Information
and Privacy
Commissioner/
Ontario

Privacy: The Key to Electronic Commerce

Ann Cavoukian, Ph.D.
Commissioner

April 1998

Information and Privacy Commissioner/Ontario

80 Bloor Street West
Suite 1700
Toronto, Ontario
M5S 2V1

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Web site: http://www.ipc.on.ca

The Information and Privacy Commissioner/Ontario gratefully acknowledges the work of John Eichmanis in preparing this report.

This publication is also available on the IPC Web site. Upon request, this publication will be made available on audio tape
to accommodate individuals with special needs.

Table of Contents

Introduction

> In the 1990s, the technology underlying the Internet is making it even easier and less expensive to gather, store, analyse, transmit and reuse personal information in ways that were unimaginable just a few years ago.[1]

With the rapid development of national information infrastructures[2] to support the creation of national and global information highways, there has been a growing recognition that the new information technologies, particularly those that utilize the Internet, could form the platform for national and international commercial transactions, or electronic commerce. National governments and the private sector, driven by global competitive pressures, are seeking to create the necessary technological, legal and policy frameworks that will support electronic commerce.[3]

The growth in the popularity of the Internet (Net),[4] particularly the portion known as the World Wide Web (Web), has focussed attention on its potential to radically alter many of the ways that humans have hitherto conducted their interactions. Many face-to-face interactions can now be conducted electronically at great distances, without the participants knowing each other.

The Internet's openness, however, poses problems as well as great promise.[5] It has been generally recognized that commercial transactions require a high level of trust and confidence in the integrity and security of the Net, before individuals will provide 'meaningful' or accurate personal data to Web sites.

In this context, privacy, as an issue for electronic commerce, has been acknowledged by national governments and international organizations. There is consensus that a solution needs to be found before the full benefits of electronic commerce will come to fruition. Among international organizations working in this field are the United Nations, the Organization for Economic Cooperation and Development (OECD), the European Union (EU),[6] and the Bank for International Settlements.[7] The Canadian government, for its part, has indicated its commitment to the early introduction and use of electronic commerce within the public and private sectors.[8] The Ontario government, too, is studying the issue and pursuing ways in which to implement electronic commerce.[9]

Another driver of the privacy issue is coming into force in October 1998, in the form of the EU's *Directive for the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data*. The Directive on Data Protection will control, among other things, the flow of personal information out of the member countries of the EU. Non-EU countries judged not to have 'adequate' protection could be prevented from receiving personal information from EU countries. Harmonization of personal data protection legislation and policies will need to be considered by other countries if they hope to conduct business with the EU. Since electronic commerce relies heavily on the collection and use of personal information, the directive could have a serious negative impact on the flow of personal information from the EU to non-member countries judged not to have adequate protections.[10]

Various pressures are creating a climate in which advanced industrial countries are engaged in an intensive dialogue, at national and international levels, over a range of issues that are seen as impediments to the rapid use of the Net for online commercial transactions. Protecting personal information is one of the issues being actively discussed. Members of the OECD hope to reach a consensus on these issues, including the question of privacy and data protection, at a meeting scheduled in Ottawa in October of 1998.[11] Canada has initiated its own debate on this issue with the release in January 1998 of the federal government's consultation paper, "*The Protection of Personal Information: Building Canada's Information Economy and Society.*"[12] Moreover, in February of this year, the European Commission proposed the adoption of a non-binding international charter to govern the Internet, including references to privacy and data protection as issues requiring international consensus.[13]

This paper will seek to identify the privacy issues involved in electronic commerce and the range of possible solutions that may be adopted as ways to resolve those issues. The first part identifies the type of electronic commerce that poses the most critical privacy problems, and provides a brief discussion of how important personal data are to that type of transaction. The second part seeks to identify what the most important privacy issues are in this context, while the third part discusses the solutions that are being considered, particularly ones that are technology-based. The final section draws some broad conclusions regarding the need for co-ordinated action by interested parties in creating consensus around the solutions proposed, followed by informing the public about its choices on dealing with privacy issues in the context of electronic transactions.

Part One:

Electronic Commerce and the Role of Personal Information

> Electronic commerce is about doing business electronically. It is based on the electronic processing and transmission of data, including text, sound and video. It encompasses many diverse activities including electronic trading of goods and services, online delivery of digital content, electronic fund transfers, electronic share trading, electronic bills of lading, commercial auctions, collaborative design and engineering, online sourcing, public procurement, direct consumer marketing, and after-sales service. It involves both products (e.g. consumer goods, specialised medical equipment) and services (e.g. information services, financial and legal services); traditional activities (e.g. health care, education) and new activities (e.g. virtual malls).[14]

Electronic commerce encompasses commercial transactions of the type described above, using open and closed networked information and communications systems that connect computers and software, facilitating the transmission of digitized data. Recently, public attention has focussed on the potential of the Internet, especially the World Wide Web, as the platform for electronic commerce, since it offers an easily accessible interface between all users of the Net, both buyers and sellers, on a global scale. Creating such a commercial platform on the Net is a relatively new development. Most electronic commerce to date has involved business to business, or business to government transactions, conducted over closed proprietary systems rather than over the open lines of the Net. There seems to be universal consensus that commercial transactions between businesses and individuals, between individuals and individuals, and between individuals and governments will form the next stage of the evolution of electronic commerce, which by the year 2001, is estimated will grow into a $220 billion market.[15]

In this paper, the focus will be on commercial transactions in which individuals are the customers or buyers of goods and services, whether from the private or public sectors, and where the transactions take place over open networks, namely, on the Internet. From a privacy perspective, the open systems of the Net pose problems of a different order than those of closed systems. The reason for this limitation is due to the nature of the technology: closed systems are relatively secure from unauthorized intrusions, while open systems are not.

Having determined that our focus will be electronic commerce over the open systems of the Net, we also have to appreciate the role and importance that personal information has come to acquire in the era of information technologies.

One of the most significant aspects of the Information Age has been the commodification of personal information, that is, its commercialization and monetization.[16] Today, personal information has a market value which has been estimated at $3 billion in the United States.[17] It is the raw material that fuels a multi-billion dollar industry. “Selling personal information is big business.”[18]

Personal data are collected by Net servers, stored by database developers, and then sold to marketers and advertisers. The value of personal data today resides in the fact that detailed information is available about a specific individual’s behaviour, personal preferences and demographic particulars, which allows him or her to be micro-targeted by customized solicitations. In the earlier days of a ‘mass’ market, little was known about any given individual’s buying preferences. While surveys were used to try to determine what those preferences might be, such surveys were too broad an aggregation to be valuable across a range of buyers and locales. Now, databases are being created that can keep a record of assorted individuals’ buying habits and preferences.[19]

Various techniques are being used to collect personal data, through a variety of means -- loyalty and credit card schemes, the creation of detailed mailing lists, and data captured over the Internet. When individuals surf the Web, a record is maintained of every Web site and every page on a Web site that has been accessed, including possibly e-mail addresses received and sent, as well as participation in various ‘newsgroups.’ This information is called *clickstream* information (clickstream literally means the recording of each mouse click that locates a Web page you have selected), and is gathered invisibly, in most cases without the knowledge or consent of the consumer. There is virtually no awareness of the fact that one’s clickstream is being tracked or that the Web sites one visits are being logged.

In addition to the automatically collected information just described, a great deal of information is unknowingly volunteered by individuals themselves. For instance, you might fill out an online questionnaire or registration form in order to receive access to a particular site or to be included in one of the many online directories (not realizing the variety of other ways in which it may be used). As well, *cookies* can be used, not only to track but also to create profiles of Net users’ interests and browsing patterns. (A cookie is information sent to your browser from a site on the Internet and stored in your hard drive that tracks which Web sites are visited; scripts on the Web server could use the cookie file for tracking user movements within that particular Web site to profile individuals.)

Such information becomes increasingly valuable for companies and firms that wish to learn about the preferences of individuals across various demographic indicators and locations. Companies that create and maintain such databases, i.e., data warehouses, can sell these databases to other businesses and create broader databases by melding together additional personal information.[20] The end result is the creation of detailed personal profiles on numerous individuals. What is now being contemplated is the linking of these databases to the Web so that users can query them and conduct their own analyses.[21]

One could argue that the collection of this type of personal information makes the information itself the unit of exchange, since the service is provided free of charge in monetary terms, but in exchange for the service, personal data are collected and most likely further sold. Indeed, some critics have argued that individuals should be able to obtain modest royalties in exchange for the use of their personal information.[22]

If personal data are commercially valuable, one may conclude that economic incentives exist that will circumscribe the privacy concerns of individuals. As recently reported:

> … the conflict between a customer's right to privacy and the money that can be made by selling that information to third parties is expected to grow as electronic commerce over the Internet becomes mainstream.[23]

And yet, the public, by overwhelming numbers and in countless surveys, has revealed a marked preference to preserve as much privacy in their personal information as possible.[24] Most recently, a poll reported that over 80% of the public was concerned about their online privacy and security.[25] In another recent survey of Web users, 72% indicated a preference for the creation of new laws to govern the Internet.[26] Such consistent public apprehension over online privacy has prompted considerable research into various privacy-enhancing technologies. These technologies range from those that entirely eliminate privacy intrusiveness, to those that seek some compromise between complete privacy (anonymity), and the disclosure of identifiable personal data with the consent of the individual. Most efforts in this area tend to favour those approaches that neither eliminate the commercial incentives to collect personal data, nor the individual's incentive to provide his or her personal data voluntarily.

Part Two: Privacy Issues

> The lack of perceived privacy in electronic transactions is a barrier to the growth of online commerce.[27]

Commercial transactions between individuals and businesses using the Net raise a variety of issues about the adequacy of the medium for this purpose, particularly with respect to how capable this medium is in protecting personal information. At this relatively early stage in the development of electronic commerce, the following problem areas have been identified: the vulnerability of the open network to interceptions and faulty technological design, as well as the question of what laws and procedures can be applied to the Internet to regulate how personal information will be collected, used and disclosed.

The Vulnerability of Open Networks

The construction of the Net as an open communications system, while making it inter-operable, has also made it vulnerable to certain risks, including surreptitious intrusions such as 'hacking,' as well as human error. Three overlapping types of risk have been identified:

- Bugs and misconfiguration problems in the Web server that allow unauthorized remote users to steal documents, gain information about the Web server's host machine, which in turn allows them to break into the system;

- Browser side risks that could result in the misuse of personal information knowingly or unknowingly provided by the end-user;

- Interception of network data sent from the browser to the server or vice versa, via network eavesdropping.[28]

These vulnerabilities have been exploited by criminals as well as others.[29] Some recent incidents include a man who hacked into company databases doing business over the Net and stole thousands of credit card numbers. When caught, he had an encrypted CD-ROM containing roughly 100,000 stolen credit card numbers.[30] A recent survey published in the U.S. indicated that there were five serious security attacks **a month** against high visibility electronic commerce Web sites.[31] The U.S. Department of Defence reported that 80% of its sites had been penetrated: in 1996 alone, there had been 250,000 hacker attacks on Department of Defence computers.[32]

This discussion of the security risks of transmitting personal information over the Internet should not lead to the conclusion that once the Net is made secure, all privacy problems will disappear. While making the Net as secure as possible is necessary for privacy, it is not sufficient in and of itself. Security is not synonymous with privacy.

Privacy, as it relates to information, deals with the broader questions of the legitimate collection, use and disclosure of personal information, and the degree to which individuals are able to exercise control over the uses of their information. As we have seen in the previous section, businesses have an incentive to collect as much personal information as possible, to create value-added features through data matching techniques, and to sell that personal information to third parties. This raises issues about the adequacy of existing privacy protection policies on the Net and what technological solutions can be devised to protect personal information as it is exchanged in electronic commercial transactions.

Inadequate Privacy Laws, Policies and Technologies

Initially, before the Web portion of the Net was fully developed, privacy issues had not been much of a concern. But as the Web grew and matured to the point where it was increasingly viewed as a revolutionary form of communication, privacy issues began to occupy a more prominent role in its further development. The publicity surrounding the vulnerability of the technology to intrusions, criminal activities and surreptitious collections of personal information has made the public more aware of the pitfalls of this technology. There is now a growing awareness of the need to create a climate of trust and confidence in the use of this technology, particularly as this relates to commercial transactions.

A number of problems have been identified, among them, inadequate or non-existent laws and policies as to how those conducting commercial transactions will treat the personal information they collect. In North America (unlike Europe), privacy or data protection legislation does not apply to the private sector except for the Province of Quebec. Canada is committed federally, however, to introducing such legislation. Until then, Canada has encouraged self-regulation in the private sector. The Canadian Standards Association (CSA) has produced a model privacy code which various industries, particularly banking and direct marketing, have adopted and tailored to their respective industries, producing their own sectoral codes.

Debate on whether industry self-regulation or government legislation is the best approach has divided the U.S. and the EU -- the former seeking to rely on self-regulation, the latter favouring government legislation. The Europeans already have in place their data protection directive, as previously noted, which will apply indirectly to countries that import personal information from the EU. In addition, individual EU countries such as Germany have adopted laws limiting the collection of personal information over the Net. The United States, on the other hand, has resisted calls to introduce private sector privacy legislation and has lobbied strongly in favour of self-regulation.

While it is not clear how this debate will ultimately end, the early indicators suggest that there is consensus that neither the U.S. nor the Europeans will quickly pass legislation to govern the Net.[33] Self-regulation will first be given an opportunity to work (or not) before any final decisions will be made concerning government regulation.

An indication that some type of regulation may be needed is revealed in an OMB Watch survey of U.S. government Web sites. The vast majority of the sites surveyed did not have explicit privacy policies posted on their home pages.[34] Similar results were obtained with respect to the top 100 Web sites in the U.S., with only 17 having explicit privacy policies.[35] That this has also been a problem in the private sector is borne out by a recent announcement by the U.S. Information Technology Industry Council, which reported that it had prepared a voluntary code to protect privacy for those who visit its members' Web sites.[36] In Canada, the Canadian Information Processing Society has adopted a code of fair information practices based on the CSA model code, as a way to encourage its members to deal with this issue.[37]

The issue of online consumer privacy has also been taken on by the U.S. Federal Trade Commission (FTC). Over the past several years, the FTC has held hearings and produced several reports on such issues as privacy and databases, children's privacy, and the privacy practices of 'look-up services' (locator services that can identify an individual's whereabouts as well as providing other personal information). The FTC also took a 'snapshot' of assorted Web sites only to discover that very few had posted their privacy policies (if they existed to begin with). A more thorough 'sweep' of Web sites will be launched in June of 1998.

To date, solutions concerning how to ensure privacy protection with respect to electronic commerce have focussed largely on industry self-regulation. Governments have indicated that they will wait for the private sector to first formulate appropriate solutions, and then will only step in if market failure takes place. As discussed previously, Canadian and American industry sectors (those most involved directly or indirectly in electronic commerce) have begun to respond to the public outcry over privacy issues on the Net. It is expected that over the next year, there will be greater activity at the policy and procedural levels, with more and more businesses placing privacy statements and policies on their Web sites.

While there appears to be considerable flux in the development of privacy laws and policies, more aggressive efforts to solve the privacy problems associated with electronic commerce have been undertaken on the technology front. If information technology has created some of the privacy problems, then, many believe, information technology can also be deployed to solve those problems. The next section discusses these efforts.

Part Three: Privacy Solutions

> The profiling of individuals, by both public and private sector bodies, made possible by the accumulation of such [personal] data, may constitute a new threat to individual privacy, which may inhibit many potential users of the global information infrastructure from participating fully in the information society revolution. One way to deal with the problem is to avoid the collection of identifiable personal data in the first place, by allowing anonymous access to the network and anonymous consumption of the services available. This of course is not always desirable nor always possible. Additionally, innovative privacy-enhancing, user-empowering technologies are being developed. These aim at allowing users to make informed decisions about the collection, use and disclosure of personal information during interactions on the Internet.[38]

Systems analysts and software designers are increasingly seeking to find new or existing technology solutions to solve the privacy issues raised by the Net. A number of private sector information technology companies and non-profit organizations have come together to explore various approaches to dealing with the issue of privacy as it applies to transactions on the Net. These efforts can be subsumed under the term, ‘privacy enhancing technologies’ or PETs in abbreviated form.[39] PETs seek to eliminate the use of personal data from transactions or give direct control for the disclosure of personal information to the individual concerned.[40]

Privacy advocates have generally taken ‘fair information practices’ as their starting point for any discussion about personal information and data protection. Consensus has formed around the implementation of these fair information practices as enunciated in the OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. The key principles, in their strict reading, are that personal data should not be collected except for specific purposes and should be obtained by lawful and fair means, preferably with the knowledge or consent of the data subject. The purpose of the collection should be specified to the individual and the data should be used only for that purpose. Except when authorized by law or for clearly compatible purposes, the data should not be disclosed to third parties, unless the individual has consented. Personal data should be accurate, complete and up-to-date. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of the data. There should be a general policy of openness (transparency) about an organization’s practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of the data, identifying the main purpose of its use, as well as a way to contact those controlling the data. An individual should have the right to access his or her own personal data and to correct any errors. Those controlling the personal data should be accountable for complying with measures created to give effect to these principles.[41]

In the context of electronic commerce conducted over the Net, the principles that bear most directly on the protection of personal data are those dealing with collection, use and disclosure. Ideally, it is preferable that personal data not be collected in identifiable form, but if they are to be collected in that manner, fair information practices would require that only the minimum be obtained, consistent with the purpose of the collection. Individuals should be made aware that their personal information is being collected, and their consent to the collection sought. The objective of these principles is to give individuals as much control over their personal data as possible. This is particularly critical when use and disclosure are considered. It is a breach of fair information practices to use personal data in ways that are not transparent to the individual, and without his or her consent. Similarly, disclosing personal data to third parties cannot be sanctioned unless the individual has consented. While leeway in interpreting these principles is permitted in appropriate circumstances, the principles should be adhered to as closely as possible. Adherence to these principles is manageable when the aim is to regulate organizational behaviour; but such adherence poses a real challenge when one tries to embed the principles in the information technology itself. What is needed are the design correlates of fair information practices.

Personal Data as a Unit of Exchange

It was argued earlier that the collection of personal data on the Net through such things as the monitoring of clickstream information and the use of cookies made personal data a unit of exchange. When personal data are collected by these means and then sold to third parties without the knowledge or consent of the individual, a number of fair information practices are breached. The practice of registration upon accessing a Web site, while perhaps following the collection principle by asking individuals to volunteer their personal data, may breach other principles such as using the data in ways that were not expected, or having the data sold without first seeking the consent of the individual. If these uses and disclosures remain unknown to the individual, the principle of openness and transparency is also breached.

A number of initiatives are now being developed that seek to give the individual greater control over his or her personal data in the context of the Net. It should be noted, however, that these applications are not necessarily intended to replace clickstream monitoring, cookies or other similar techniques.

Labelling and Licensing Technologies

Labelling technologies license the use of symbols called *trustmarks* to online merchants through an ongoing program of certification and auditing. Auditing conducted by well-respected firms will ensure the integrity of the trustmarks and strengthen consumer confidence. It seeks to promote full disclosure of how a merchant’s Web site will use and disseminate personal data, thereby promoting consumer choice. Participating Web sites are given a licence to post a trustmark on their home page, or on individual pages that confirm that the Web site is committed to disclosing its online personal data collection and dissemination practices. By clicking on the trustmark symbol, the individual can read the Web site’s privacy statement. At a minimum, the site should reveal what type of information it collects, how the site uses that data, with whom the site shares that information, whether the individual can ‘opt out’ of having the data used by that site or a third party, whether the data can be changed or updated by the individual, and whether one can delete or deactivate oneself from the Web site database. ‘TRUSTe’ is the most widely known and respected of these technologies.[42]

Another example of such a labelling technology is WebTrust.[43] The result of the combined efforts of the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants, WebTrust involves the awarding of a seal of assurance to a Web site that has complied with WebTrust’s Criteria and Principles. These include a requirement that a Web site maintain effective controls to ensure that private customer information is protected from uses not related to its business. Audits would be conducted to ensure that a Web site’s statements were accurate.

The objective of these technologies is to provide a system of recognizing Web sites that are privacy compliant. Beyond labelling and licensing, however, an individual has no ability to negotiate or set limits on the disclosure of his or her personal data to the Web site, nor to control what that Web site may do with the data. For that, we must turn elsewhere (see P3P below).

Blocking Technologies

A technology known as PICS, or the Platform for Internet Content Selection, developed by MIT’s World Wide Web Consortium (W3C), will attach labels to describe any document on the Net or any Web site. In browsing the Web, an individual will not be able to enter those sites which he or she has set as being undesirable (for example, pornographic sites). In addition to labelling offensive material, the technology can also describe a Web site’s information practices, such as what personal information it collects and whether that information is re-used or resold.[44] PICS will not only allow the blocking out of undesirable material but also the selection of desirable material, such as Web sites that have a clearly posted privacy code. From a privacy perspective, this technology can ensure that personal data will not be released without an individual’s consent, however, it has some practical drawbacks. For example, individuals must continuously reset their privacy preferences, depending on how a particular Web site’s privacy practices have been labelled.[45]

Data Exchange Technologies

One example of this type of technology is the Open Profiling Standard, which permits users to control the release of information about themselves. Individuals enter their personal information once on their computer’s hard drive, then a set of rules is established as to how and when that information can be transmitted to online services. However, there are no rules in the standard about how a site may use that information. Essentially, what is secured is the electronic transmission of the information. The standard relies on several technologies including digital signatures and public key encryption. The profile of the individual will bear a certificate verifying one’s identity.[46] Its main drawback is that it fails to identify the privacy practices of the online service or Web site.[47]

Another project, this time developed by the W3C, is called P3P, short for Platform for Privacy Preferences.[48] P3P seeks to incorporate basic privacy principles accepted in North America, Europe and elsewhere in order to make this technology acceptable to as many countries as possible.

Once implemented, P3P would permit Web sites to state their privacy practices, based on a specified set of statements about how they would use, transfer, disclose and allow access to personal data collected by them, either from clickstream data or data provided by the user in response to a request from a Web site. The user would also create a set of privacy preferences, based on a parallel set of privacy statements about how the user's personal data may be used, transferred, disclosed and accessed. If the Web site's practices and the user's preferences matched, there would be seamless access to that Web site. However, if a match could not be achieved, the user could negotiate with the Web site (though the possibility exists that a user could be denied entry if not enough personal data was volunteered to the site). These negotiations would not be conducted directly by the user, but through a computer agent, such as a search engine. In order for the user not to have to repeatedly provide personal data to each Web site manually, one's personal data, organized into data elements, would reside in a central depository, maintained perhaps by the service provider. Missing as yet from this technology is the ability to ensure a secure transfer of the personal data from the depository to the Web site, though consideration is being given to the use of OPS technology.

The objection made by privacy advocates to the type of initiatives described above is that they require individuals to disclose their privacy preferences as a condition of a commercial transaction.[49] There is a certain apprehension that individuals will bargain away more of their privacy than may be necessary, if they think they may obtain a benefit or service in return. One must remember, however, that privacy revolves around choice -- the freedom to choose the level of privacy that one wishes and the ability to maintain control over the uses of one's personal information. Such decisions must remain in the hands of the individual.

Anonymous Profiling

An alternative approach to collecting personal data over the Net is 'anonymous profiling.' While demographic information would still be released under this scheme, personally identifying data would not. In other words, the data would not be linked to a subject or associated with a particular name.

While this approach has not received wide support in North America, it has gained greater acceptance in Europe, where Germany has specifically introduced this concept in its telecommunications legislation, which also happens to cover the Net. Service providers are required to offer customers the option of anonymous use and payment, or use and payment under a pseudonym. Moreover, individuals are protected from third parties attempting to access their personal data.[50]

Electronic Payment Systems

Over the last few years, various electronic payment systems have been devised in an effort to create confidence in buyers and sellers using the Net as a platform for commercial transactions. The lack of trust arises from the accurate public perception that providing sensitive personal and financial information over the Net may pose serious risks, especially in light of the vulnerabilities of the Net identified earlier.

From a privacy perspective, sending credit card information over the Net entails a risk that the information may be intercepted and used by someone other than the individual to whom the information was intended. Quite apart from unauthorized access to the information and loss of confidentiality, this could give rise to various forms of 'identity theft,' wherein individuals not only lose control over their personal information, but also their identities.

To resolve this problem and create trust and confidence in Net-based transactions, a variety of technologies have been devised. In the first instance, they seek to overcome the security vulnerabilities of an open network. In so doing, they also, in varying degrees, provide confidentiality in the transmitted information; they may also be privacy-enhancing to the degree that they give individuals greater control over how their personal information is collected, transmitted and used.

Encryption

Although many of these technologies and applications are still in the developmental stage, what can be said with some assurance is that there is a growing consensus that digital signatures and encryption will form the basic tools for electronic transactions.[51] Encryption is needed to ensure security including authentication, confidentiality, data integrity and non-repudiation. Several forms of electronic encryption exist, with public key encryption being strongly favoured, often in conjunction with the use of single key systems.

Digital Signatures

Digital signatures are needed to authenticate the parties to an online transaction, just as handwritten signatures affixed to paper documents authenticate the identity of the individuals involved. A word of caution, however, on relying too heavily on digital signatures as the sole means of authentication, in the absence of proper risk management techniques. "The deployment of this technology creates new kinds of risks which must be managed in order to gain possible benefits."[52] Unlike handwritten signatures, digital signatures are transferable, and that 'transferability' needs to be managed and contained.

A digital signature resembles a pseudonym more closely than a real name because it is a secret piece of information that one possesses, which is then linked to an individual's name. This leads to two central risks associated with its use: 1) initial impersonation at the time of certification of the digital signature (the risk of false attestation); and 2) the 'secret' information, namely the digital signature, being duplicated outside of the control of the bona fide individual (the risk of theft, misuse or loss).[53] In addition, for fraudulent purposes, one could have multiple digital signatures registered by different certification authorities. In order to address these concerns, a number of measures -- including the creation of certification replication lists (revoking certificates issued earlier or elsewhere) and technical standards and controls -- will become essential to the use and risk management of digital signatures.

In the search for ironclad methods of authentication for online transactions, there are also proposals, not surprisingly, to use biometric information to authenticate parties to a transaction.[54] A biometric is a unique physiological or behavioural measure that can only be associated with the individual who generated it (such as fingerprints, voiceprints, retinal scans, iris scans, hand geometry, facial thermograms, etc.) The advantage of a biometric is its unique ability to unquestionably place the identity of the individual involved. However, in order to ensure privacy, the biometric must, at an absolute minimum, be encrypted, its uses stringently controlled, and the biometric rendered incapable of functioning as a unique identifer.[55] Which technology will ultimately be accepted by the marketplace is difficult to predict at this point in time.

Turning to security, there are essentially three models for secure electronic transactions:

> Those that seek merely to provide secure transportation of transaction information from purchaser to merchant; those that attempt to facilitate the actual funds' authorization and transaction settlement process; and those that aim to reproduce the essential features of money in digital form.[56]

Secure Transmission

These applications provide secure transfer of information between a browser and a server through the use of encryption. Two competing standards exist: Secure HTTP and Secure Sockets Layer (SSL). The drawback to these technologies is that they allow the Web site to de-encrypt the transmitted information, opening the door to the possibility of fraudulent use.

Authorization and Transaction Settlement

Using public key cryptographic techniques and digital signatures, Secure Electronic Transactions (SET) protocol mimics the current credit card processing system.[57] Its advantage is that it does not permit the online merchant to read the credit card information, thereby providing the individual user with greater security.

Electronic Cash or Virtual Money

Electronic money or e-cash is predicated on a different strategy in order to be used over an open network. The strategy is to avoid sending personal data, as is the case with credit card information, but rather to send electronic cash or tokens, where an individual provides no identifiable personal data over the Net. With one form of this technology developed by David Chaum,[58] the individual remains completely anonymous. From a privacy perspective, the individual can use electronic cash just as he or she would use real cash, without having to reveal his or her identity or have any transactional data captured or linked to one's purchase. Objections have been levelled, however, from auditing and law enforcement circles against this type of anonymizing technology.

Under consideration here will be two systems: 1) hardware based 'stored-value cards' or 'smart cards' and 2) software based stored value or prepaid payment systems for executing payments over open networks. The former are hardware or card-based systems that permit individuals to use plastic cards with a magnetic strip or a smart card embedded with a computer chip; the latter are software or network-based systems that work with installed software through a personal computer connected to a network.

There are two basic ways to represent the value of the funds stored: 'balance based,' in which a single balance is stored and updated with each transaction, and 'note based,' in which electronic notes, each with a fixed value and serial number (comparable, for example, to a one-dollar bill, a five-dollar bill, etc.), are transferred from one device to another. These values are encrypted when transmitted in order to ensure confidentiality and data integrity.[59] In one instance, a note-based technology developed by DigiCash uses a 'blind signature' where the process ensures that no identifying information may be traced back to the individual.[60]

From a privacy perspective, electronic cash is the most privacy protective payment scheme since this technology permits the individual to withhold personal data from being associated with transactions, thereby eliminating the creation of transaction-generated information. In turn, the need to address privacy issues relating to the collection, use and disclosure of personal data are avoided.

Conclusions

In an era of networked information technologies, personal information has acquired intrinsic commercial value, whether collected directly or indirectly, to serve a variety of commercial purposes. However, an open networked system such as the Net remains at present an uncertain environment, particularly for the conduct of commercial transactions. Such transactions in the 'real' world are enveloped in a framework of laws, customs and practices that create the necessary trust and confidence to ensure wide public participation. In the unstructured framework of the virtual world, however, the traditional ways of conducting business are not always appropriate nor adequate. To a much greater extent, the virtual world, a creation of technology, will be dependent on technology for many of its solutions.

The challenge is to transport the basic principles that exist in the physical world through laws, customs and practices, into the virtual world -- in effect, to create a parallel process. This is the case to be made for privacy and the principles that protect our personal information in the world of e-commerce. Specifically, fair information practices provide a framework by which to assess technology-based solutions and to serve as a benchmark in creating those solutions. The combined efforts of technology experts, cryptographers, lawyers, policy-makers, privacy advocates and ultimately the public will be needed to create acceptable solutions to the privacy dilemmas arising out of a networked world.

Given the broad public apprehension about using the Net to conduct commercial transactions, and consumers' concerns over the prospect of losing their privacy, it is incumbent on all of us who wish to make electronic commerce a viable form of transacting business to inform the public about these issues. It is particularly important that the public understand the different options being considered and the choices available to them.

As we enter into the 21st century, all present indications suggest that privacy will continue to resonate as a significant public issue. The challenge will be to develop and advance information technologies, supported by appropriate legal and policy frameworks, that can minimize the public's apprehensions about technology, and, in the process, enhance personal privacy.

End Notes

1. U.S., Federal Telecommunications Commission, Staff Report, *Public Workshop on Consumer Privacy on the Global Information Infrastructure,* December 1996.

2. For the Canadian context see, Canada, Information Highway Advisory Council, *Final Report: Preparing Canada For A Digital World*, 1997.

3. Implementation of electronic commerce within the Canadian government is explored by the government's Chief Information Officer, "Interview with Paul Rummell," *Government Computer*, December 1997. For an international perspective see, OECD, *Electronic Commerce; Opportunities and Challenges for Government*, (The Sacher Report), 12 June 1997, (http://www.oecd.org/dsti/sti/it/ec/index.htm). For the U.S. position, see A Framework For Global Electronic Commerce (http://www.iitf.nist.gov/eleccomm/ecomm.htm).

4. Estimates vary as to how popular the Web has become. For recent Canadian statistics see, Geoffrey Rowan, "Internet home access almost doubles: StatsCan," *Globe and Mail*, Nov. 28, 1997; also see, IDC Executive Insights, 'Internet leapfrog: The Impact of the Internet on Global Economic Competition' (http://www.idc.com/f/Ei/gens15.htm).

5. As succinctly explained "messages can be intercepted and manipulated, the validity of documents denied, personal data can be illicitly collected." European Union, *Towards a European Framework for Digital Signatures and Encryption* (http://www.ispo.cec.be/eif/policy/97503toc.html).

6. European Union Telecommunication Commissioner, Martin Bangemann has recently called for an international charter with respect to the Internet that would deal with various issues, including privacy. See, "A New World Order for Global Communications: The Need for an International Charter" (http://www.ispo.cec.be/infosoc/promo/speech/geneva.html).

7. Other international organizations include: World Trade Organization, the International Telecommunication Union, the World Intellectual Property Organization, the World Bank Group, the International Organization for Standardization, the InterAmerican Development Bank. James A. Johnson, *Report on International Organizations*, March 1997 (http://nii.nist.gov/pubs/intl_org.html).

8. The Canadian federal government is reported to have 150 projects dealing with electronic commerce underway. Kathleen Sibley, "Show me the e-money' say Canadians cruising for easier government access," *Technology in Government* (http://www.plesman.com/archive/tig/97gtg15.htm).

9. Ontario, Management Board of Cabinet, "Information Technology as a Key Enabler for Change: An Overview of the Ontario Government Information Technology Strategy Project," Presentation, October 1997.

10. Further information on the status of the Directive and how it may be interpreted can be found at the following site: http://www.open.gov.uk/dpr/d5020en2.htm.

11. The OECD has organized several conferences and workshops on these issues. The most recent conference was held in Turku, Finland , 12–20 Nov.1997, (http://www.oecd.org/dsti/sti/it/ec/act/turku.htm). It should be noted that there are two differing views on how the Internet should be regulated with respect to privacy: The U.S. prefers self-regulation and the use of contractual relationships, while the Europeans, along with Canada, prefer to rely on self-regulation when it is in conformity with broad normative legislation. European Commission, Legal Advisory Board, Meeting on Electronic Commerce/Computer Crime, 6–7 Oct.1997, *Draft Minutes* (http://www.echo.lu/legal/en/lab/971006/minutes.html).

12. Task Force on Electronic Commerce, Industry Canada and Justice Canada, *The Protection of Personal Information: Building Canada's Information Economy and Society*. January 1998. (http://strategis.ic.gc.ca/sc_mrksv/privacy/engdoc/homepage.html).

13. European Commission, *The Need for Strengthening International Coordination*, COM(98)50, Feb.4,1998 (http://www.ispo.cec.be/eif/poli...ml#1). Interestingly, this call was supported by Bill Gates of Microsoft. Phil Jones, 'Gates Backs European calls for Internet Charter', *TechWeb News*, Feb.5,1998(http://www.techweb.com/wire/story/TWB19980205S0008).

14. European Commission, *A European Initiative in Electronic Commerce*, 1997 (http://www.cordis.lu/esprit/src/ecomcom.htm).

15. *IDC Executive Insights*, Nov. 1997, (http://www.idc.com/f/Ei/gens15.htm). Also see, Ben Elgin, 'No more Business as Usual," *ZDNet*, (http://www.zdnet.com/products/ecommerceuser/intro.html*);* John Chambers, CEO of Cisco Systems says this figure is too low and could go over $1 trillion. *International Herald Tribune*, Nov. 19, 1997 (http://www.iht.com/IHT/TECH2dex.html).

16. "The United States, probably more than any other country in the world, has made personal information a commodity," Valerie Lawton, "Experts warn about data on the Internet," *Toronto Star*, Oct. 24,1997.

17. U.S. National Telecommunications and Information Administration, *Privacy and the NII: Safeguarding Telecommunications-Related Personal Information*, October 1995, (http://www.ntia.doc.gov/ntiahome/privwhitepaper.html). For a view of how individuals are affected by this personal information economy, see Nina Bernstein, 'On the Frontier of Cyberspace; Data is Money and a Threat,' *New York Times*, June 12,1997.

18. U.S. National Telecommunications and Information Administration, see above.

19. Some have argued that this is a form of customer surveillance, see Rohan Samarajiva, "Privacy in Electronic Public Spaces: Emerging Issues," *Canadian Journal of Communication (*http://www.ccsp.sfu.ca/calj/cjc/BackIssues/19.1/samaraj/html).

20. For a discussion of the privacy implications of data warehouses see, Office of the Information and Privacy Commissioner/Ontario, *Data Mining: Staking a Claim on Your Privacy*, January 1998.

21. John Foley and Bruce Caldwell, “Dangerous Data,” *Information Week*, Sept. 30, 1996.

22. This issue is discussed in Ann Cavoukian, Ph.D. and Don Tapscott, *WHO KNOWS: Safeguarding Your Privacy in a Networked World*, McGraw-Hill: New York, 1996. pp 99-102.

23. *Globe and Mail*, 25 Nov. 1997. There have been a number of well publicized incidents in the U.S. that give credence to this conflict: reference is to Lotus Marketplace, Lexis-Nexis, and AOL companies that sought to sell their customers’ personal information, but had to retract after opposition from their customers.

24. See the polls conducted in the U.S. by Alan Westin and Louis Harris Associates, and in Canada by EKOS Research Associates, Inc.

25. The survey was conducted for Taxsoft Inc and released at the COMDEX fair in October 19, 1997, (http://real.NewsHub.com/1197/17_02.htm). Alan Westin in a recent survey found that privacy and confidentiality are major issues with Internet users. Fifty-eight per cent of those polled said they support government passing laws protecting privacy as they do not trust information gathers on the Net to properly protect their privacy. *Access Reports*, June 25, 1997.

26. Georgia Institute of Technology, College of Computing, “GVU’s 8th WWW User Survey: Executive Summary” (http://www.gvu.gatech.edu/user_surveys/survey-1997-10/#exec).

27. Michael Nash, *Future of Web Success Relies on Converging Micro-Payments Model with Privacy Technology*, Gartners Group Leaders Online, Sept. 1997, (http://www.digicash.com/news/room/art/gartners01.html). Susan Scott, Executive Director of TRUSTe has stated that “privacy is a real and growing concern among online users and their concern is greatly hindering electronic commerce. As more and more users log on to explore and browse the Internet, e-commerce stands to lose significant revenue — as much as an estimated $6 million — if consumers’ privacy concerns are not met head on.” Letter to Dr. Ann Cavoukian, Ontario Information and Privacy Commissioner, Dec. 15, 1997.

28. World Wide Web Consortium, *The World Wide Web Security FAQ* (http://www.genome.wi.mit.edu/WWW/faqs/wwwsf1.html). Also see, Arnup K. Ghosh, “Securing E-Commerce: A Systematic Approach” (http://www.ARRAYdev.com/commerce/JIBC/9704-04.htm).

29. For a comprehensive discussion in the U.S. context, see The President’s Commission on Critical Infrastructure Protection, *Report Summary* (http//www.pccip.gov/summary.html); for an assessment of the situation in Canada, see Noreen Flanagan, “Government urged to buckle up when cruising the information highway”, *Technology in Government* (http://www.plesman.com/archive/tig/97itg04b.htm).

30. Bruce Ward, “Hackers find theft at fingertips”, *Windsor Star*, Oct. 21, 1997.

31. Rutrell Yasin, “E-Commerce Sites Top Hacker Hit List”, *Internet Week* reported in TechWeb News, 20 Nov. 1997 (http://www.techweb.com/wire/news/1997/11/1120hack.html).

32. U.S., General Accounting Office, “Information Security: Computer Attacks at Department of Defense Pose Increasing Risks”, May 22, 1996 (http://www.gao.gov/AIndexFY96/abstracts/ai96084.htm).

33. “Electronic Commerce Announcement May Signal U.S.– European Cooperation”, *Privacy Times*, Dec. 12, 1997. The Clinton Administration has given the US Commerce Department until July 1,1998 to come up with a plan on how to deal with this issue. David Joachim, ‘Clinton Administration Turns UP Heat On Privacy’, *TechWeb News*, Jan.27,1998 (http://www.techweb.com/wire/story/TWB19980127S0009)

34. OMB Watch, “A Delicate Balance: The Privacy and Access Practices of Federal Government World Wide Web Sites”, Aug. 1997 (http://ombwatch.org/ombw/info/balance.html).

35. EPIC, “Surfer Beware: Personal Privacy and the Internet”, June, 1997 (http://www.epic.org/reports/surfer-beware.html).

36. U.S. Information Technology Industry Council, “The Protection of Personal Data in Electronic Commerce’, *Public Policy Document*, Nov. 20, 1997 (http://www.itic.org/iss_pol/ppdocs/pp-privprin.html).

37. Canadian Information Processing Society, “Privacy & Information Technology Paper: Implementation & Operational Guidelines” (http://www.cips.ca/papers/privacy/default.htm).

38. Ministerial Conference, Global Information Networks, 6–8 July 1997, *Theme Paper* (http://www2.echo.lu/bonn/themepaper.html).

39. Privacy enhancing technologies are explored in Office of the Information and Privacy Commissioner/Ontario and the Registratiekamer (Netherlands), *Privacy-Enhancing Technologies: The Path to Anonymity*, August 1995.

40. Herbert Burkert, “Privacy-Enhancing Technologies: Typology, Critique, Vision”, in Philip E. Agre and Marc Rotenberg (eds.), *Technology and Privacy: The New Landscape*. MIT Press, Cambridge, Mass., 1997.

41. The OECD believes that “At a minimum, Governments need to ensure broad national guidelines or modifications of existing national guidelines on privacy in accordance with the 1980 OECD Privacy Guidelines. Guidelines should be based on the principle of protecting individuals privacy without imposing unnecessary burdens on business and the community. In particular: (I) transparency must be ensured as to use of personal data; (ii) limitations, where required, should be imposed on the secondary use of personal data and (iii) rights to access and to correct one’s own personal data must be clarified, and requirements to ensure accuracy of data be set forth”, OECD, Council at Ministerial Level, *Global Information Infrastructure — Global Information Society (GII-GIS): Policy Recommendations for Action*, 26–27 May 1997.

42. TRUSTe, “About TRUSTe Privacy Program” (http://www.etrust.org/users/program.html).

43. For more information on this process, see the Web site of the Canadian Institute of Chartered Accountants. (http://www.cica.ca/new/index.htm)

44. Paul Resnick, “Filtering Information on the Internet”, *Scientific American* (http://www.sciam.com/0397issue/0397resnick.html).

45. World Wide Web Consortium (W3), “Platform for Internet Content Selection” (http://www.w3.org/PICS/).

46. Netscape, “Proposal for an Open Profiling Standard, Document version 1.0, June 2, 1997” (http://developer.netscape.com/ops/proposal.html).

47. World Wide Web Consortium, “P3P and Privacy on the Web FAQ”, Oct. 29, 1997 (http://www.w3.org/P3P/P3FAQ.html).

48. World Wide Web Consortium, P3P Vocabulary Working Group, “Grammatical Model and Data Design Model,” 14 Oct. 22, 1997, (http://www.w3.org/TR/WD-P3P-grammar.html) and P3P Architecture Working Group, “General Overview of the P3P Architecture”, Oct. 22, 1997 (http://www.w3.org/TR/WD-P3P-arch.html).

49. EPIC, “Comments of the Electronic Privacy Information Center Before the Federal Trade Commission”, April 15, 1997 (http://www.epic.org/privacy/Internet/FTC/epic_comments_497.html).

50. Datenschutz Berlin, “Federal Act Establishing the General Conditions for Information and Communications Services”, 13 June 1997 (http://www.datenschutz-berlin.de/gesetze/medien/iukdge.htm).

51. There has been some controversy over encryption technology in the U.S., where the present administration has been reluctant to endorse the export of certain long bit encryption techniques. However, most governments, even in the U.S., endorse the rapid introduction of sophisticated cryptography. See, for example, European Commission, “Ensuring Security and Trust in Electronic Communication: Towards A European Framework for Digital Signatures and Encryption” (http:// www.ispo.cec.be/eif/policy/97503toc.html).

52. Eric Hughes, Chief Technology Officer, Simple Access Corp., Symposium on Privacy-Enhancing Technologies, September 17, 1996, Ottawa, Canada.

53. *Ibid*.

54. The National Registry Inc., “NRI Announces Availability of Human Authentication Application Program Interface Specification to Promote Interchangeability of Biometric Technologies”, Dec. 5, 1997 (http://www.nrid.com/97024.html).

55. For a further discussion, see Ann Cavoukian, “Privacy and Biometrics: An Oxymoron or Time to Take a 2nd Look?”, Computers, Freedom and Privacy Conference, 18 Feb. 1998, Austin, Texas.

56. Blaise Cronin and Geoffrey McKim, “The Internet”, in UNESCO, *World Information Report*, July 24, 1997 (http://www.unesco.org/webworld/wirerpt/report.htm).

57. IBM, “Secure Electronic Transactions: Credit Card Payment on the Web in Theory and Practice”, May 16, 1997 (http://www.redbooks.ibm.com/redbooks/SG244978/setbk.htm).

58. David Chaum: “*Achieving Electronic Privacy*,” Scientific American, August 1992.

59. Bank for International Settlements, Group of Ten, Report of the working party on electronic money, *Electronic Money: Consumer protection, law enforcement, supervisory and cross border issues*, April 1997 (http://www.bis.org/publ/index/htm).

60. For a theoretical discussion of how this system works see, David Chaum, “A Cryptographic Invention Known as a Blind Signature Permits Numbers to Serve as Electronic Cash or to Replace Conventional Identification. The Author Hopes It May Return Control of Personal Information to the Individual” (http://www.eff.org/pub/Privacy/chaum_privacy_id.article), which appeared in *Scientific American*, August 1992.