery of products, customized services, and the ability to buy things on credit. In so doing, they may also become vulnerable to other uses of

their personal information that they find undesirable. The Internet and computerized databases make automated collection and processing of information particularly easy and convenient. As a result, individuals may take advantage of new services, such as personalized electronic newspapers and shopping from home, but they may also become more vulnerable to misuses of personal information.

Just as technology can be used to automate data collection and processing, it can also be used to automate individual control over personal information. In particular, technology can:

- Facilitate the seamless exchange of information about data collectors' information practices and individuals' privacy preferences;
- Automate audits of data collectors' information practices;
- Enable secure transactions in which minimal personal information is revealed;
- Empower individuals to control the messages they receive over telecommunications channels; and
- Prevent private communications from being intercepted and databases from being compromised.

Technologies to support these applications are in varying stages of development, deployment, and adoption. This paper presents an overview of these technologies in order to inform discussion about which tools and techniques are most worth pursuing.

SEAMLESS INFORMATION EXCHANGE

Notice and choice are among the most important principles of fair information practice. Responsible data collectors provide individuals with clear advance notice about the types of data they collect and how that data will be treated. They also provide individuals with the means to choose what data they provide for specific purposes. (Of course, individuals who choose not to provide essential data in some situations might be denied services as a consequence.) Traditional means of providing notice and choice generally require individuals to divert their attention away from the task at hand in order to read or listen to lengthy explanations and answer questions. When such disruptions occur frequently, individuals are unlikely to pay close attention to them. On the Internet, individuals typically wander from site to site without such interruptions. However, if most Internet content and service providers provided notice and choice through traditional means, interruptions would be a common occurrence. Fortunately, a number of alternative mechanisms may facilitate the provision of notice and choice over telecommunications networks while preserving the seamless browsing experience.

One way to simplify notice and choice is to provide standard notices with consistent choice options. Currently, some organizations are experimenting with privacy rating structures that classify each Web site into one of several categories based on the site's information practices. For example, one category might be used for sites that do not reveal information collected from visitors, while another category might be used for sites that may trade or sell information they collect from visitors. Sites rated under such systems display icons on their pages that notify individuals of their information practices.

This solution provides individuals with a means of quickly determining a site's information practices. However, the number of information practice categories must remain small if the category icons are to remain easily distinguishable. But with only a limited number of categories, it may not be possible to encode all details about information practices that individuals might find important. For example, individuals might want to visit sites that

may reveal personal information to third parties only if that information is limited to names and contact information and does not include transactional data. In addition, because these systems rely on visual icons, individuals must consciously remember to look for these icons at every site they visit and take additional actions to confirm that the icon has not been forged.

Some of the problems inherent in icon-based systems can be overcome by a machine-readable label system. The Platform for Internet Content Selection (PICS), developed by the World Wide Web Consortium (W3C), is one such system.[1] PICS was originally developed as a user-empowerment approach to protecting children from Internet content that their parents consider objectionable. It is an infrastructure for associating descriptions, called *labels,* with documents and Web sites on the Internet. PICS can accommodate any labeling vocabulary: currently several vocabularies are in use that indicate either age-appropriateness or the presence of potentially objectionable content such as offensive language or nudity. A label is not normally visible when a document is displayed to a user; instead, when a PICS-compliant browser is used, the browser reads the PICS label and determines if the associated document meets the user's criteria for display. If a document fails to meet the user's criteria, it is blocked, unless the user chooses to override the block. As of December 1996, Microsoft Internet Explorer 3.0 is PICS compliant, as are a number of stand-alone filtering products. This user-empowerment approach has played an important role in public discussion, both in the U.S. and around the world, of how best to protect children from objectionable content without introducing government censorship.

The PICS technology also offers promise in the privacy realm for user empowerment through automated notice and choice.[2] Labeling vocabularies might be developed to describe the information practices of organizations that collect data over the Internet. For example, a vocabulary might encode the categories used in existing icon-based systems. Other vocabularies might also employ multiple dimensions, for example, one dimension for practices pertaining to each type of information a site collects (demographic information, contact information, transactional data, etc.). Individuals might choose to have their browsers automatically block sites that do not have information practices consistent with their personal privacy preferences.

The PICS infrastructure allows sites to describe their own information practices or for independent monitoring organizations to compose and distribute labels describing a site's practices. Unlike objectionable content, however, a site's information practices are not immediately visible to a casual observer. Thus, the most effective notice about information practices is likely to come from the Web sites themselves.

In order to provide the most flexibility for both individuals and Internet content providers, it would be useful if browsers could negotiate information practices with content providers automatically, rather than just blocking access to those sites with undesirable practices. For example, if a Web site does not have practices consistent with an individual's preferences, the browser might contact the site and ask how the individual might be accommodated. The server could respond by agreeing to honor the individual's preferences, by offering a restricted portion of the site in which the individual's preferences will be honored, or by providing an explanation as to why the individual's preferences cannot be honored or an incentive for the individual to access the site even though it does not honor the stated preferences. The PICS infrastructure cannot currently support such a negotiation; however, it could be expanded to include a negotiation protocol. Web negotiation protocols are currently under development by W3C and other

organizations. Once a negotiation protocol is developed, it will take some time to incorporate it into Web browsers and servers.

Another possible extension of the PICS infrastructure might be used to specify the conditions under which an individual would allow the automatic transfer of certain types of information. Such information might include contact information needed for business transactions, or demographic and personal preference information used by Web sites to customize the services they provide. Automated transfer of this information would be more convenient for users than typing the information each time they visit a site, and users could set up their browsers to ensure transfers only to Web sites that have certain information practices.

The user empowerment tools described above depend on cooperation between individuals and information gathering organizations. When there are mutually acceptable terms for transfer of individual information and conditions on its use, these tools allow the negotiation and information transfer to happen in the background, without consuming the individual's valuable time and attention. The opportunity to automate the notice and choice process is a major advantage of the Internet over other media for commercial interaction. As in the physical world, however, these tools do not guarantee that mutually acceptable terms will always be found: depending on market conditions, individuals may or may not find privacy-friendly choices available.

AUTOMATED PRIVACY AUDITS

While the approaches outlined here facilitate the seamless exchange of information about data collectors' information practices and individuals' privacy preferences, they do not ensure that data collectors will report their information practices accurately. Independent labeling services can label bad actors once they have been identified, but it may be difficult to detect sites that violate their reported practices. An audit may help a site to convince consumers of its good information practices and to distinguish it from other sites that may dishonestly report their practices. However, traditional audits are likely to be prohibitively expensive for most Web site operators. It may be possible to use technology to automate the information practice audit process to some extent. For example, systems might be developed to systematically reveal decoy data to Web sites and monitor the propagation of that data. Further work is needed to develop techniques for automating the information practice auditing process.

TRANSACTIONS THAT REVEAL MINIMAL PERSONAL INFORMATION

Another approach to safeguarding personal information is to minimize the need for collecting such information or minimize the number of times the information must be accessed. This can be done through the use of trusted intermediaries or technologies designed for this purpose.

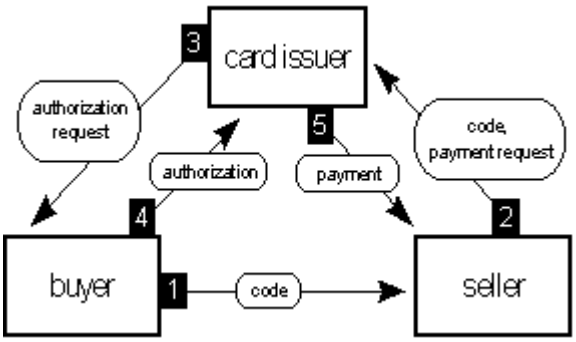
Several trusted intermediary systems currently in use on the Internet are designed to prevent the release of personal information. These anonymizing systems generally remove all personally-identifiable information (such as name and email address) from communications before forwarding them to the intended recipients. For example, anonymizing proxy servers allow individuals to surf the Web without revealing their network location,[3] and anonymous remailers allow individuals to send electronic mail without revealing their email addresses to their correspondents.[4]

One step removed from anonymous interactions are interactions under a pseudonym. In such interactions individuals do not reveal their true identity, but reveal pseudonyms instead. Each individual may reveal the same pseudonym each time he or she visits a particular Web site, but may reveal different pseudonyms to other sites. This allows a site to accumulate a profile of each individual's preferences over time so that it may tailor content and advertisements to that individual's interests, while preventing information revealed to different sites from being combined into a comprehensive profile.

Pseudonyms also allow a site to maintain information about the state of an individual's interactions with that site, such as the contents of an individual's virtual shopping basket. Many Web sites currently use an alternative mechanism called "cookies" to maintain such information.[5,6] Cookies are pieces of information stored on a user's computer at the request of a particular Web site. The next time the user visits that site, the site can retrieve any cookies that it previously stored. In practice, however, multiple Web sites sometimes share access to cookies. A user who reveals personal information to one Web site may unwittingly reveal that information to other sites. By contrast, pseudonyms allow users to decide when to allow their information to be shared among Web sites, preventing unwanted information leakage. From a privacy perspective, interaction under a pseudonym offers users more control over the release of information than cookies do, but retains the benefits that come from allowing sites to maintain information about an individual's interaction with them.

Anonymizing intermediaries and pseudonyms are insufficient for some types of transactions. For example, imagine an individual who wants to purchase software over the Internet. The individual might have used a pseudonym in her relationship with the vendor, allowing the vendor to keep a profile of her preferences and maintain information about the state of her virtual shopping cart. She might have also used an anonymizing server whenever she visited the vendor's Web site so as not to reveal her network location. But these systems cannot help her transfer funds to the vendor from her bank account without revealing personal information to the vendor.

Fortunately, trusted intermediaries can also enable monetary transactions with minimal requirements for personal information. For example, some Internet credit card systems currently in use allow individuals to make a credit card purchase over the Internet without transferring their card numbers directly to vendors. Instead, an individual sends a vendor a special-purpose code that identifies the transaction. The vendor forwards the code to the card issuer with a request for payment. The issuer then contacts the buyer and asks that the transaction be authorized. Upon receiving authorization, the issuer bills the buyer's credit card and pays the vendor, without revealing the buyer's credit card number to the vendor. Thus the danger of an individual's credit card number being misappropriated is substantially reduced. However, as with traditional credit cards, the card issuer has a complete record of the individual's credit card transactions and must be trusted to safeguard this information.



Example Internet Credit Card Transaction

In general, the more information can be consolidated in the databases of trusted intermediaries, the less need there is to transfer information in the course of completing a transaction. This approach allows attention to be focused on the information practices of a small number of intermediaries rather than on all parties that might engage in transactions. However, the potential for damage can be quite large in the event that the trusted database is compromised or that the intermediary proves to be untrustworthy. This is true whether transactions take place over the Internet or over traditional means.

An alternative to consolidating information in the databases of trusted intermediaries is to keep information in the hands of individuals as much as possible. This can be done by designing transaction systems that transfer only the information that each party absolutely needs to know. For example, in an electronic payment transaction the bank need only know that the individual is authorized to withdraw money from a particular account, the identification number of that account, and the sum of money to be withdrawn; the vendor need only know that it has received a valid payment. The bank need not know what the individual is doing with the withdrawn money, and the vendor need not know the individual's name or bank account number (in contrast, these pieces of information must be transferred, for example, when individuals purchase goods with checks). Thus, only the purchaser has access to the list of purchases that he or she has made. Of course, if the bank does not have access to information about how individuals spend their money, the individuals must maintain their own records. Electronic cash systems can offer the privacy of cash payments with the convenience of electronic payments. However, some of these systems have many of the same vulnerabilities as traditional cash, including risk of theft or loss.

The underlying technology behind some electronic cash systems is a special type of digital signature called a blind signature.[7] Introduced by David Chaum, blind signatures allow a document to be signed without revealing its contents. The effect is analogous to placing a document and a sheet of carbon paper inside an envelope. If somebody signs the outside of the envelope, they also sign the document on the inside of the envelope. The signature remains attached to the document, even when it is removed from the envelope. Blind signatures can be used in electronic payment systems to allow banks to sign and distribute digital notes without keeping a record of which notes an individual has been given. An individual who wishes to withdraw money from a bank account must prepare a digital note with a secret serial number and submit it to the bank. The bank withdraws the money from the individual's account and signs the note. However, the bank does not know the serial number of the note. When the individual gives the digital note to a vendor in exchange for a purchase, the vendor may take the note to the bank and ask for it to be deposited. The bank can verify its signature on the note to determine whether

it is legitimate, and it can record the serial number and make sure notes with the same serial number are not spent multiple times. But as with most cash transactions, the bank cannot determine which individual gave the note to the vendor.

Electronic payment systems may be designed as software-only systems that can be used to make payments over computer networks, smart card systems that can be used to purchase goods from vendors who have smart card hardware, or hybrid systems. Regardless of whether the system is implemented in hardware or software, it may be used to store information so that the information is always under the control of the individual to whom it belongs. Thus transaction records may be stored on a chip in the smart card itself or on an individual's computer. The individual may view these records to keep track of personal finances, but the card issuer does not have access to these records.

Blind signatures and smart card technologies can be used for other types of transactions as well. For example blind signatures can be used in electronic voting systems to ensure that each registered voter votes only once while at the same time ensuring that nobody can find out who each person voted for.[8] Smart cards can be used to store credential information (academic degrees, financial credit, certification to enter a restricted area of a building, etc.) and produce convincing evidence that an individual holds requested credentials without requiring the individual to supply the credential checker with the personal information ordinarily required to verify the individual's credentials through traditional means.[9]

INDIVIDUAL CONTROL OVER INCOMING COMMUNICATIONS

So far, the approaches discussed here have been aimed at preventing the unwanted release of personal information. Another area in which technology can play a role is in reducing the ability of people and organizations to use personal information to invade an individual's privacy. Today, many individuals become aware of the extent to which their personal information is bought and sold when they start receiving unwanted solicitations over the telephone or in the postal mail. Already, some of these solicitations have begun arriving via electronic mail. Because sending large volumes of electronic mail is so inexpensive, electronic junk mail is likely to become a significant problem in the future if preventative steps are not taken. Currently some Internet service providers filter email sent from addresses known to send mass junk email. However, due to the ease with which junk emailers may forge return addresses, this is not likely to be a long-term solution to the ever-increasing junk email problem.

The junk email problem might be addressed through technologies that sort incoming email according to sender, placing email from unknown senders in a low-priority mailbox. Robert Hall, a researcher at AT&T Labs, has developed a system of channelized electronic mail in which individuals set up many email channels and assign a different channel to each of their correspondents.[10] Correspondents who have not been assigned a channel can only communicate with the individual on a low-priority public channel. The system may be augmented so that the individual may choose to ignore messages received on the public channel unless they are accompanied by an electronic payment. If a message is from someone the individual wishes to correspond with, such as a long lost friend, the individual might refund the payment; however, if the message is a solicitation, he or she would likely keep the payment. This would make it more costly to send unsolicited email, and it would compensate people for spending time reading this mail.

Hall's implementation of channels requires that individuals ask each of their correspondents to contact them at a different email address, a requirement that may prove inconvenient. Alternatively, an individual's email software might sort correspondence into channels based on the name of the sender. Digital signatures might be used in such a system to authenticate senders, thus allowing each person to maintain a single email address. While no email system that performs all of these operations seamlessly currently exists, such an email system could be built using currently available technology.

Unsolicited email could also be read by software programmed to identify unwanted messages. This might be done by looking for patterns that are indicative of junk mail or looking for messages that are similar to messages in a database of known junk mail. People might subscribe to junk mail filtering services that maintain databases of junk mail submitted by subscribers and periodically send updates to each subscriber's computer with instructions on how to identify and delete newly discovered junk mail. Current technology cannot be used to filter junk mail with perfect accuracy, but our ability to filter accurately should improve over time.

DATA AND COMMUNICATIONS SECURITY

It is important to recognize that the technologies presented here address only part of the problem. Even the most privacy-friendly information policies may be thwarted if data collectors do not protect their communications and databases. Security precautions should be taken to prevent communications from being intercepted and databases from being compromised. Organizations should develop procedures to protect passwords and prevent employees from accessing data for unauthorized purposes. Data and communications security is an important component of all privacy protection schemes, whether the data in question was collected over the Internet or by traditional means.

CONCLUSIONS

A variety of technologies can be used to safeguard personal privacy on the Internet while allowing individuals to reap the benefits of customized services and convenient payment mechanisms. These technologies can be used to build applications that minimize the need to reveal personal information and empower individuals to control the personal information they reveal and understand how it will be used. The technologies needed to implement these applications are fairly well understood. However, a strong industry-wide commitment will be necessary to drive deployment and adoption. To be effective, these applications will need user-friendly interfaces. Some may also require widespread adoption by both consumers and Web sites before they can be successful.

ENDNOTES

1 Paul Resnick and James Miller, *PICS: Internet Access Controls Without Censorship,* Communications of the ACM, 39(10):87-93, (1996).

2 Paul Resnick, Privacy applications of PICS: the Platform for Internet Content Selection, Prepared for the Federal Trade Commission Public Workshop on Consumer Privacy on the Global Information Infrastructure, (June 4-5, 1996). http://www.research.att.com/~pres nick/papers/ftc96/testimony.htm

3 Community ConneXion, The anonymizer FAQ (1996).
http://www.anonymizer.com/faq.html

4 Andre Bacard. Anonymous Remailer FAQ (November,1996).
http://www.well.com/user/abacard/remail.html

5 Tom Negrino, *So What Are Browser Cookies, Anyway?* Macworld Online (1996).
http://www.macworld.com/netsmart/cookiestory.html

6 Netscape Communications Corporation, Persistent client state HTTP cookies, preliminary specification (1996). http://www.netscape.com/newsref/std/cookie_spec.html

7 David Chaum, *Achieving Electronic Privacy,* Scientific American, 266(8):96-101, (August 1992).

8 Lorrie Faith Cranor and Ron K. Cytron, *Sensus: A Security-Conscious Electronic Polling System for the Internet,* Proceedings of the Hawaii International Conference on System Sciences, (Forthcoming January 7-10, 1997), Wailea, Hawaii, USA. http://www.research.att.com/~lorrie/pubs/hicss/hicss.html

9 Chaum, *supra* note 7

10 Robert J. Hall, Channels: Avoiding Unwanted Electronic Mail. To appear in Communications of the ACM, 1997. ftp://ftp.research. att.com/dist/hall/papers/agents/channels-long. ps

AUTHOR'S BIOGRAPHY

Lorrie Faith Cranor is a researcher in the Public Policy Research Department at AT&T Labs-Research. She received her doctorate in Engineering & Policy from Washington University in 1996. Her graduate research focused on electronic voting system design and the development of a new voting paradigm made practical through the use of computers. Prior to joining AT&T, Cranor was a lecturer in the Engineering & Policy and Computer Science departments at Washington University.

Labeling Practices for Privacy Protection

Esther Dyson
Edventure Holdings, Inc.

A self-regulatory approach to protecting privacy on the Net is worthwhile both in itself and as a way to avoid government regulation. It is likely to be more flexible, more decentralized, and more responsive to actual conditions than government regulation. It will also foster maximum user choice, while at the same time breeding confidence among users that they can trust the medium.

This paper discusses the protection of privacy on the Net through the use of labels. The value of labels is that people can pick rules that suit them, rather than be forced to operate in a one-size-fits-all environment where everyone has to follow the same rules.

That works only when one person's selection of rules doesn't impinge on another's. Labeling allows each person to select the privacy rules she prefers for herself or for her children or pupils. The basic rule is that through labeling providers must disclose themselves clearly and honestly. And they must do what they promise.

Making the Net self-regulated instead of controlled by the government is the goal of eTRUST[1] and the Internet Privacy Working Group (IPWG).[2] The underlying question that is faced by eTRUST and IPWG is whether they can successfully garner industry support without the heavy threat of government regulation behind them. In short, can they raise the issue's visibility enough to get the public to care about it and Websites to self-regulate but still not provoke a government-mandated/controlled system?

The goal is a market that, as a whole, fosters good privacy practices. Such a market will result in constantly improving practices rather than rigid ones set by law, and in decentralized, speedy enforcement.

The major challenge in privacy comes once personal data leaves any particular Web site. Nonetheless, even dealing with privacy as a local problem should go a long way towards encourag- ing consumer comfort. Little can be determined about privacy or security looking at a site; privacy and security are dependent upon *processes* which may not be visible to outsiders--and may be too complex to rate easily. The details need to be specified. "No data is kept" is easy. But "certain data are transferred to others" is complex: To whom? Under what conditions? And so forth. If there is a problem, you may find out the awful truth only when it is too late.

Moreover, rules concerning privacy may apply differently to different customers, at the site's or at the customer's option. In the simple model, each Website may have a blanket policy about data reuse, and customers decide whether or not to interact with it. But a Website may instead offer a number of options, and customers can negotiate--perhaps paying in anonymous e-cash to see something that would be free, or providing demographic information in exchange for a discount or customized service.

But right now, a consumer can't easily express his privacy preferences: He may have one preference for a site dealing with computer-industry issues, and another for his neighborhood after-school chat. We present different faces at work, at school, at church or temple, at the doctor's office. Likewise, your concerns for security may depend on the kind of interaction you are having: Are you simply revealing your name, or are you transferring cash, or revealing deep dark secrets? Of course, right now you can refuse to supply any data, but greater granularity would be beneficial to both sides.

What is needed is a way for both sides to express themselves, and a way to ensure that they are telling the truth. In practice, that means self-rating and honest disclosure, and with third-party verification to ensure honesty on one side and trust on the other. Such verification has another benefit: the spread of best practices via firms that specialize in privacy and security methodologies.

Privacy as an Assignable Right

The ideal solution for commercial consumer privacy is to rely on market principles rather than blanket regulation. As background, consider the work of economist Ronald Coase, who won the Nobel Prize for this insight among others. If you establish a right--whether it's for clean air, privacy, a pound of potatoes or a copy of a newsletter--that right will be allocated efficiently in a free market, regardless to whom it is worth more.[3] That is, the

market looks at the difference between the two sides' preferences, and the right goes to whomever values it more; a corresponding amount of value may change hands in the opposite direction.

In the context of privacy, the first question is whether Alice values her right to privacy more than WonderWidgets values the right to call her at home at 9 pm. If she does, she will effectively pay WonderWidgets for her privacy by foregoing the opportunity to receive a fee from the company. On the other hand, if she values her privacy less, she may sell the privacy--the right to call her--to WonderWidgets for that amount.

Defining "Privacy"

Unfortunately, those rights are not clearly defined. Second, they don't map easily to the pieces of data that we take to represent them: How does Alice distinguish between the right not to be called at 8 pm and the right not to be called at 9 pm--although they're based on the same telephone number? How does she control the proliferation of those rights (de facto, information) into the hand of others who might use it differently? Does she need separate contracts with all the people who might possibly telephone her? The market works well with defined items, less well with slippery pieces of data that change value as they get combined or change hands. Is the right to the piece of data, or to particular uses of it?

Indeed, when we say "privacy" we mean lots of things--everything from the (non)publication of information to control over exactly when one receives a telephone call. Does Juan mind if his information is in a data bank somewhere, unseen by prying eyes? No. But he goes ballistic if he gets called after 7 pm. Alice, by contrast gets the willies when she thinks of her transactions being recorded anywhere and seen by others, but she doesn't really mind the phone calls since the callers don't seem to know much about her. One does not want to be disturbed; the other is concerned specifically about privacy as an information issue.

Different people have different preferences for their own privacy.[4] Any of these preferences is fine--as long as it's clear what the rules are. The point here is that each Website should cater to the specific preferences of its users, rather than all following the same rules. Some people object in principle to the concept of privacy as an assignable right--one that can be sold or bargained away. They'd rather see it as an inalienable right, one the poor can enjoy as fully as the rich. But our principles tend toward maximum personal freedom--that people should decide for themselves how to value their rights. Since privacy is not an absolute, and individuals' preferences vary, it seems foolish to insist on an absolute approach.

SYSTEMS FOR LABELING CONSUMER PRIVACY PRACTICES

Fortunately, there are systems in the works not for privacy regulation, but for privacy *disclosure* and the labeling of data-management practices. Also, many Websites also have specific, disclosed privacy policies. It is up to the customer to decide on the value of his data and to act accordingly.

The first is eTRUST, a labeling and certification program sponsored by the EFF and CommerceNet of California. eTRUST is in pilot operations currently.

The second, complementary effort is in an even earlier stage; it is the IPWG, a coalition of about 15 companies and organizations convened by Washington's Center for Democracy and Technology. The IPWG is working with the World Wide Web Consortium trying to figure out how to extend the PICS content labeling protocol to the electronic labeling of privacy/data practices in a way that would allow automatic negotiation between a person's browser or agent, and the privacy rules of a Website.

eTRUST is a labeling system with three gradations, along with local rules specific to a site underlying the gradations. The IPWG's Platform for Privacy Preferences (P3) will be more granular, and will enable a way of representing specific privacy rules in computer-readable form. The combination of eTRUST's approach to labeling and certification, and the IPWG's approach to representation and automatic negotiation, could end up as a powerful advance in Net civilization.

These systems are contractual, and they can work without any changes in existing law. The initiatives described are grass-roots, and they are designed to foster a multiplicity of approaches to privacy management, rather than a Central Bureau of Privacy Protection.

eTRUST

Since work started last year, the eTRUST partnership has been enlisting sponsors/partners who will help to cover the start-up costs of the free-to-users pilot program. Participants in the pilot, with various kinds of involvement, include InfoSeek, WorldPages, Firefly, EUnet, Four11, Quarterdeck, CMG Direct Interactive, InterMind, Narrowline, Portland Software, TestDrive, Britnet, Perot Systems, USWeb, Switchboard, the Boston Consulting Group, and a variety of other organizations, commercial and otherwise. Two leading accounting firms are also involved in helping to design the program and in validating Websites' privacy claims: Coopers & Lybrand (C&L) and KPMG.

How it Works

To post the Trustmarks on its Website, the site must execute a contract with eTRUST, undergo an audit with an eTRUST approved auditing firm, and agree to certain conditions. The three levels of the Trustmarks are fairly simple:

No exchange: The site will not capture any personally identifiable information for anything other than billing and transactions.

1-to-1 exchange: The service will not disclose individual or transaction data to third parties. Individual usage and transaction data may be used for direct customer response only.

Third-party exchange: The service may disclose individual or transaction data to third parties, *provided it explains* what personally identifiable information is being gathered, what the information is used for, and with whom the information is being shared.

Of course, the devil is in the details, or in the phrase *provided it explains*. What exactly *will* the service do with the data and to whom will it be provided? Are those third parties bound by eTRUST too? Probably not.

Raising Awareness

Everyone involved with eTRUST stresses that it is a pilot program without final answers. Its goal is not to ensure universal privacy, but to get users to ask about and Websites to explain their privacy practices. The underlying assumption is that an informed market works better, and that customers need some guarantee that the information they get is true. Informed consumers can negotiate better deals individually, and shift the market towards more customer-friendly behavior in general.

eTRUST will work not by giving people new rights, but by encouraging people to exercise their existing rights and market power and by providing a model of how the market can work best by informing its participants. The Trustmarks call users' attention to the proposition that their data may be valuable and should be protected. Then they need to read further to find out exactly what the vendor is proposing.

eTRUST is a brand name; the premium value it indicates--its secret ingredient or unique selling proposition--is validation of the promises behind the Trustmarks. An audit by an accounting firm is a much better way of fostering compliance than a lot of regulations.

"Third-party Attestation"

What is the role of the accounting firm? Coopers & Lybrand has made an aggressive strategic move into what it calls "Computer Assurance Services." Over 1500 of its 70,000 professionals worldwide work in this practice. C&L's Internet Assurance practice, a 150-person subset of Computer Assurance, focuses on a small handful of areas, notable among them privacy reviews. C&L's eTRUST clients include Firefly, InterMind (a privacy-oriented publishing intermediary that G1lets you receive tailored content anonymously), and Narrowline. In an attestation review, the client makes specific assertions, which are then "attested" to by the independent auditor. These attestation reviews are governed by American Institute of Certified Public Accountants standards of practice. Independent third-party attestations from C&L about consumer data practices offer reasonable assurance that the business practices operate as intended.

For a Web-oriented client, the firm can support any of three stages: system design (establish audit, control and security requirements), system implementation (configure system and processes), and post-implementation assessment (validate that the control system is well designed and works as intended). All three are ongoing: Systems must be reassessed and updated, and procedures must continually be refined both to combat erosion and to adjust to new technology--particularly in security, which is basically an arms race with malicious crackers and negligent employees.

Site Oversight

Of course, an accounting firm cannot guarantee privacy. In conjunction with eTRUST it can offer a compliance mechanism--a license subject to review. The presence of a third-party auditing firm adds elements of oversight and trust to the eTRUST program. Obviously, any accounting firm could do the same, but eTRUST is an education and branding campaign as well as a compliance system with licensed auditors. Over time, eTRUST will have competitors. And obviously, eTRUST itself is eager to sign up as many accounting firms as it can.

Cost

While it should cost very little to participate in eTRUST itself, it does cost a lot to be properly certified, just as it costs a lot to be audited, especially for a public company. That's one of the realities of doing business. We can just hope that there will be vigorous competition in privacy attestation services as in other markets, and that supply will rise quickly to meet demand.

Although Webmasters who post the eTRUST logos on their sites will eventually have to pay a "small, graduated" fee to eTRUST, the service right now is free.[5] Logo posters will have to pay third-party attestors commercial rates for their validation service; that's between attesting accountants and their logo-posting clients. The accounting firms will also have to pay eTRUST a license fee. Beyond that, eTRUST is still working out its precise business model; it cannot support itself during its first couple of years. To the extent possible, we believe eTRUST should get its funds from the accounting firms--the people who get tangible revenue due to the program--rather than from the logo-posters. After all, the accounting firms have an immediate vested interest in the success of the project, although in the long run the logo-posters will find it useful in attracting customers.

Pilot Preliminaries

Money flow is only one of the issues the pilot is intended to sort out. Exactly how much work does it take to test for compliance? How often should logo-posters' claims be spot-checked? What are the vulnerabilities? Are the logos and their explanations intelligible to users?

What happens when someone fails in compliance? That's part of what eTRUST hopes to determine during the pilot and over the next year-- ideally without too many instances of non-compliance, but enough to show that the program is for real. The initial steps are cancellation of the right to use the logo and posting the wrong-doer on a "bad-actors" list; of course, the wrongdoer has to pay the costs of determining its non-compliance and ultimately could be sued for fraud. But stiffer, quicker penalties may be needed: The conditions shouldn't be so onerous that no one signs up, but they should be severe enough to be meaningful. Breaches are likely to be noticed through spot-checks by the third party attestors. Other sources of challenges are whistle-blowing employees or aggrieved users, although it's usually difficult to figure out who compromised privacy.

The data processing requirements behind privacy protection are also challenging, since some data will need to be tagged to be used only in certain ways.

There will also need to be contracts specifying the sanctity of the data as companies form, merge and break up. Do the contracts governing the use of data survive a bankruptcy proceeding? They should.

THE INTERNET PRIVACY WORKING GROUP

Independently responding to many of the same pressures as eTRUST, the Internet Privacy Working Group was convened by the Center for Democracy and Technology in Washington. Its planned "product" is a technical standard called P3, for Platform for Privacy Preferences. The IPWG is in many ways a continuation of the group that produced the PICS[6] content-labeling standard, and includes many of the same players. Members include America Online, Microsoft, Consumers Union, MCI, Dun & Bradstreet,

IBM, AT&T, the Direct Marketers Association, the Electronic Frontier Foundation, eTRUST, the Coalition for Advertising-Supported Information and Entertainment, the National Consumer's League, the Interactive Services Association and at least indirectly the members of the World Wide Web Consortium (W3C), which developed PICS and is developing P3.

The IPWG plans to produce substantial technical work later this year, but the first step is to come up with a vocabulary so people can accurately and explicitly describe what they want, to allow them to craft their preferences. The group hopes to develop demos for user testing by May, and then the developers at W3C can take it from there for implementation.

P3 in Practice

While content rating requires some formatting, its vocabulary is fairly free-form; any third-party rating service can establish its own terms and definitions. By contrast, a privacy vocabulary is more complex, and needs a grammar for expressing conditional preferences. That will enable not just static labeling of privacy practices, but actual negotiation between a customer's self-described preferences and the options a site offers.

Using P3, a user could specify what kind of privacy rules he wants to find or avoid, and his browser or other tool could implement those preferences automatically. A P3 program at the Website could describe its own practices and could also read a user's self-description. The two agents would then negotiate the terms of a transaction. At its simplest, this might mean that the user could see/ use only certain pages of a site that meet his privacy criteria. Special areas would be reserved for those willing to part with certain information. But as use of P3 spreads, users and sites could automatically negotiate far more complex interactions.

Would users trust such an automated system? That would depend in part on the auditing/compliance system behind the scheme. (The user's and the site's choice of auditor or auditing scheme could of course be specified in the label.) For all the same reasons as for eTRUST, IPWG label-posters will also have to devise some provisions for attestation--or ally with eTRUST--if P3 is to have any credibility.[7] With such a validation/ enforcement structure in place, P3 could have immense power.

MAKING IT REAL

How can these two complementary systems succeed? This question is of broad interest, since these two groups face the fundamental challenges of anyone trying to foster self-regulation in order to forestall *government* regulation. The Boston Consulting Group volunteered to do a pro-bono assessment of eTRUST's positioning and prospects, and its mid-term findings promise some interesting conclusions, for eTRUST specifically, for P3 and for other such efforts in the future.

The main conclusion is simple: eTRUST, P3 and efforts like them rarely work without a "hammer." Adoption of self regulation is a slow and arduous process absent some external pressure to prompt urgent action. The government or the threat of government action may promote urgency.

Hammers over Our Heads

Currently, the government is paying substantial attention to privacy issues on several fronts.

The Federal Trade Commission is conducting a long-term Privacy Initiative and is planning a privacy workshop to study technical tools and self-regulatory models to protect privacy--an effort in the right direction. At the same time, the Commerce Department's National Telecommunications and Information Administration is compiling a report on the issues around privacy self-regulation.

Both these efforts look promising for self-regulatory efforts such as eTRUST and P3. However, there are also several bills pending in congress: The Consumer Internet Privacy Protection Act of 1997 (Rep. Bruce Vento, D-MN), the Children's Privacy Protection and Parental Empowerment Act (Rep. Bob Franks, R-NJ), and the Communications Privacy and Consumer Empowerment Act (Rep. Ed Markey, D-MA). Whatever they are now, there is no telling what these bills may become as a result of political negotiations in Congress, where the focus is more on government regulation than on market-based solutions. Nor would the laws apply overseas, as both eTRUST and P3 will.

It remains to be seen whether eTRUST and P3 beat Congress to the punch, and whether the government's activities will hasten adoption of eTRUST and P3 in the marketplace.

Controlling the Sorcerer's Apprentice

What BCG found is not surprising. Industry disclosure schemes often founder without strong government/public pressure. Otherwise, companies are simply too busy to adopt them and customers don't factor the information disclosed into their buying habits. eTRUST's and IPWG's challenge is to raise the public's awareness just enough to make it want eTRUST and P3, but not enough that it puts the issue into the hands of the government.

Perhaps the most successful disclosure rules are those of the National Association of Securities Dealers; not surprisingly, they are mandated by law. Other schemes allow opt-in and opt-out, such as movie or television ratings--but the entertainment industry as a whole adopted them in direct response to the threat of worse from government. (These systems are not entirely satisfactory, as they involve central rating systems rather than a diversity of opinion and enforcement.) In many cases, BCG found, there is some complementary sector that forces self-regulation: In the case of movies, it was the theater owners; in the case of Underwriters Lab, it was first insurance companies and then retailers. For BPA International (formerly the Business Publishers Association), which audits business publications, advertising agencies forced regular auditing of circulation and other claims.

Beyond the Hammers: Making the Case

So beyond government "hammers," what are the forces that can encourage P3 and eTRUST? Who can play the role of hammer for eTRUST and IPWG, or for privacy self-regulation generally? "Anyone who provides a conduit between merchant and customer could potentially exert such influence," says BCG's Blackburn. "Browser vendors and

online services could offer privacy filters" much as many now offer (mostly optional) content filters.

Other possible players include the credit card vendors or newer payment and verification systems, on the one hand, and accounting firms on the other. The payment/verification systems need a lively new market which they could serve, and the accounting firms are looking for new forms of business--specifically, attestation about privacy and security practices. Is this enough to force the issue?

However, credit card companies are not so enthusiastic. They and their partner banks have significant interests in the use and exchange of customer information. To some extent, most major vendors and financial companies would not mind strong privacy-protection practices as long as their competitors were hampered by the same restrictions. It's simply that no one wants to go first.

Among the merchants--potential logo-posters--themselves, what kind of firms are most enthusiastic about eTRUST? Primarily smaller, less-known firms who ask customers personal questions about finances, health and the like. Unfortunately, those middle-market firms don't have large budgets to spend on auditing. Nor are they influential in persuading other firms to follow suit.

Larger firms with existing customer bases and reputations don't need eTRUST and P3 so much; the truly bad actors don't want them. For the larger firms it's not merely a question of brand recognition and size. Big firms with good reputations are also likely to have a lot of data from other sources, and they may not want to apply different standards for Web-source data. Nor do they necessarily want to adopt the same standards they use for Website data for all their data. They may not want to go through the expense and hassle of a privacy audit without a clear idea of how it might benefit their business.

Nonetheless--or accordingly--BCG and eTRUST would dearly like to see a couple of large influential merchants adopt eTRUST. Yes, Amazon may be more influential on the Net than, say, Borders; on the other hand, traditional merchants may be much more influential among customers new to the Net.

The trick is to persuade merchants of all sizes that privacy is a compelling and vital marketing issue. There are two groups that can deliver this message most effectively: the accounting firms who see privacy attestation as a business opportunity; and customers themselvesassuming that the message is true.

Remember the Customer

Little can be done without a clear customer benefit. So BCG is trying to discover just what concerns consumers about privacy--which is often confused with security. Consumers say they would be a lot more active on the Net if there were privacy, but what does that mean? Are they afraid of having a credit card stolen? Do they simply want to know what happens to their data, or do they actually want to stop its spread? In fact, their answers vary a lot--by vendor, by kind of data and subjectively. How much do they want that loan? Are they in a good mood?

How do we get people who don't necessarily care about privacy to do so? How can we take the generalized resistance to the Net, sharpen it into privacy concerns, and then assuage those concerns with eTRUST?

Indeed, should we? Or are we simply creating spurious needs to fill? Yes, we should. Everything tells us that customers feel more and more bewildered by the array of choices facing them. They may not worry about a telemarketer's calls, but they do feel uncomfortable at the prospect of giving personal information to strangers. eTRUST and P3 are all about giving people control to use the powers created by technology.

Where to From Here?

eTRUST and P3 possess the advantage that they are not moralistic, evangelistic or dependent on government (other than for enforcement on the basis of fraud). They are simply two examples of the kind of grass-roots effort at self-regulation in all spheres that may well benefit users of the Net.

CASE STUDIES

In practice, privacy protection is more than technology. How can we achieve it without making the world into a sterile place where everyone is anonymous? Customers actually like to be treated as known individuals by marketers that they in turn know and trust. After all, the rhetoric promises a global village, not a global city.

The following case studies show how individual companies can handle privacy issues, and present their practices as a customer benefit rather than a legal issue. Their practices are still evolving, along with customer preferences and pressures from those outside hammers.

Four11: Privacy Issues in Practice

Simply managing transaction data is simple compared to the privacy issue of running a directory service. For example, take Four11, a leading Web "white pages" company. The basic service is collecting and maintaining a database of individuals' names, e-mail addresses, phone numbers and other data. The telephone data is licensed from Metromail; the e-mail addresses come from user registrations (20 percent and growing), public-domain directories on the Net (50 percent), and Usenet (declining).

People are encouraged to register; you can also ask to be stricken (even if you show up again from another source). All this data is available to anyone who visits Four11's Website--but only a bit at a time. Aside from its acceptable-use policies (restricting wholesale reuse and general abuse), the company has no hard and fast rules in order to be flexible enough to stop new problems as they arise. For example, the company makes it difficult for users to collect names for mass e-mailing or for building any kind of secondary database. It supplies information only one e-mail address at a time, and it monitors user activity for unusual behavior, such as downloading one address after another. (It doesn't care who you are, but it does care what you do.) Currently, when Four11's server detects such a pattern it notifies a system administrator; in the future, it may invoke an automated response.

Also, you can't find a name from a phone number or from an e-mail address; you need to know a person's name before you can get anywhere. However, that wasn't always true. The company licensed its database to Yahoo! last summer. Yahoo! did allow reverse searching, using the Four11 data--creating the Net's most visible, most-used reverse look-up for phone numbers. Yahoo! put it up in April last year, and it quickly became one

of the most-used functions within Yahoo!'s people search. Four11 CEO Mike Santullo says he felt uncomfortable about the reverse look-up service, but both parties note that it was tremendously popular and did not actually lead to many problems.

Both companies were punctilious about delisting people who asked for their names to be removed. Meanwhile, police departments, suicide prevention centers and other "good guys" made good use of the service. "Bad guys" didn't seem to be more prevalent than the annoying people who use caller ID. But in December, in response to perceived pressure, the companies dropped the service. Similar information is still available, but sometimes from companies who may be less careful than Yahoo and Four11.

It's a pity that such a potentially valuable service should be abandoned and relegated to non-mainstream providers. The moral of this story-- which is not yet over--is that a little self-regulation or more fine-grained control over personal data may actually yield a situation where information is more readily available. But for now, it's all or nothing.

That's the long-term question: How can you make information available selectively? Four11 is addressing that in part, although not with reverse look-up for now. People willing to register with the service can get selected additional information about others; presumably, being registered themselves makes them less likely to abuse the information. For example, they are allowed to search the database for people by affiliation, such as Princeton High School, violinist, etc. This information comes from individuals and from the groups themselves; they in turn can specify what information they give should be made available, and to whom. For example, a person's initial record won't show the schools he attended, but if you happen to know (or guess) Princeton High School, that will show up once you ask specifically. Some groups let only group members query on group-oriented data, so only PHS alumni could find out that other people are PHS alumni, or what year they attended. In fact, Four11's business model includes support of such interest groups, even as it is also addressing the mass market through alliances with companies such as Yahoo!, InfoSeek, Nynex and US West.

Yes, it sounds cumbersome and awkward and somewhat arbitrary, but isn't that the way it is in real life? The folks at Four11 have thought about all this a lot, and will refine their approach as they encounter new problems and solutions over time, says CEO Mike Santullo. The main thing is to be aware of the issue.

Narrowline: Mediating Between Advertisers and Audience

Narrowline is an ideal customer for a new-style auditing firm: It sells things you can't see, and part of the value of the service is that you can't see them--in the sense of protecting the privacy of customers. The company is about to roll out its service, Brought To You By, a trading floor for sponsorship of content and events. Brought to You By has the granularity of a classified-ad market where what Narrowline calls "Netcasters" (content/community providers) and sponsors (advertisers) can find one another, based on the audiences they're seeking or can deliver.

Narrowline adds value to its market with metering and verification for the advertisers and privacy protection for the Netcasters and their audiences. Not only do the audiences presumably appreciate their privacy, but the Netcasters can also keep the sponsors from bypassing them to talk to individuals directly--unless an individual makes the first approach back to the sponsor.

Founder Tara Lemmey understands that a primary feature of the Internet is its support for reaching market segments, instead of broadcasting the same message to everyone--even if you don't know each one individually. But you can't do that unless you find and define those markets and figure out how to reach them in almost real time. Narrowline sells access to particular demographics through sites, but doesn't pass on to the sponsors any detailed information about the visitors/members of the site. Obviously the value of the service depends on rigorous integrity, both in guaranteeing the users their privacy and sponsors that they are getting the demographics they are paying for even if they can't see them. In that context, Narrowline is an ideal customer for C&L, because it needs auditing for just about everything.

When a customer visits a site sponsored by a Narrowline advertiser, the text and editorial come from the Netcaster, while the banners come from Narrowline and its advertisers. Narrowline meters the banners and knows who's receiving them. It provides a barrier with assurances to both sides: That their identity is safe to customers, and that the demographics are reliable to advertisers.

What this means is that the customer simply has to trust Narrowline instead of all the advertisers he may encounter. For now, however, consumers don't necessarily know Narrowline either, but its use of the eTRUST Trustmarks means that the eTRUST brand will be applied to advertising from sponsors who don't sign up with eTRUST specifically. The sponsors get demographics they can trust, but they don't have to go through the trouble of an eTRUST audit because they never see the data that only Narrowline collects.

Narrowline's approach raises an issue that will increase in visibility as more and more Websites are acquired by other companies or join alliances. Just how broad is the entity to whom you are giving your information? Can you trust it? Or is it really "they"?

Juno: Free E-mail in Exchange for Your

Information

Many sites and services make more explicit bargains. Juno, for example, offers customers free e-mail in exchange for exposure to specific advertising based on the user's characteristics. The service has been a success with end-users: About 1.5 million people have signed up for it, filling in a detailed profile in exchange for free e-mail. They do not have to have Internet access, since Juno offers its own local dial-up throughout the US, and they do not get Internet access, but they can send and receive e-mail across the Internet. They can also view graphics-filled ads from Juno's advertisers and from Juno itself. The site looks something like a Website, and its ads look like Web banner ads, but the only people who can use it are registered Juno customers.

Although the service is free, it's not quite "the people's e-mail." It still skews Internet-wards, says Juno president Charles Ardai: mostly male and higher income. You may not need to pay for Internet access, but you still do need a computer with a modem.

The users' identity is not revealed to the advertisers, who simply get a report such as "5482 men between 18 and 49 who have expressed interest in new car saw your ad last month; please pay $2,741 within 30 days." Juno may also tell them, for example, that 25 percent of the people who clicked on their ad were female.

But how is an advertiser to know this is true? Juno's financials and other numbers, including claims to advertisers, are audited by Coopers & Lybrand. "Unlike a Website,

we're pretty simple to audit," notes Ardai. The only people who visit are its own registered and profiled customers, using Juno's own software.

On the revenue side, Ardai isn't ready to proclaim victory, but he notes a set of repeat advertisers: American Express, Lincoln Mercury, Miramax, Okidata, Bausch & Lomb. "When we hit a million members, major advertisers started returning our calls," he says.

Juno has discovered that it can also sell products itself to its customers--a cookbook to someone who's indicated an interest in cooking, for example. She can send back a purchase order with ease, he notes, and her credit card never goes over the Internet. (That may not be a real issue, but it makes some customers feel more secure.) And people who respond to an advertiser's direct offer, of course, lose their anonymity.

Given that this is a free service, we wondered if there were any people who might be left out, if their demographics just don't meet any advertisers' criteria. That could happen as far as advertisers are concerned, says Ardai, but it sends at least some of its own product offers to each of its customers. And it allows anyone to be a customer. As a private company, for now, Juno can afford to serve everyone--founder David Shaw's quiet little contribution to the public welfare.

ENDNOTES

1 eTRUST is a joint project of CommerceNet and the Electronic Frontier Foundation. It is chaired by the author.

2 The Internet Privacy Working Group is separate from eTRUST, but responding to many of the same pressures. IPWG was convened by the Center for Democracy and Technology. Still in its early stages of development, IPWG is discussed later in this paper.

3 The issue of who owns rights (and other assets), and who can afford to keep and exercise them rather than sell or exchange them, is one of social justice, which is not our concern here. The only point to make here is that if rights are too concentrated, their owners may not use them properly--and the outcome will certainly be unfair.

4 There are already many laws concerning privacy. In the United States, information about individuals' video purchases is protected--the result of one unfortunate experience by one legislator that resulted in the law. On the other hand, data linking a person's driver's license number with name, address, age and other personal data is available from Departments of Motor Vehicles in many states. Much commercial data is more carefully protected, but often more for commercial reasons than out of respect for the privacy of the individuals concerned. By contrast, the European Commission places strong controls on the use of personal data, to the extent that many companies find it difficult to do business across borders; they can't even transfer data about their own employees from one country to another.

5 "Users" are end-users, customers, people who visit a site, and who read and rely on the logos. "Logo posters" are users of the logo, but are referred to as posters to distinguish them from their customers. A third class of users are the firms licensed by eTRUST who validate the logo-posters' claims, usually accounting firms; we call them "third-party attestors."

6 PICS stands for Platform for Internet Content Selection and is a standard protocol for labeling Internet content.

7 eTRUST Trustmarks are a logo for people to see on a Website; P3 labels are executable code for a browser or other software tool to read and communicate with.

A Description of the eTRUST Model

Andy Blackburn
Manager
Boston Consulting Group

Lori Fena
Executive Director
Electronic Frontier Foundation

Gigi Wang
Director of eTRUST Program
Commerce Net

EXECUTIVE SUMMARY

Growing concerns about the security and privacy of telecommunications-related personal information are threatening to constrain the growth of electronic commerce. Effective action to increase the level of confidence in online privacy must include assurance and monitoring (through both active and passive means) of the business practices of entities that have the ability to collect, use and distribute personal information. Without such action, numerous violations of privacy are likely to occur, damaging public confidence in electronic commerce and potentially precipitating government action.

The eTRUST model provides a mechanism for industry self-regulation that can provide public assurance of privacy. It utilizes an approach that combines long-term sustainability through industry financial support with consumer credibility through a process of independent assessment and monitoring of business practices.

In order to be successful in its mission, eTRUST must build consensus within the online business community that the self-regulation represented by the eTRUST licensing program is worthwhile from a business and societal perspective. It will also establish awareness and confidence with online consumers that the eTRUST logo provides adequate assurance that their personal information is being protected. In order to build critical mass it is essential that eTRUST simultaneously build customer awareness and merchant acceptance.

In the short run, this will require that eTRUST obtain the financial sponsorship and operational involvement of leading business and government organizations that have vital interests in ensuring online privacy. To that end, eTRUST welcomes involvement, support and sponsorship from relevant business and government entities in helping to

build an effective structure for industry self-regulation and growth.

CONTEXT

Electronic commerce over the Internet has been growing at an accelerating rate, transforming the once academic- and research-oriented network into a global electronic marketplace. Participants in electronic commerce envision that this marketplace will be enabled by:

Millions of consumers, companies and value added services;

Consumer and business-to-business oriented online transactions in financial services, health care, manufacturing, retailing and hundreds of other market segments;

Common technology platforms for security, payment, directories, EDI, collaboration and other essential services; and

A global business community with conducive legal and regulatory structures and standards for business practices.

The new world of electronic commerce has the potential to make many existing forms commerce more efficient, productive and convenient. It also offers the possibility of entirely new forms of business that have been impractical until now. The potential benefits to the US and world economies in terms of growth and job creation are quite large.

Electronic commerce is now at a crossroads as it makes the transition from early adopters to mass market. As the user profile grows more mainstream there is an increasing focus on transactions, leading to a fundamental rethinking of how personal and business information is exchanged and used.

The growth of electronic commerce is in danger of being hampered by customer concerns about the security, privacy and content of Internet- based offerings. Concerns regarding security, privacy protection and content are further heightened by the growing proportion of children online. Recent privacy-related scandals have helped turn trust into a key issue for consumers in particular. Results from a recent survey underscore that privacy and security are leading concerns to consumers.

Top-ranked barriers to electronic commerce adoption[1] are:

- Lack of security 26.6%
- Privacy 19.5%
- Availability of content 11.7%
- Lack of standards/infrastructure 10.9%
- Social acceptance 7.0%
- Multiple other reasons 18.1%

The current absence of privacy assurances exposes online users to serious risks of privacy violation. Privacy applies to both individual and corporate-oriented transactions--from information transiting the World Wide Web to the electronic records employers keep

about their personnel. Although commerce is a major driver of these kinds of information transfers, privacy issues also arise from wide range of non-financial information transactions.

Direct marketers have shown increasing creativity in developing new channels to gather highly valued customer information in the offline world. The Internet and the World Wide Web give marketers and merchants access to sophisticated tracking systems which are becoming the main tools for gathering and manipulating customer information online, and offer the potential to go well beyond existing practices. These powerful new tools also offer the opportunity to misuse or abuse private, sensitive, personal information, often without the subject's knowledge or consent.

It is important for merchants and other major players in Internet commerce to put in place some system for addressing this customer concern both to further the development of online transactions and to obviate potential government regulatory intrusion in the electronic marketplace. Considerable effort is being devoted to developing technologies that will ensure security for online transactions. But technology-oriented approaches alone do not represent an adequate solution for privacy concerns, because assurance of privacy requires analysis and monitoring of vendors' business practices in order to be effective and credible with the public.

THE eTRUST MODEL

eTRUST's mission is to establish individual and institutional trust and confidence in electronic transactions. The organization intends to build this public trust and confidence through a system of "trustmarks", or logos, covering issues of concern to end users. The "trustmarks" will be backed by an accreditation procedure with guidelines for businesses and organizations who license them. The eTRUST concept is modeled on approaches that have proven effective in the self-regulation of other industries, and includes:

A branded, integrated system of"trustmarks" which represents assurance of privacy and transactional security. These "trustmarks" are backed by an accreditation procedure with guidelines and standards for businesses or organizations who license them.

An extensive education and awareness campaign for both businesses and consumers.

An assurance/enforcement/compliance process involving self-assessment, community monitoring, spot checks and professional third- party auditing.

A scalable system for the components of the program, including the compliance process, based on the different types and sizes of businesses and organizations and the changing marketplace.

An open process and infrastructure for establishing and modifying guidelines as market needs change.

Privacy and security are in many ways interlinked. While the eTRUST model is applicable to both privacy and security, privacy assurance will be the initial focus of the trustmark system. eTRUST is currently developing a three-tiered series of privacy trustmarks which characterize how personal information will be used:

No Exchange--for anonymous usage of a site

1-to-1 Exchange--for information that will be used interactively between the user and the site, but not released to third parties

3rd Party Exchange--for information that may be disclosed to third parties.

Each of these trustmarks indicates that sites bearing them adhere to a specific set of guidelines.

In addition to providing a process whereby business practices relating to the use of personal information can be assessed and monitored, the eTRUST model also requires *disclosure* of those business practices to the individual providing the information prior to any transaction. Disclosure falls into two categories:

Privacy disclosure. Elaborates on an Internet business's information gathering practices. A user should be informed in advance what personally identifiable data is being gathered, what the information is used for, and with whom the information is being shared. The eTRUST service mark or "trustmark" assures the user that his personal data is being handled as outlined in the privacy guidelines and disclosures policy.

Transaction security disclosure. Elaborates on the execution of the transaction from the user to the actual point of service. A user has a right to know if the transaction into which they are entering will be protected during its execution and storage. The "trustmark" will provide users with the data necessary to judge for themselves if the protection of the transaction is sufficient.

General operating guidelines for sites licensing any of the eTRUST logos are as follows:

Disclosure of Information

The service must explain and summarize its general information gathering practices.

The service must explain in advance what personally identifiable data is being gathered, what the information is used for, and with whom the information may be shared.

The user can correct and update personally identifiable information.

The user can request to be deleted from the site's database.

Communication Monitoring

The service may not monitor personal communications such as e-mail or instant messages.

Display of Names and Contacts

The service will not display or make available personally identifiable name or contact information without the consent of the user, unless the information is publicly available.

In order to obtain an eTRUST trustmark license, an applicant organization must submit to a site review prior to receiving the license, to ensure conformance with guidelines. In addition, eTRUST may conduct subsequent audits of the site at any time during the license period. eTRUST will put in place an enforcement process to ensure that sites displaying the trustmarks are in compliance. Violations could include license revocation under appropriate circumstances.

The eTRUST model is also scalable, allowing the organization to address, under the same umbrella concept, a broader array of online security and privacy issues:

Accrediting businesses and merchants who deal directly with consumers. In later phases, accrediting providers of products and services that contribute towards building trust on the Internet, including a process for accrediting certification authorities.

Extension of the eTRUST system to provide the consumer with more precise control over how and with whom his/her personal information will be shared.

Expansion into other relevant elements of the Internet marketplace such as quality (Better Business Bureau-type of service) and content rating (PICS) is also planned.

Extension to additional value-added services (*e.g.* 3rd party provision of liability coverage for the assurance process).

Development of "vertical" offerings (*e.g.* focusing on children or medical information).

Precedents of the eTRUST Model

There is a well established history in the US and around the world of industry sponsored entities that promote voluntary self-regulation. eTRUST seeks to emulate the successful, relevant aspects of these organizations in developing its operating model. Examples of US-based industry groups that offer product or business-practice oriented monitoring and self regulation include:

Underwriters Laboratories (UL). UL's primary mission is to help get safer products to market by offering manufacturers a array of conformity assessment and product certification services. Nearly 40,000 companies worldwide have paid UL to have their products certified. Conforming products bear one of UL's familiar listing or classification marks.[2]

Better Business Bureau (BBB). The BBB is made up of 137 local, business funded organizations whose mission is to "foster the highest ethical relationship between businesses and the public through voluntary self regulation, consumer and business education"[3] The local BBB system and the National Council of Better Business Bureaus together are sponsored by 230,000 local business members and some 300 national corporations. The organization is currently considering allowing business members in good standing to use the BBB logo in their advertising.

National Association of Securities Dealers (NASD). The NASD was established under the 1938 Maloney Act Amendments to the Securities Exchange Act of 1934, and is responsible for the regulation of the Nasdaq stock market and the over the counter securities market. NASD carries out its regulatory responsibilities through "education, registration and testing of securities professionals; on-site examination of securities firms;and cooperative arrangements with government agencies and industry organizations."[4] These organizations, and many others like them, provide effective, voluntary self-regulation to their respective industries, with the active support of business sponsors and relevant government bodies. They also demonstrate the potential viability of an analogous entity to serve the interests of online privacy and security.

eTRUST OPERATIONS

For an industry self-regulating entity like eTRUST to be practical, it must be economically self-sustaining. It must also be built on a model that is affordable to the industry in order to build a critical mass of participants. It is also clear from existing examples of industry self-regulation that the self-regulating entity must provide meaningful, independent monitoring and assessment of business practices to have credibility with consumers. These factors point to an operating model that generates revenues from the market in order to fund independent monitoring of the businesses in that market. Like the many analogous organizations currently serving other industries, eTRUST is intended to be an industry funded organization.

Financial Model

Preliminary financial forecasts project that eTRUST can become self-sustaining after a two year ramp-up period. In the mean time, sponsorships will provide the financial resources to develop the brand and fund operations for the first two years.

Revenues will be generated from: licensing the "trustmarks" to businesses/merchants and to third-party organizations--both domestically and internationally; sponsor fees; value-added services.

Major expenses primarily will be related to the salaried staff in charge of managing and operating eTRUST, as well as covering auditing costs, marketing communication/PR and education campaign expenses to build awareness of eTRUST in the marketplace.

Working Groups

eTRUST establishes industry standards and practices through a series of working groups on each of the relevant topics. There are currently five working groups: privacy, transaction security, accredited authentication, eTRUST business model (including pricing and audit issues), and marketing/public relations. These working groups are made up of representatives from the Internet community and other interested parties. Membership in the working groups is completely open.

Current eTRUST Sponsors/Participants

Widespread support and participation from all areas is critical for eTRUST to succeed as the self-regulation model for privacy issues on the Internee. eTRUST has a growing base of support and participation from industry, consumer groups, and the government. The initiative was launched in July 1996 by a coalition led by the Electronic Frontier Foundation (EFF) and included the following group of companies involved in the Internet marketplace:

Coopers & Lybrand

CyberSource

Firefly Network

InfoOnline

KPMG Peat Marwick

Narrow Line

Organic Online

Portland Software

Test Drive Corp.

TS Communications

World Pages

This group developed the initial concept for eTRUST along with developing the first set of guidelines for privacy disclosure of information on a Web site.

CommerceNet and the EFF then joined together in October 1996 to form a partnership of industry and consumers to develop and implement the eTRUST concept. Commerce Net is recognized as a leader in electronic commerce with over 200 international member companies and organizations. EFF is a recognized champion of civil liberties and consumer rights in the electronic medium with widespread influence with consumers worldwide.

eTRUST already has received extensive media attention in newspaper articles in *The San Jose Mercury News* and *American Banker's News* and in magazine articles in *Business Week* and *PCWeek,* along with television coverage in *CNN Headline News* and *MSNBC.*

eTRUST Roll-out

Response has been received from over 200 parties interested in being involved in the eTRUST pilot program, which was announced in November 1996. This pilot program will evaluate the eTRUST model and refine design and implementation details beginning in the first quarter of 1997. eTRUST has engaged The Boston Consulting Group to assist in this process. Initially, 50 sites have been chosen as participants with the goal of reaching 100 pilot sites by the end of the program. Interested parties include corporations such as America Online, Sun Microsystems, DigiCash and the US Post Office. International players like EUNet and BritNet are also joining the pilot program.

In the first half of 1997, eTRUST will launch a commercial offering for businesses and other organizations to license the eTRUST privacy "trustmarks" for their Web sites. In the interim eTRUST is seeking sponsors to provide seed money to support eTRUST in the startup phase and to subsidize the first two years of operation.

SUMMARY

The eTRUST model provides a mechanism for industry self-regulation that can provide public assurance of privacy. It utilizes an approach that combines long-term sustainability through industry financial support with consumer credibility through a process of independent assessment and monitoring of business practices.

ENDNOTES

1 Arthur D. Little/Giga Information Group Study, October 1996.

2 Source: Underwriters Laboratories Web site (**www.ul.com**).

3 Source: Better Business Bureau Web site (**www.bbb.org**).

4 Source: National Association of Securities Dealers Web site (**www.nasd.com**).

1. This paper was invited by the National Telecommunications and Information Administration as part of its effort to further the debate on effective implementation of privacy practices using a self-regulatory approach. In order to meet length constraints, we have omitted here discussions of a number of related topics and provided only a few general references. A longer paper treating this topic and others ("Using Computers to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes") with a more extensive reference list is available at http://www.cpi.seas.gwu.edu/Papers/.

2. This paper does not reflect official AT&T policy. AT&T Labs' Public Policy Research Department creates and analyses new communication technologies that are intended to serve public goals, and facilitates public discussion of these technologies.