Organisation de Coopération et de Développement Economiques
Organisation for Economic Co-operation and Development

OLIS : 07-Sep-1998
Dist. : 09-Sep-1998

Or. Eng.

DIRECTORATE FOR SCIENCE, TECHNOLOGY AND INDUSTRY
COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY

Cancels & replaces the same document:
distributed 27-May-1998

Group of Experts on Information Security and Privacy

IMPLEMENTING THE OECD "PRIVACY GUIDELINES" IN THE ELECTRONIC ENVIRONMENT: FOCUS ON THE INTERNET

68807

Or. Eng.

FOREWORD

This document was prepared by the Information, Computer and Communications Policy Division (ICCP) and was submitted to the Group of Experts on Information Security and Privacy at its meeting on 20-21 October 1997 for discussion and to assist that Group in taking a decision on its future work in this area during 1998. The Group recommended declassification of the document to the ICCP Committee.

In accordance with the decision of the ICCP Committee at its October 1997 meeting, the document has been declassified by written procedure after being revised in line with written comments received from Member countries.

TABLE OF CONTENTS

MAIN POINTS

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) were adopted as a Recommendation of the OECD Council on 23 September 1980. The Recommendation provides general guidance concerning the collection and management of personal information. These technologically neutral principles are still being used -- both in the public and private sectors -- and are included in a large number of national and international instruments. In this context, the Information, Computer and Communications Policy (ICCP) Committee as well as the Group of Experts on Information Security and Privacy have deemed that it is not necessary to revise the Guidelines.

In the context of the development of electronic commerce, this report outlines the concerns relating to privacy expressed by a certain number of network users, as well as the conditions for collecting data on the Internet; it presents a survey recently undertaken in the United States to measure the application of data privacy rules on the World Wide Web. The report also covers diverse initiatives undertaken by the private sector to develop privacy-enhancing technology on the global network.

On this basis, considering that consumer confidence is a key element in the development of electronic commerce, the report suggests the following action:

- to reaffirm that the Privacy Guidelines are applicable with regard to any technology used for collecting and processing data;

- for those businesses who choose to expand their activities to information and communication networks, to encourage them to adopt policies and technical solutions which will guarantee the protection of the privacy of individuals on these networks, and particularly on the Internet;

- to foster public education on issues related to protection of privacy and the use of technology.

Given its history in developing the Privacy Guidelines and its established competence in addressing issues related to the global information society, the OECD is a good place to undertake consideration of this issue. As a first step, one way to initiate this process could be through a *workshop* involving governments, industry and businesses, individual users and data protection authorities, to discuss trends, issues and policies in this area.

On the basis of the results of the *workshop*, OECD Member countries might consider the design of a framework for international co-operation in the field of privacy protection in the global information society.

IMPLEMENTING THE OECD PRIVACY GUIDELINES IN THE ELECTRONIC ENVIRONMENT: FOCUS ON THE INTERNET

I. Introduction

The general concept of privacy

The concept of "privacy" can be interpreted in a variety of ways, but for the purposes of this report "privacy protection" refers to those principles which were agreed upon in the 1980 OECD Guidelines on Protection of Privacy and Transborder Flows of Personal Data (the OECD "Privacy Guidelines"). While, in the economic context of free flows of information, these principles for privacy protection were agreed upon, there remain different concepts about the understanding of privacy. In some countries the concept of privacy is built upon the idea of a "right of personality" of an individual whereas in other countries, privacy is understood more in terms of protection against intrusion. However, regardless of any conceptual basis for understanding privacy, the fact that the basic values agreed upon in the OECD Guidelines appear in a large number of national or international instruments and are still accepted world-wide indicate that they represent the primary components for the protection of privacy and personal data, comprising a commonly understood reference point.

Background

Basic ideas about privacy protection emerged in the 1970s, dating back to the advent of the information society and the introduction of computers into various areas of economic and social life. At that time, governments had to deal with the public's growing perception that the greater need for information, and the proliferation of computerised systems, would ultimately mean a reduction in the power of individuals to control the personal information collected and stored about them. Computers were seen as a tool for processing volumes of data quickly and cheaply which concentrated enormous power in the hands of computer specialists and data processing managers. The combination of computer technology and telecommunications was already holding out the prospect of complex information and communications networks at the national and international level.

During the 1970s the Member countries of the OECD came together to promote the free flow of information across their borders and to prevent legal issues related to the protection of privacy from creating obstacles to the development of their economic and social relations. To this end, the Privacy Guidelines were adopted as a Recommendation of the OECD Council on 23 September 1980. The Recommendation represents international consensus on general guidance concerning the collection and management of personal information. The drafters of the Guidelines foresaw that technology would develop rapidly, and the principles set forth in the Guidelines were designed in a technology-neutral way to accommodate future developments.

Since then, advances in information and communication technologies have fostered the development of complex national and international networks which enable thousands of geographically dispersed users to distribute, transmit, gather and exchange all kinds of data. Transborder electronic exchanges -- private, professional, industrial and commercial -- have proliferated on a global scale and are bound to intensify among businesses, and between businesses and consumers, as electronic commerce develops. At the same time developments in digital computing have increased the capacity for accessing, gathering, recording, processing, sorting, comparing and linking alphanumeric, voice and image data.

These changes in technology do not diminish the relevance of the consensus achieved in 1980: despite technological advances and the evolution of an electronic environment based on world-wide information and communications networks, the Guidelines are still applicable today. Over the years, the principles set forth in the Guidelines have been put to use in a large number of national and international instruments and they are still widely used both in the public and private sectors. In that context, the Information, Computer and Communications Policy (ICCP) Committee and its subsidiary body, the Group of Experts on Information Security and Privacy have deemed that it is not necessary to revise the Guidelines at this time. The Guidelines are, in fact, technologically neutral and apply to all types of personal data, whether traffic data (such as date, time, or duration) or content data (for example, information contained inside an electronic message, such as personal information like name or address, information about personal preferences, or information about the kinds of transactions conducted, what was purchased at what price, etc.).

The relevant question today is not, therefore, whether it is necessary to define new principles for the protection of privacy in an expanding global electronic environment, but rather what are the appropriate means of putting these established principles into practice, particularly on the information and communication networks. To this end, it would be useful for governments to engage in a dialogue involving the private sector and individual users of networks in order to learn about their needs for implementing the Guidelines, to undertake an examination of private sector technical initiatives and to encourage the development, for application within global networks, of technological solutions that implement the principles in the Guidelines and uphold the right of users and consumers to protection of their privacy in the electronic environment.

One way to launch such a dialogue could be to organise a workshop to foster an exchange of views. Such a discussion involving governments, the private sector and consumers would enhance the work on electronic commerce being carried out within the OECD and in other organisations. Governments could draw upon the outcome of such talks to consider the design of a framework for international co-operation in the field of privacy protection in the global information society. On that occasion, they could reaffirm the principles on the protection of privacy set forth in the Privacy Guidelines, and, in the light of the development of electronic commerce, call for the adoption of pragmatic and flexible solutions that could ensure implementation of the principles.

II. Review of OECD Privacy Guidelines

The OECD was the first international organisation, in 1980, to issue an international policy for the protection of privacy in computerised data processing. By the end of the 1970s the OECD identified the common threads of the approaches adopted by individual countries, and defined certain interests and basic values commonly considered as primary components for the protection of privacy and personal data in terms of the processing of personal information.

The OECD principles identified in the Guidelines outline the rights and obligations of individuals in the context of automated processing of personal data, and the rights and obligations of those who engage in such processing. The Guidelines apply to personal data, whether in the public or private sectors, which pose a danger to privacy and individual liberties because of the manner in which it is processed, or because of its nature or the context in which it is used. Furthermore, the basic principles outlined in the Guidelines are applicable at both the national and international level.

The Guidelines outline the following basic principles of national application:

***Collection Limitation Principle**: There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.*

***Data Quality Principle**: Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.*

***Purpose Specification Principle**: The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.*

***Use Limitation Principle**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with [the Purpose Specification Principle] except:*

(a) with the consent of the data subject; or
(b) by the authority of law.

***Security Safeguards Principle**: Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.*

***Openness Principle**: There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.*

***Individual Participation Principle**: An individual should have the right:*

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

***Accountability Principle**: A data controller should be accountable for complying with measures which give effect to the principles stated above.*

The Guidelines also identify the following basic principles of international application in terms of free flow and legitimate restrictions:

Member countries should take into consideration the implications for other Member countries of domestic processing and re-export of personal data.

Member countries should take all reasonable and appropriate steps to ensure that transborder flows of personal data, including transit through a Member country, are uninterrupted and secure.

A Member country should refrain from restricting transborder flows of personal data between itself and another Member country except where the latter does not yet substantially observe these Guidelines or where the re-export of such data would circumvent its domestic privacy legislation. A Member country may also impose restrictions in respect of certain categories of personal data for which its domestic privacy legislation includes specific regulations in view of the nature of those data and for which the other Member country provides no equivalent protection.

Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.

The Guidelines call upon Member countries to implement these principles domestically by establishing legal, administrative or other procedures or institutions for the protection of privacy and personal data, in particular by:

- *adopting appropriate domestic legislation;*
- *encouraging and supporting self-regulation, whether in the form of codes of conduct or otherwise;*
- *providing for reasonable means for individuals to exercise their rights;*
- *providing for adequate sanctions and remedies in case of failures to comply with measures which implement the principles; and*
- *ensuring that there is no unfair discrimination against data subjects.*

At the international level, Member countries were called upon in the Guidelines to make known, where requested, to other Member countries the details of their observance of the principles. Furthermore, Member countries were directed to ensure that procedures for transborder flows of personal data and for the protection of privacy are simple and compatible with those of other Member countries which comply

with the Guidelines. In that context, a logical consequence of implementation of the principles in the Guidelines is the free transborder flow of information. Legitimate restrictions are possible for certain categories of so-called "sensitive" data for which other countries do not provide equivalent protection.

The principles set forth in the Guidelines are characterised by their clarity and flexibility of application, and they were formulated broadly enough to adapt to technological change. They encompass all media for the computerised processing of data on individuals (from local computers to networks with global ramifications), all sorts of personal data processing (from personnel administration to the compilation of consumer profiles) and all categories of data (from traffic data to content data, from the most mundane to the most sensitive). They are applied in many countries in both the private and public sectors.

Subsequent to the Privacy Guidelines, in 1985 the governments of the OECD Member countries adopted a declaration on transborder data flows, stressing *inter alia* their intention to seek transparency in regulations and policies affecting the international exchange of data and to develop common approaches and, when appropriate, harmonised solutions for dealing with problems arising from such flows.

III. Further developments

The growing importance of data protection

Since 1980, considerable research and a range of initiatives, at both the national and international level, have been undertaken to explore and address issues related to the collection and use of personal data: in addition to the OECD instrument, two other international instruments -- prepared by the Council of Europe and the United Nations -- were adopted in 1981 and 1990, respectively.

Thirty-four countries, including the 15 Member States of the European Union, have adopted legislation in this area, applicable, depending on the country, to the public and private sectors or to the public sector alone. Furthermore in October 1998, a European Union Directive (95/46/EC) on the protection of individuals with regard to the processing of personal data and on the free movement of such data, has to be implemented in order to harmonise data protection laws within the European Union.

In countries that do not have special legislation to protect privacy and personal data, texts which apply to specific industry sectors are nevertheless applicable as well as a number of industry-wide provisions. General principles or standards have also been established and they serve as a reference; and codes of good conduct have been adopted in many sectors of the economy.

Technological developments

In parallel, since 1980 advances in information and communication technologies have fostered the proliferation of private, professional, industrial and commercial transborder electronic exchanges on a global scale which are bound to intensify among businesses and between businesses and consumers as electronic commerce develops. The volume and nature of personal data disclosed on networks during electronic transactions have increased and the temptation to capture this data to produce value-added information on customer and prospect profiles has increased as a result. New methods for processing the vast accumulation of data -- such as data mining techniques -- make it possible, on the basis of

demographic data, credit information, details of on-line transactions ..., to identify new kinds of purchasing patterns or unusual relationships.

Despite these technological advances and the evolution of an electronic environment based on world-wide information and communications networks, the basic privacy principles are still applicable today and may be more relevant than ever. However changes in technology do prompt a move from a conceptual phase to a new practical phase, whereby the question of how to implement the principles in the electronic environment should be considered for their effective application across the world.

Indeed, compliance with rules governing the protection of privacy and personal data is crucial to establishing confidence in electronic transactions, and particularly in Europe, which has traditionally been heavily regulated in this area. The development of the global information society makes the convergence of government policies, the transparency of rules and regulations and their effective implementation on information networks a necessary condition for development of transborder activities in all sectors of economic and social life. In particular, in the context of electronic commerce, the development of on-line commercial activities hinges to a large extent not only on the faith consumers have in businesses in terms of guaranteed product delivery or security of payment systems, but also on the confidence that users and consumers will have in the ways that businesses handle their personal data.

Policy developments in the public and private sectors

To operate with confidence on the global networks, most users and consumers need assurance that the personal information concerning their on-line activities and electronic transactions will not be collected or used without their knowledge or made available to parties other than their initial correspondents, or linked to other data about them in order to compile behavioural profiles without their consent. Furthermore, users and consumers might have a reasonable expectation that businesses adopt transparent privacy policies at all points of the network.

To this end, a number of countries have undertaken to study, develop and harmonise application of the general principles of privacy protection in various ways. After the adoption by the Member States of the European Union of a general Directive on the protection of personal data in 1995, Canada prepared a Model Code for the Protection of Personal Information in 1996, and the United States for the past two years has been extensively exploring relevant issues and objectives and various ways of dealing with them. In Japan, the Ministry of International Trade and Industry (MITI) released a set of privacy guidelines in early 1997. Based on the Guidelines, industries will issue their own privacy guidelines and individual companies will set their compliance programmes by Spring 1998. MITI and the Ministry of Finance (MOF) are jointly engaged in a study envisioning legislation which includes penalties for the misuse of financial records. The Electronic Commerce Promotion Council of Japan (ECOM) independently issued privacy guidelines based on MITI's guidelines. Three hundred companies participating in the 19 electronic commerce projects should comply with the guidelines. Also ECOM will soon release a "privacy-friendly" model homepage, which will be adopted by the participating companies.

At the same time, a large number of private sector actors are trying to assess network users' demands for privacy protection and to promote, particularly on the Internet, various solutions -- in particular technologically-based solutions -- that could address consumers' concerns while still preserving business interests. Along with the debate in various countries on criteria for adequate protection with regard to transborder data flows from the European Union to third countries, it would be useful and timely for governments to acknowledge that the private sector has an important role to play in promoting harmonised, effective solutions that respect the privacy of users and consumers, specifically on open information and communication networks. While encouraging transborder data exchanges governments

should seek a balance between promotion of a free electronic market and consumers' need to operate in an environment of trust, confident that their privacy is being respected.

Commitment to pragmatic action along these lines would be consistent with the objectives set forth in May 1997 by the OECD Council at Ministerial Level [see box below]. The result, with regard to aspects involving protection of the privacy of network users, would be to enhance the work already underway at the OECD on electronic commerce, work giving rise to two high-level OECD conferences on electronic commerce in 1997 and 1998, in Finland and Canada respectively.

Box 1. **Meeting of the OECD Council at Ministerial Level**
Paris, 26-27 May 1997

The communiqué of the 1997 OECD Council at Ministerial Level expressed the explicit desire of OECD Member countries that the consequences in various areas, including the protection of privacy, of the development of the information society and electronic commerce be examined within a coherent framework of action:

"Information and communication technologies are fundamental driving forces in globalisation. The information society promises economic and social benefits for all our citizens, companies and governments. (...) Ministers noted the great potential of electronic commerce. They asked the OECD to examine carefully its implications for areas such as taxation, commercial transactions, consumer protection, privacy and security, so that these issues can be addressed within a coherent policy framework; Ministers further asked for an updated report in 1998."

IV. Focus on privacy issues on the Internet

The Internet provides a good context for consideration of privacy issues. While the Internet comprises only one element of the new information and communications networks and technologies to which the Privacy Guidelines should be applied, its open distributed nature and widespread use provide an accessible example for practical insight into real-life issues that should also be considered in the wider electronic environment.

The concern of users

The concern of a great number of Internet users is that personally revealing information about them is automatically generated, collected, stored, interconnected and put to a variety of uses, including commercial purposes. This is what has emerged from different surveys, one of which, published in March 1997[1], reveals that 70 per cent of consumers fear that the privacy of their personal data is more at risk with the Internet than with the telephone or postal services. This fear constitutes a major impediment to business on the Internet and is an obstacle to the spread of electronic commerce. It prompts 41 per cent of respondents to exit a Web site as soon as they see a registration request, and it causes 27 per cent to furnish false information (Annex 1).

In addition, according to a brief internal study carried out in July 1997 for the OECD Secretariat by the office of the Data Protection Registrar in the United Kingdom[2], complaints arising from use of the Internet within its jurisdiction have been limited in number but extremely varied. These complaints raise the following issues:

- use of electronic addresses and the right of employers to examine their employees' e-mail;
- the ease with which false information can be distributed by e-mail or made available on Web sites;
- use of the Internet to conduct fraudulent activities;
- the way in which information about individuals, and specifically their e-mail addresses, can be extracted from Internet activity and compiled into commercial marketing lists without the knowledge of the individual.

Some examples of data collection on the Internet

Data can be collected over the Internet either directly or indirectly; in other words, it can be collected either at the time of contact with a correspondent or without the knowledge of the person concerned, often automatically. The nature of the data collected varies according to the protocol used on the network, i.e. according to the type of service. In practice, different protocols are very often used in combination to augment the profitability or quality of exchanges. For example, a Web page may propose an exchange of correspondence or a transfer of documents via links with the e-mail protocol and the protocol used for transferring files, which is more powerful.

When electronic messaging is used (Simple Mail Transfer Protocol -- SMTP -- and Network News transfer protocol -- NNTP--), communication is established from one personal mailbox to another, or between a personal mailbox and a mailbox common to a number of correspondents. The information transmitted consists of the name and e-mail address, the server address and the signature file (sig.file) if created by the user of the machine. If a communication is addressed to a joint mailbox, this information is given out to an indeterminate number of correspondents, participation in a discussion group being theoretically free. As a result, any person listed on a distribution list can at the very least obtain the e-mail addresses of all other listed parties, since this information is provided automatically for purposes of communication on a given topic.

While most downloading (File Transfer Protocol -- FTP --) is done anonymously, with only the network's Internet Protocol -- IP -- address being revealed, the same cannot be said for document presentation (World Wide Web -- WWW --, Hyper Text Transfer Protocol -- HTTP --). The minimum information revealed at each step in the Web is the name of the network machine making the request and the type of browser being used. Browsers contain an identification -- ID -- file which, if configured by the user or at the user's request, stores various personal data such as the user's name or e-mail address. If a Web server requests this information, it can be automatically given out.

A Web server can also send out information which is stored by the user's navigator (so-called "cookies") and retrieved at a subsequent connection to the server. This system indicates that a visitor has been there before, but without revealing his identity: identification requires matching with other information. As a result, when linked to the ID file incorporated into the browser and transmitted to a

server, the information recorded in cookies can yield valuable user profiles. It can be noted, however, that some navigators -- to a varying and often inadequate extent -- allow use of these cookies to be blocked.

Box 2. **Categories of visitors to Web sites**
By James Pitkow, Xerox Palo Alto Research Center
(For a comprehensive version, see Annex 2)

An **unidentified visitor** is a person who visits a Web site where no information is available about the visitor. This type of visitor does not truly exist on the Web since the Internet Protocol requires at least a machine name to return the requested information.

A **session visitor** is a visitor to a Web site where an identifier is created either explicitly via cookie generation or inferred through heuristics. This is the default type of visitor on the WWW today. Several revealing pieces of information are typically available which enable the heuristic identification of users even if cookies are not used. With each request, information about the machine name from which the visitor made the request, the type of software the visitor is using to experience the Web, the operating system on which the software operates and the page viewed prior to the current request is typically known.

A **tracked visitor** is a visitor who is uniquely and reliably identifiable across multiple visits to a site. In the earlier days of the Web, the tracking of visitors was often accomplished by inserting identifiers into the URLs issued by the server and channelling all subsequent requests through a CGI script. These days, this form of identification is typically accomplished by setting the expiration of an issued cookie into the far future. Thus, each time a visitor returns to the site, the same identifier will be used.

An **identified visitor** is a tracked visitor where additional information is available. This is the most common type of visitor when persistent identifiers are employed to monitor usage. Rough estimates of the demographics of a user can be made since the entity that owns the domain from which the request was issued can be determined somewhat reliably from InterNIC's publicly accessible domain registration database. Once the entity have been established, this information can be matched against other databases that enable the construction of user profiles. **Of course, the most obvious method of collecting additional demographics of users is by asking the actual users of the site. This is routinely accomplished via online registration forms.**

Privacy practices on Web sites

Considering the technological complexity of the network and in order to determine what privacy policies and practices are actually in place, the Electronic Privacy Information Centre (EPIC) reviewed in June 1997 100 of the most frequently visited Web sites on the Internet.[3] It was interested in determining when personal information was being collected. It wanted to see if Web sites had explicit privacy policies and how good those policies were and was curious to know whether sites made it possible for individuals to view their own information collected at the site. It checked to see if users could visit a site anonymously. It also wanted to look at the use of cookies.

As a result, EPIC stressed that even though privacy is one of the top concerns among Internet users, few Web sites today actually have privacy policies or provide users with information about privacy practices. It found that 17 of the sample Web sites had explicit privacy policies and none of the top 100 Web sites met basic standards for privacy protection. To the question whether the site collects Personally Identifiable Information (PII), such as name or address (e-mail address included), directly from the user, EPIC found that many Web sites (49 of the sample) collect personal information through on-line registrations, mailing lists, surveys, user profiles, and order fulfilment requirements. To the question whether the site tells the user why personal information is being collected and how it will be used, it found that several Web sites provide reasonably good privacy notices stating that individuals using their sites cannot transmit information that violates privacy, but have no privacy policies themselves. To the question to which extent users are able to restrict the secondary use of their personal information, the EPIC found that eight of the surveyed sites provide some degree of use limitation mainly restricted to determining whether the collecting organisation will be authorised to share (or sell) the information to a third party. To the question whether Web sites make it possible for users to access the information that the site collects about them, it found only one site in its sample that currently allows users to access their own file. Finally, EPIC found that none of the sites that enable cookies tells the user that information about the user is being placed on the user's system.

In conclusion, the great disparity in knowledge of the technological workings of networks and the absence of clear information on terms for the collection and use of personal data on their users justify, from the electronic commerce standpoint, the study and promotion of the technological means necessary to ensure on-line compliance, on the Web in particular, with the basic principles of privacy protection. The success of individual-oriented commercial activities in the new electronic environment will hinge to a large extent on the climate of confidence that businesses are able to create in their relations with consumers.

V. The search for solutions

To instil confidence in users and consumers, governments and the private sector each have an important role to play. In protecting privacy, the role of governments is to reaffirm the fundamental values considered as cornerstones of concepts about the protection of privacy and personal data, and to consider establishing a framework which will encourage businesses to develop and adopt technological solutions to guarantee that these values are respected on line and which will foster public education on these issues. The role of the private sector is to adopt transparent privacy policies and to develop

technological solutions which can be widely used. Beyond theoretical considerations, consumers expect guarantees concerning their privacy and the use of their personal data at all geographic points in a network.

The role of governments

It is important for governments to reaffirm the following guiding principles for the protection of privacy and personal data and to call for their implementation whether based on formal law or self-regulation as well as for redress for individuals in the event of non-compliance:

- principle of transparency regarding the collection of personal data: implementation of this principle requires informing people when data about them are being collected directly or indirectly (in particular when on-line surveillance and tracking is performed through electronic footprints, cookies or other means);

- principle of transparency regarding the use of personal data: implementation of this principle requires allowing people to prevent receipt of electronic junk mail (spamming) and prevent the use of information about them to constitute user or consumer profiles (data-mining);

- principle of control of personal data and access to such data by the individual: implementation of this principle requires enabling people to check the accuracy of consumer data and to restrict the transfer, sale or other distribution thereof.

It would be also useful and timely for governments to acknowledge that the private sector has an important role to play in promoting harmonised, effective solutions that respect the privacy of users and consumers, specifically on open information and communication networks. In this sense, governments could launch a dialogue involving the private sector and consumers in order to examine the various technical initiatives underway to ensure the application of the privacy principles in the on-line environment (e.g. E-mail, Internet, Minitel, World Wide Web ...).

Finally, a more general issue to take into consideration to help raise consumer confidence in the electronic environment is the need for public education on privacy issues and technologies. Policies for promoting the use of information and communication networks must be directed toward developing and implementing trustworthy technologies; planning for avoiding or coping with failure of the technologies; and gaining public support and trust in the use of the technologies.

Private sector initiatives

A large number of private sector interests, in the United States in particular, are attempting, with a view to fostering electronic commerce, to promote technological solutions that will provide a practical response to consumer concerns while still preserving business interests. In other words, they are starting to explore ways and means of making privacy work in communication networks. These initiatives go in the right direction and it would be worthwhile for governments to engage in a dialogue on that basis.

As an example, Netscape, joined by Microsoft, is leading an industry initiative (40 companies) to cope with privacy issues and proposes standard software intended to enable computer users to control what personal information is obtained when they visit Internet sites and how the information is used, as well as avoid unwanted e-mail. The proposal, called the OPS -- Open Profiling Standard --, which has

been submitted to the World Wide Web Consortium -- W3 -- (see annex 3), provides the users with a way to pre-package the personal registration information Web sites may require. At the same time, OPS lets users control when and how much of their personal profiles can be passed to a third party. OPS would have users fill out profiles and preference information in a standard that could be identified by a digital certificate (that would give a guarantee from a trusted third party that a person is really who they say they are). The standardised format and brand names associated with the profile forms would be incorporated, in the case of Netscape, into the Communicator browser. According to some specialists, OPS is an addition to rather than replacement for the intrusive cookie method of tracking user information.

Another project is the new W3C Platform for Privacy Preferences (P3) Project developed by the W3C. The P3 Project is a platform on which other technological, market and regulatory solutions can interoperate and build. The P3 prototype allows Web sites to easily describe their privacy practices as well as users to set policies about the collection and use of their personal data. A flexible "negotiation" between the Web site's practices and the user's preferences, allows services to offer the preferred level of service and data protection to the user. If there is a match, access to the site is seamless; otherwise the user is notified of the difference and is offered other access options to proceed. With P3, users can download "recommended" settings established by organisations such as industry associations and consumer advocacy groups. According to some privacy specialists, P3 requires users to disclose privacy preferences when good privacy policies should provide meaningful information for users about Web site practices and not require users to disclose personal information (see Annex 4).

Techniques to provide users with more information about privacy practices are also being developed. For instance, a number of companies and service operators have a Privacy Icon which appears either when the user enters a site, or when the user starts to provide information. The icon can either lead by hyper-link to a sophisticated service providing details of the company's (service operator) data protection policies and a tick box(es) allowing the user to opt out of having his/her data used for specific purposes, or the icon can lead to a page referring the user, for example, to an address from which further details are available.

Another example is the development of services and branding techniques which intend to provide clear and meaningful designations for privacy practices such as TRUSTe, formerly eTRUST (see Annex 5). When visiting a site, the user is informed of what the site is doing with his/her data, and with whom these collected data can be shared by "trustmarks" (i.e. recognisable systems). These Trustmarks are linked to a site's data protection statement which gives to the user a detailed description of what kind of information a site gathers, what the site operator does with that information, and with whom that information is shared.

Finally, systems for implementing on-line E-mail Preference Services (EPS) or "E-mail Robinson Lists" are also under consideration (EPS allow consumers who do not wish to receive e-mails to be excluded from lists, the common database used to register opt out demands being then used to clean marketing lists). As an example, a software package is being developed in the USA which would allow consumers to register on-line ; would be secure from intruders, and yet user-friendly for industry to clean their E-mail marketing lists; and which could be serviced easily by the operator (the Direct Marketing Association (DMA-US)). A similar system will be developed in the United Kingdom, and it is planned that these two countries would then spear-head a Global Convention on EPS inviting other DMAs to join. Another proposal, which has yet to be fully considered by industry, comes from the UK data protection Registrar, which has suggested a mechanism enabling the consumers to indicate if they do not wish to be contacted by e-mail in their e-mail address. A universally agreed character (a marker) would indicate that

the user does not want to receive any marketing solicitations. The user would also be free to make different choices : i.e. to use the marker when visiting one site and not to use it when visiting another. This system could be combined with others, such as the proposed E-mail Preference Service.

VI. Future work and the role of the OECD

General conclusions

The relevant question today is not whether it is necessary to define new principles for the protection of privacy in an expanding global electronic environment, but rather what are the appropriate means of putting these established principles into practice on the information and communication networks. There is a need to reaffirm the principles on protection of privacy and personal data; to encourage the adoption of practices in the electronic world which address both business interests to develop electronic commerce and the concerns of individual users to enjoy protection of their privacy and to foster public education on these issues.

It would be useful for governments to engage in a dialogue with the private sector in order to learn about business needs and proposals for implementing the Guidelines in the context of global networks and to encourage the development, in particular on the Internet, of technological solutions that implement the principles in the Guidelines and uphold the right of users and consumers to protection of their privacy. The initiatives outlined above, possibly together with others, should be examined so that an international policy for the development of electronic commerce may be accompanied by a full understanding of the possibilities for technological solutions for privacy protection tailored to the particularities of information and communications networks.

The following could be considered:

- means of ensuring transparency regarding the collection of personal data on the Internet so that privacy practices would state clearly how and when personal information is collected and the use and content of cookies would be more transparent;

- means of ensuring transparency regarding the use of personal data on the Internet so that users and consumers would be informed of the purposes for which the processed data are to be used;

- means of allowing control of personal data by the individual so that users and consumers would be able to oppose the use of their e-mail addresses and other personal data; and

- means of guaranteeing the right of an individual to access and amend personal data;

- finally, means of implementing the above-mentioned principles, whether based on formal law or self-regulation.

The OECD role

Given its history in developing the Privacy Guidelines and its established competence in addressing issues related to the global information society, the OECD is an appropriate place in which to

undertake consideration of this issue. In the context of the development of electronic commerce, the OECD can best make its experience available to its Member countries by reaffirming the principles of the Privacy Guidelines and encouraging the adoption of pragmatic and flexible technological solutions to address the needs of users and consumers for privacy protection on open or closed information and communication networks, while at the same time fostering the further development of electronic commerce.

The OECD could make a contribution in this area by launching a dialogue involving the private sector and consumers to consider technological solutions for implementing the Privacy Guidelines on global networks and particularly on the Internet. One way to initiate this process could be through the organisation in early 1998 of a workshop to discuss trends, issues, policies and technological developments in this area. The outcome of such a *workshop* could enhance the OECD's work in the realm of electronic commerce. Governments could then consider the design of a framework for international co-operation in the field of privacy protection in the global information society. This framework could also be adopted in non-Member countries.

NOTES

1. eTRUST Internet Privacy Study conducted by the Boston Consulting Group.
2. The Registrar is responsible for application of the 1984 Data Protection Act.
3. Electronic Privacy Information Center, Washington, DC, http://www.epic.org/

ANNEXES

ANNEX 1

EXTRACTS

1. From PRIVACY JOURNAL, June 1997, Vol.23, No.8

Louis Harris & Associates released a survey of computer users June 11 showing that 25 percent of them would be using the Internet if assured that their privacy would be protected. Another 25 percent say they are likely to begin using the Internet within a year. “The factor most likely to influence whether the non-users join the on-line world is privacy protection” Alan F. Westin, the survey’s author, told the FTC. Fifty-three percent of all Internet users are concerned about confidentiality, although fewer than one in ten have experienced an invasion of privacy on-line. Seven out of ten at some time have declined to give personal information at World Wide Web sites. (Poll results available from Privacy and American Business, 201/996-1154).

2. From : http://www.truste.org/news/article003.html

SURVEY REVEALS CONSUMER FEAR OF PRIVACY INFRINGEMENT INHIBITS GROWTH OF ELECTRONIC COMMERCE

Palo Alto, CA, March 24, 1997--A consumer study completed this month reveals that privacy of personal information on the Internet is a consistent, significant concern for consumers--greatly limiting their commercial Internet activity and impeding growth of electronic commerce. According to the eTRUST Internet Privacy Study, conducted by the Boston Consulting Group, over 70 percent of the 9,300 consumers who responded to an online survey are more concerned about privacy on the Internet than they are about information transmitted by traditional media such as phone and mail.

The survey also indicates that consumers' mistrust often leads them to either refuse to provide information on the Internet or to give inaccurate information: Over 41 percent of respondents report leaving Web sites when asked to provide registration information on the Internet. In addition to the above, another 27 percent of respondents provide false personal information on Web site registration forms.

“The study reveals that almost three in five consumers do not trust Web merchants with their personal information," said Lori Fena, executive director of the Electronic Frontier Foundation (EFF). "They need assurance that this information will be treated responsibly. Internet companies can provide this assurance by telling consumers exactly how and with whom their information will be shared."

The survey data also indicates that disclosure practices would raise consumers' comfort level in providing information. According to the survey, consumers are about twice as willing to divulge sensitive personal and financial information to companies that disclose their information gathering and dissemination policies than to companies with no posted privacy policy.

Fear of privacy infringement hinders electronic commerce

Based on the survey results, the Boston Consulting Group estimates that as much as $6 billion in additional electronic commerce could be gained by the year 2000 if consumers' privacy issues were addressed. This projection is based on increases in the proportion of Internet users who are willing to make retail purchases online.

"Web merchants, Web advertisers, data warehouses and data miners are just some of the Internet industries that would benefit from their increased trust," said Andy Blackburn of The Boston Consulting Group. Even if only 10 percent of online retail sites adopt eTRUST, the higher number of transactions alone could add another quarter of a billion dollars to electronic commerce in the next year. This revenue would shift disproportionately to retailers with assurance."

"The other side of the coin is, if infringements of consumer privacy on the Internet continue to proliferate, the industry will undoubtedly face the threat of government regulation," said Susan Scott, executive director of eTRUST. "The solution to the problem of consumer trust is informed consent -- telling the consumer how their information will be used, and obtaining their consent before using it. (...)."

ANNEX 2

Terminology (according to James Pitkow, Xerox Palo Alto Research Center) : Visitors to Web sites can be separated into the following categories : unidentified, session, tracked and identified (Novak and Hoffman 1996).

A **unidentified visitor** is a person who visits a Web site where no information is available about the visitor. This type of visitor does not truly exist on the Web since the Internet Protocol requires at least a machine name to return the requested information. This form of return address reveals information about the users in a similar manner to that of a phone number, where a one-to-one or a many-to-one correspondence may exist between the address and the number of users at the address. Unidentified visitors may indeed exist in other interactive digital systems, where a user's anonymity is explicitly preserved. It is arguable that anonymous proxies, programs that act as an intermediary between clients and servers, enable users to experience the Web in an anonymous manner. While this form of server may exist to a limited number of users, it does not scale well to handle the entire user population since it effectively doubles the amount of traffic required to request a page (by first sending a request to the anonymous server which then sends a second request to the actual server) and requires a fair amount of centralisation of resources, another potential bottleneck.

A **session visitor** is a visitor to a Web site where an identifier is created either explicitly via cookie generation or inferred through heuristics. This is the default type of visitor on the WWW today. Several revealing pieces of information are typically available which enable the heuristic identification of users even if cookies are not used. With each request, information about the machine name from which the visitor made the request, the type of software the visitor is using to experience the Web, the operating system on which the software operates and the page viewed prior to the current request is typically known.

The latter piece of information is called the referrer field. While this ancillary information may enable a user to be identified within a session, it is not guaranteed to be accurate nor will it be able to reliably identify the same user in future sessions.

Some heuristics for identifying users without cookies include:

The use of Internet protocols to help determine if the user is the sole user of the machine making the request, e.g. identity, finger, etc. If a one-to-one correspondence exists between a visitor and a machine, the machine essentially becomes a unique identifier, and the visitor becomes a 'tracked visitor' as described below. These techniques fail if a visitor exists behind a proxy, shares machines with other users, or the machine being used to experience the Web does not support or allow these protocols.

To uniquely identify users suspected of existing behind proxies, session limits, the site's topology (the global hyperlink structure across pages), and browser characteristics can be used. One such algorithm implemented in [Pirolli, Pitkow, and Rao 1996] checks that each incoming request is reachable from the set of already visited pages. This is done by consulting the site's topology. If all subsequent requests are made to pages that the visitor could have reached by selecting a hyperlink embedded in any of the already requested pages, the user is assumed to be the sole visitor behind the site. If requests from the same machine name occur for pages that are not reachable from the set of hyperlinks embedded in the pages already visited, multiple visitors are suspected. Multiple visitors are also suspected when pages are requested that have already been visited. The algorithm treats these cases as separate visitors and adds subsequent page to each visitor's path based upon the topology of the site. A least recently used policy is used to add pages to visitors if ambiguity exists between which user could have made the request. Visitors who do not request pages within a certain time limit are assumed to have left the site. Appropriate time-

out periods are typically determined by inspection of the distribution of time between all page requests to a site. While the above algorithm performs reasonably well, it is heuristic in nature and has not been shown to reliably identify users with any measure of accuracy, especially across sessions.

A **tracked visitor** is a visitor who is uniquely and reliably identifiable across multiple visits to a site. In the earlier days of the Web, the tracking of visitors was often accomplished by inserting identifiers into the URLs issued by the server and channelling all subsequent requests through a CGI script. Not only was this method expensive computationally to the sever, but it defeated intermediary caching and did not correctly handle the exchanging of URLs between people, i.e. the person using a URL of this sort mailed to them by a friend could be incorrectly tracked as the friend. These days, this form of identification is typically accomplished by setting the expiration of an issued cookie into the far future. Thus, each time a visitor returns to the site, the same identifier will be used.

The increased use of this technique to track users has not been without notice by the user community, where rather rudimentary but effective practices have emerged that periodically erase cookies stored on the visitor's file system or do not permit the storing of cookies between sessions by disabling write permissions to the appropriate files. These practices have the effect of causing the site issuing the cookie to issue another identifier, resulting in potential over-inflation of the number of unique visitors to the site. Commercial software that performs cookie obfuscation is also emerging, e.g. PGPCookie.Cutter [PGP; 1996].

An **identified visitor** is a tracked visitor where additional information is available. This is the most common type of visitor when persistent identifiers are employed to monitor usage. While it may appear that tracked visitors would be more common, additional information as mentioned in the above section of session visitors accompanies each request. Rough estimates of the demographics of a user can be made since the entity that owns the domain from which the request was issued can be determined somewhat reliably from InterNIC's publicly accessible domain registration database. Once the entity have been established, this information can be matched against other databases that enable the construction of user profiles. For example, if a request comes from a visitor behind a corporate proxy named xyz.com, via InterNIC's database, one can discover that the actual company that owns that domain is FooBar Corp., and then lookup information on FooBar Corp. in other sources. Many of the commercially available log file analysis programs come with databases that match domain names to core demographics, e.g. Interse [Interse 1996].

Of course, the most obvious method of collecting additional demographics of users is by asking the actual users of the site. This is routinely accomplished via online registration forms. However, GVU's most recent WWW User Survey data show that 33 per cent of the over 14 500 respondents have falsified the information for online registration forms at least once [Pitkow and Kehoe 1996]. Over 10 per cent reported that they provided incorrect information over 25 per cent of the time. Although online registration is currently common practice and will remain so for the foreseeable future, the information collected from online registration systems needs to be thoroughly examined on a per-site basis before reliable statements about the users of a site can be made from this information.

Other methods for collecting demographics of users at a site include Universal Registration Systems, e.g. I/PRO's I/COUNT [I/PRO 1996]. These systems require a user to register only once in exchange for an identifier. This identifier can then be used across the set of participating sites. While the goal is to 1) make registration easier for users and 2) provide sites with valuable demographic information, scalability issues have hindered the development of most of these types of systems, and as such, few Universal Registration Systems exist in practice today.

ANNEX 3

The submission by Microsoft to the W3C on 2 June 1997 (Privacy and Profiling on the Web) can be seen at : http://www.w3.org/TR/NOTE-Web-privacy.html

The complete submission by Netscape to the W3C on 2 June 1997 (Proposal for an Open Profiling Standard) can be seen at : http://www.w3.org/TR/NOTE-OPS-FrameWork.html

EXTRACT

Abstract

This specification proposes a means for the exchange of profile information. For the purposes of OPS, we define profile information as any feature and corresponding values of an end user or service provider. The specification provides for the trusted communication (mediated by computer software and communication systems) 1) between people and services, 2) between services mediated by people, and 3) between people.

A profile exchange is the informed, secure exchange of profile information between two parties. Thus, this specification discusses the control of profile information flow by both the creator and the recipient of the information, as well as third parties acting of behalf of either party. OPS also creates a framework for disclosure of intended usage of the information. This framework forms a basis for the further protection of privacy and usage through legal and social contracts and agreements as well as associated business processes.

This document is the first in a series of OPS related specifications. This document covers the framework for profile exchange, including data structure and operational primitives. (...)

1. Introduction

As more and more users, and more and more services come to the Internet, users are finding themselves increasingly overwhelmed with the richness of new possibilities, and new service providers are discovering that rapidly building systems to fit these users' information needs becomes ever more challenging.

In general, a solution to these problems often involves delivery of highly customised and personalised information to end users, which raises the profound and valid concern about making and keeping explicit commitments to users about how their most sensitive personal information, choices, preferences, and interest will be protected in these exchanges.

Companies and service organisations worldwide want to take advantage of the 1-to-1 nature of communications on the Internet or within intranets to provide their customers, employees and visitors with individualised information, entertainment and services. However, there are two barriers to the feasibility and widespread adoption of such products and services:

1) **The potential threat to individual privacy makes end users wary of sharing any information**. Today, there are few measures or safeguards which offer an end user any awareness of or any control over the usage of his or her personal information. This concern often outweighs the incentive of a personalised service and makes a person justifiably cautious about revealing any personal information.

2) **Gathering the information that makes this personalisation possible is inefficient**. Service providers need to ask their visitors for information -- who they are, where they live, what they do, what they like -- in order to personalise the user experience. This data collection can be very time consuming for both the service provider and the end user, and can't be leveraged for their mutual benefit. Furthermore, a single individual might provide much the same information to dozens or even hundreds of parties over time - an inefficient and frustrating experience.

The Open Profiling Standard (or OPS) is a proposed standard for exchanging profile information between individuals and service-providing parties, with built-in safeguards for individual privacy.

OPS gives individuals the ability to enter the information once, and to give specific rules about how and when that information can be exchanged with services. This saves the user time, and gives service providers access to better information about their customers, allowing them to offer a better service and to understand their customer base. Furthermore, OPS greatly enhances personal privacy by giving the end user the ability to 1) control the release of their information and 2) track the exchange and usage of their personal profile.

1.1 Guiding Principles

The design of the Open Profiling Standard is motivated by three core guiding principles for the exchange of profile information. These principles are intended to protect the interests of end users and any party whose potentially sensitive and proprietary data is being exchanged. OPS is the technical framework that drives towards the goals, we envision two other key components: a policy/business practice and a growing social practice.

The core guiding principles are:

-- Control by Source

-- Informed Consent

-- Value Exchange

- Control by Source

Access to information is controlled by its source. The parties responsible for creation of any information should rightfully control permission for its dissemination. These parties minimally include the end user and the entity gathering the profile data. If the end user creates profile information, then the user has sole control over permissions for dissemination.

- Informed Consent

A party requesting an end user's profile must receive the informed consent of the source(s) before collecting and using their information in any manner. The individual must be given complete information as to how their data will be used, and with that knowledge, has the option of consenting to its usage and/or exchange. The communication of the consent may be entrusted to a third party or an automated process or system. Furthermore, as much as possible, the enforceability and verifiability of each profile exchange should be enabled by this process or system.

- Appropriate Value Exchange

No party should collect information without offering the individual value in exchange. Adherence to this principle assures that an individual's profile is not freely taken with no benefit for the user. Additionally, offering value to the individual provides an incentive for the user to provide valid and truthful information. For example, if a person's locale is requested in order to provide appropriate local news, it is in the user's best interest to provide their true information. Finally, the information requested should be appropriate to the application – in the case of local news, requesting a user's hair colour, for example, lacks relevance; in an online shopping application, on the other hand, fulfilling a user's order for an audio CD clearly requires knowing a "ship-to" address for the order in question.

1.2 Related Work (...)

1.3 Definition of Terms (...)

1.4 Parties in an Exchange

There are a number of parties potentially involved in a profile exchange:

- **End users**: The individuals managing their personal profile.
- **User agents**: Client software which manages the end user profile and its interaction with profile readers and writers. The user agent can abstract much of the underlying complexity within OPS in order to simplify user management of their profile.
- **Service Providers**: Profile readers or writers. Web sites which offer personalised news, stock quotes, or the ability to communicate with other users are examples of service providers.
- **Profile readers**: The party asking to gain access to a portion of the end user profile in exchange for some service.
- **Profile writers**: The party which adds or updates information within an end user profile.
- **Section authority**: A profile writer which has qualified rights to control access to information within that section (fully explained in Section 3.1, "Naming and Authority"). In OPS the profile naming convention encodes the section authority.

- **Access providers**: The party physically supplying network access and/or hosting to end users, profile readers and profile writers. Within the context of this protocol, the role of the access provider revolves around the security of the information being exchanged.

- **Certificate authorities**: Third parties who certify the identity of an end user, profile reader, or profile writer.

- **Auditors**: Third parties which verify the practices of a profile reader or profile writer and grant them the appropriate credentials. (...)

1.5 Symbols (...)

2. Overview

Profile data is the record of the end user's features. It consists of a hierarchical set of named attributes. (...)

The communication encoding of profile data is specified by this document, along with mechanisms for alternate encodings. The representation of this data at the endpoints (end user system and profile reader system) is not restricted or specified by this document.

This specification describes two types of operations that can be performed: profile read and profile write. (...)

An important part of secure and trusted exchange of profile data is a robust permissions model. The OPS framework requires that applications implement permissions to control profile read and write operations. The "Standard Practices" document describes the required minimum permission capabilities and their implications in detail.

In reading this document, the key point is that a permission set must be established for both read and write operations, and that both the end user and the service provider shall have an equal role in controlling the exchange of profile data. That is to say, if the service provider's read permissions are not satisfied for a given exchange, the exchange will not occur; if the end user's read permissions are not satisfied for a given exchange, the exchange will not occur.

3. Profile Data

3.1 Naming and Authority

An end-user's profile data is organised as a hierarchical collection of attribute-value pairs. (...)

3.2 Communication Encoding (...)

4. Security Foundations

The risks associated with the abuse of user's privacy advocate a diligent use of leading security technologies, most prominent of which are public key cryptography, digital certificates, and public certification services. (...) The approach to security in OPS is therefore to allow the end users and services to choose the level of security appropriate for transactions . (...)

4.1 Identity

In any exchange, the first step is to determine, with appropriate assurance, the identity of all parties. OPS does not specify a standard means for services to identify users, as many protocols and practices exist for that purpose. OPS specifies a means for end users to reliably verify the identity and practices of services, using existing certificate methods and protocols. Furthermore, OPS specifies a way, built on the domain naming system, to enable non-reliable service provider identification for insecure profile exchange. (...)

4.2 Credentials

At least two parties are involved in every profile exchange, the end user and the reader/writer. Often, however, a trusted third-party will audit or verify that a profile reader/writer abides by the policies they describe. (...)

5. Profile Operations

5.1 Profile Read

When a profile reader wishes to access an end user profile, it must present a profile request object which outlines:

1) The reader's identity

2) The profile information requested of the end user

3) The intended usage codes for each section of the profile, in machine readable form

4) The fallback mode for each section of the profile, in machine readable form

5) The reader's credentials

6) The terms of exchange, in human readable form (...)

5.2 Profile Write

A profile write operation is a request from a service provider to store a profile element in the end user profile. A profile writer must provide proof of identity, third-party certifications, the desired property write operations, and Directives specifying the intended accessibility of the data (i.e. service provider permissions). (...)

6. Security Considerations

OPS attempts to insure that profile information is securely communicated and managed. (...)

6.1 End-user Security

Privacy of Information on Workstation. (...)

Privacy of Information when in transit to a Service Provider. (...)

6.2 Service Provider Assurance (...)

6.3 Import and Export of Certificates from vCard (...)

6.4 Certificate Revocation (...)

6.5 OPS Compliance (...)

7. Acknowledgements (...)

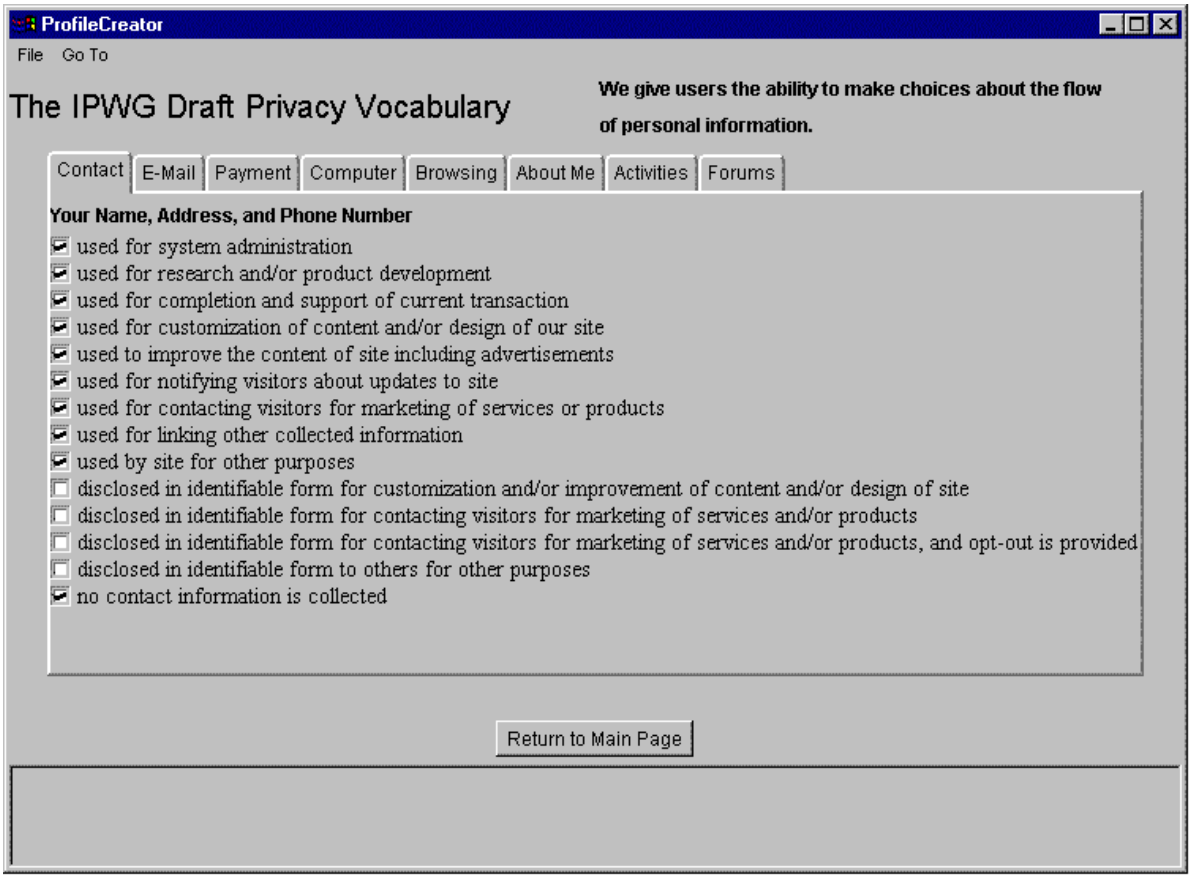
ANNEX 4

Script of W3C P3 Prototype (FTC Comment)

0. Platform for Privacy Preferences

The W3C's Platform for Privacy Preferences, often referred to as P3, addresses some of the key technical aspects of Web privacy concerns. P3 will allow sites to easily describe their privacy practices and allow users to set preferences about the release and use of their data. We call the description of privacy practices or preferences a "privacy assertion" or "privacy policy." Between the site's practices and the user's preferences, a flexible "negotiation" allows services to offer the preferred level of service and data protection to the user. Consequently, P3 promotes user confidence on the Web by enabling the fair information practice principles of "notice" and "choice." This presentation briefly describes the salient characteristics of a P3 prototype using a preliminary privacy "language" developed by the Internet Privacy Working Group.

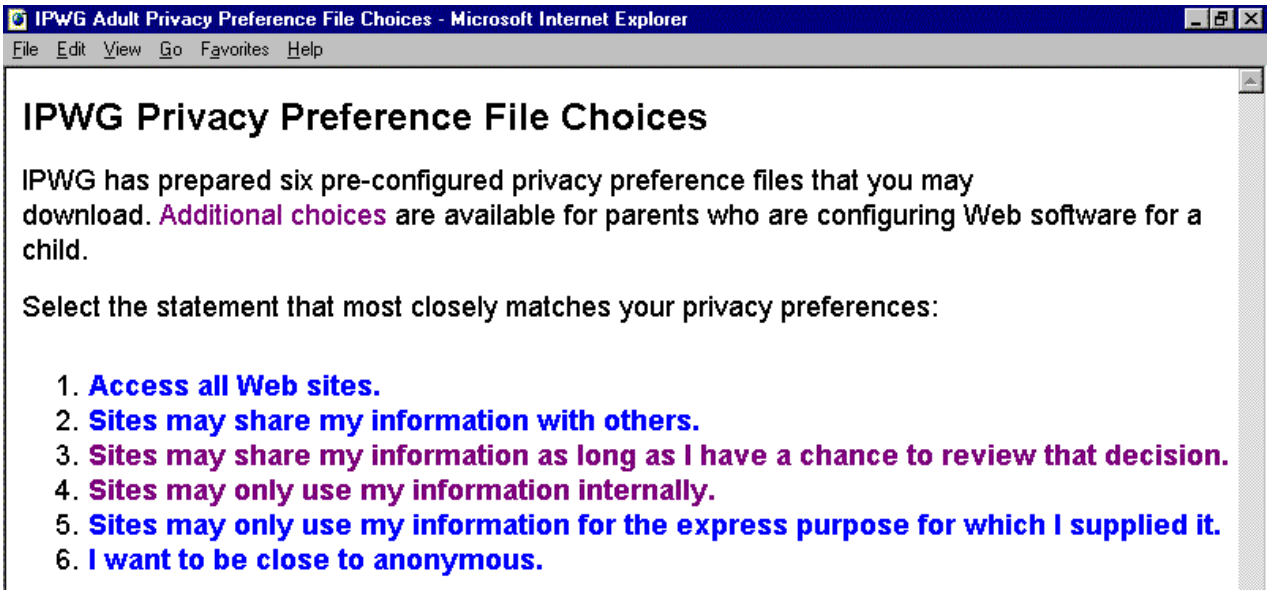
1. User is shown interface



We see a prototype of what a user sees (a user interface) when configuring P3. It is actually generated from an underlying syntax and vocabulary from which the computer can automatically describe and read privacy policies. Having the computer be able to understand the privacy policies is crucial since the computer can then act on behalf of its user to seamlessly access sites which fall within the user's preferences, or notify the user if a sites practices do not meet their preferences.

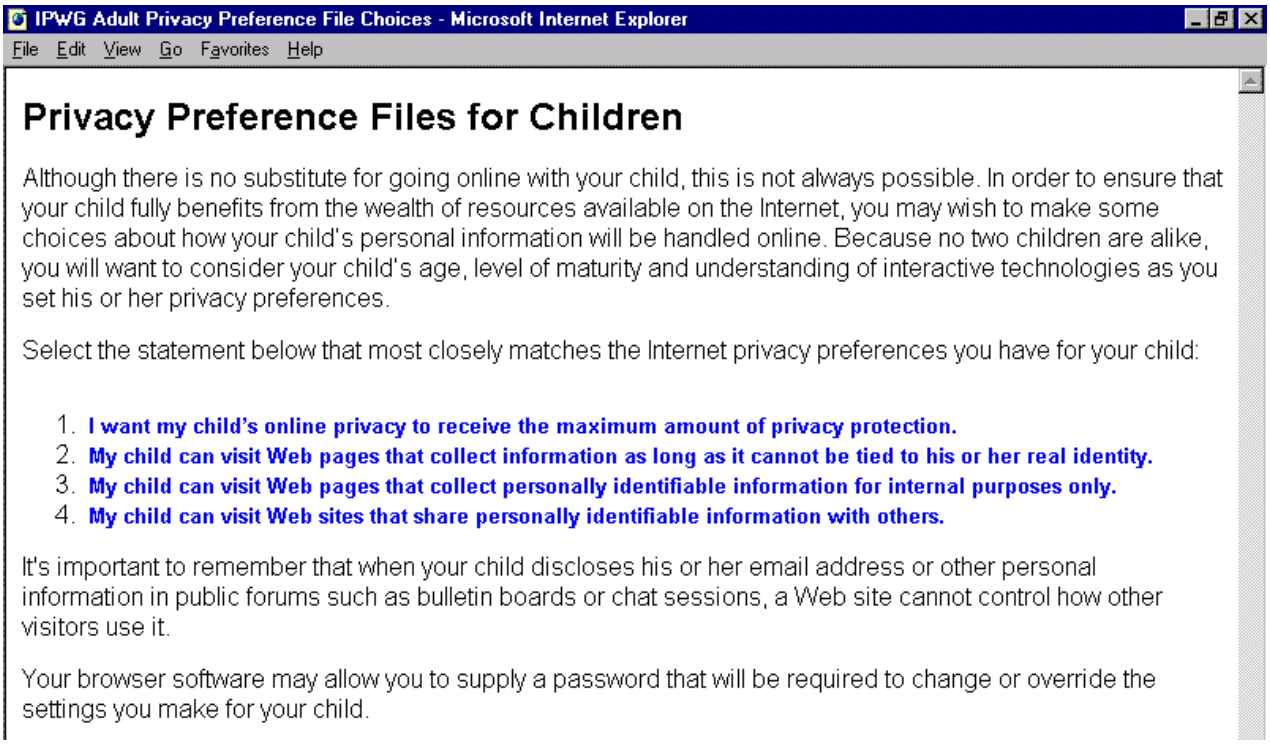
Configuring all of these options may be time consuming to a beginning user. A number of steps can be taken to simplify the setting of preferences. Organisations can offer individuals "recommended" or "automated" settings that they feel represent advisable settings for a typical adult or child browsing the Web.

2 User is shown a Web page with recommended settings



To grab one of these settings, a user can go to a Web page that they feel is reputable and offers "recommended settings." Anyone, including organisations like browser developers, Internet service providers, trade organisations, governments, or privacy advocates can provide settings to users.

Users may also be able to download recommended settings for their children:

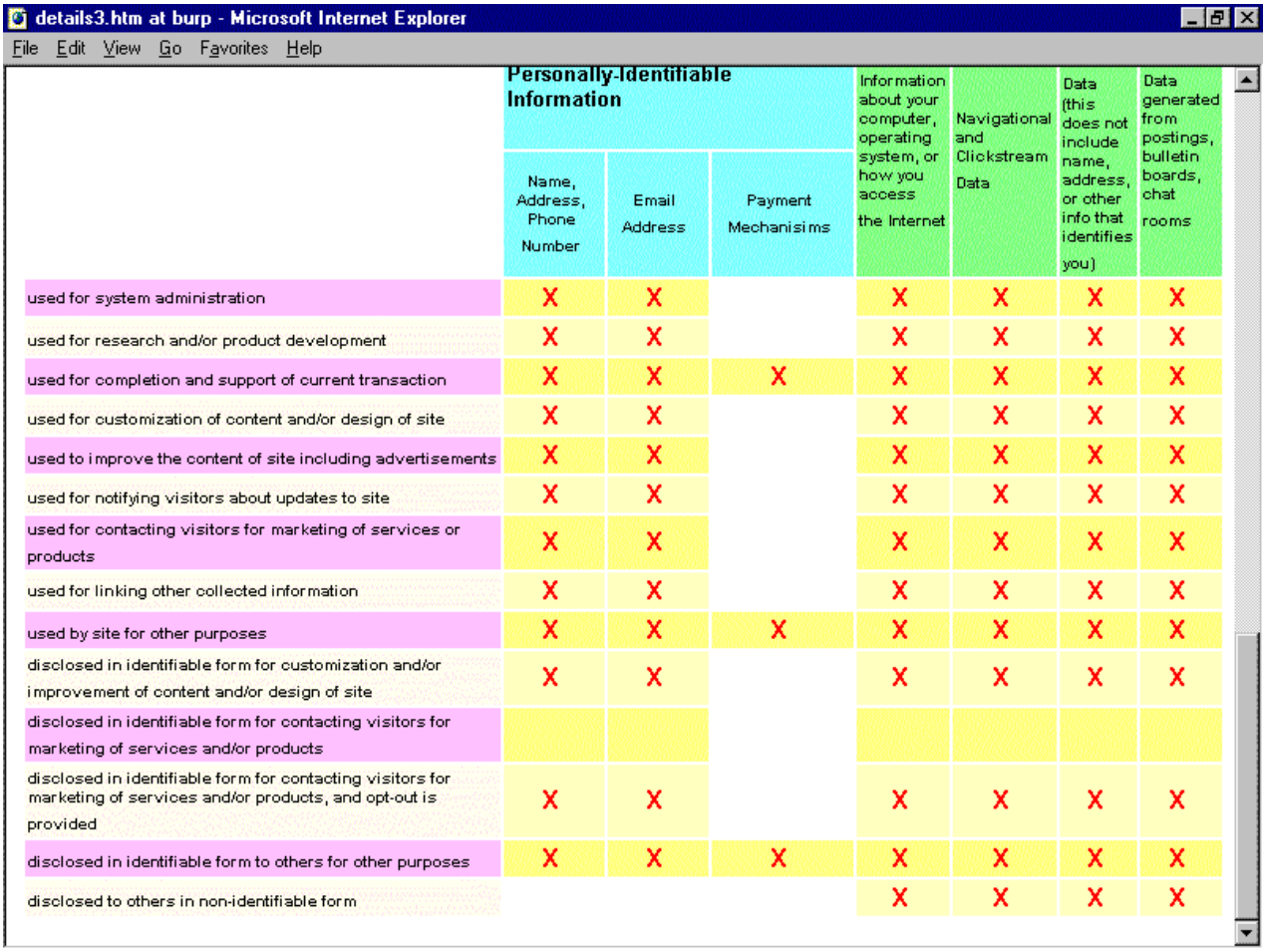


Upon arriving at the site, the user browses for the most appropriate settings.

2.1 User examines the on line "recommended setting" descriptions

Seeing a description of interest, the user can click on the description and see a fuller explanation as well as the specific settings.

2.2 User examines the full descriptions



	Personally-Identifiable Information			Information about your computer, operating system, or how you access the Internet	Navigational and Clickstream Data	Data (this does not include name, address, or other info that identifies you)	Data generated from postings, bulletin boards, chat rooms
	Name, Address, Phone Number	Email Address	Payment Mechanisims				
used for system administration	X	X		X	X	X	X
used for research and/or product development	X	X		X	X	X	X
used for completion and support of current transaction	X	X	X	X	X	X	X
used for customization of content and/or design of site	X	X		X	X	X	X
used to improve the content of site including advertisements	X	X		X	X	X	X
used for notifying visitors about updates to site	X	X		X	X	X	X
used for contacting visitors for marketing of services or products	X	X		X	X	X	X
used for linking other collected information	X	X		X	X	X	X
used by site for other purposes	X	X	X	X	X	X	X
disclosed in identifiable form for customization and/or improvement of content and/or design of site	X	X		X	X	X	X
disclosed in identifiable form for contacting visitors for marketing of services and/or products							
disclosed in identifiable form for contacting visitors for marketing of services and/or products, and opt-out is provided	X	X		X	X	X	X
disclosed in identifiable form to others for other purposes	X	X	X	X	X	X	X
disclosed to others in non-identifiable form				X	X	X	X

If the user finds a recommended setting they like, they download it to their computer for their own personal use.

2.3 User downloads the "OK to share with third parties" recommended setting to disk

3 User is shown profile editor interface, user selects IPWG and saves profile

Once the recommended setting is in place, the user can always change it or tune it to his or her specific preferences as the user becomes more experienced. Afterwards, the user is ready to browse the Web.

4 User sees a "P3 Demo Home" page with a link to the Princeton Review www.review.com

In this example, the user goes to a site that has privacy practices that fall within the scope of their preferences. For most of this page this may include the collection of clickstream data for system administration purposes.

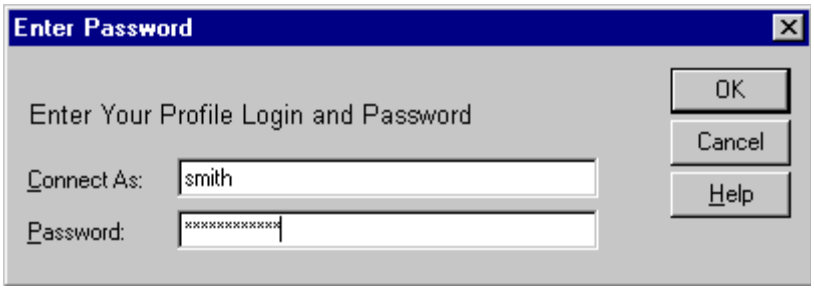
4.1 User navigates two links on the site (top go to college banner).

Nothing out of the ordinary occurs! This is because there was a direct match between the user's preferences and the site's practices, hence we had a direct match and seamless interaction.

4.2 When the user hits the last go to college button, she is shown the redirect for consent page

In this case, the site is asking for more information than the user allows for. Hence we have a "mediated interaction." The site can choose to not admit the user since it cannot comply with the user's preferences, it may inform the user of its practices and ask the user to consent to them, or it may be willing to be responsive to the user's specific preferences. The option to turn this capability to "over-ride" or "consent" may be disabled for child profiles.

4.3 Clicks consent page, and we can see that information is solicited by a form.



5 Return to user interface

This demonstration has been a very simple display of how the Platform for Privacy Preferences may be realised. It is important to note that users have a great deal of control and choice in which practices are accepted. And that sites can offer multiple practices depending on what service the user wants. For instance, a customised news service requires the collection of more information than a simple Web page. Also, client technologies (like browsers) are developing to allow family members to set up their own preferences and that parents could set password-protected preferences for their children.

In this demonstration we do not fully represent the benefits trusted third parties can play in the P3 scheme. They can offer recommended privacy settings, their own opinion of a site's practices, or auditing services and icon programs to increase the confidence users place in P3 assertions. Privacy assertions made using P3 are only a piece of the puzzle but an important one. P3 is a platform on which other technologies can interoperate and a bridge to social and market concerns about user privacy on the Web. P3 is a platform on which technical, market and social solutions for protecting privacy on the World Wide Web can be built.

ANNEX 5

EXTRACT of a Press Release

TRUSTe, Formerly eTRUST, Launches Commercial Availability

Global Consumer Privacy Initiative Backed Tandem Computers, Oracle, Lands' End, Excite, AT&T, Netscape, IBM, Cybercash, VeriSign, Wired Ventures, Progressive Networks, Coopers & Lybrand, KPMG, NCSA, MatchLogic and InterNex, Palo Alto, CA, June 10, 1997 --

TRUSTe, the global initiative for establishing consumer trust and confidence in electronic commerce, formerly eTRUST, today announced that the program is available for commercial use and that it is being backed by several leading companies. TRUSTe assures online consumers' privacy through a progressive policy of informed consent utilising a branded system of "trustmarks" which represent a company's online information privacy policy.

Companies spanning several different industries, from retail to telecommunications, are backing TRUSTe by becoming premier members. TRUSTe's premier members include: AT&T, IBM, Oracle, Lands' End, Tandem Computers, Excite, Progressive Networks, Wired Ventures, Netscape, CyberCash, MatchLogic, National Computer Security Association.

"The broad industry utilisation of TRUSTe is an acceptance that business practices which protect people's privacy are a competitive advantage worldwide," said Lori Fena, executive director of the Electronic Frontier Foundation (EFF). "By utilising TRUSTe, consumers around the world can know what's happening to their personally identifying information without having to understand the global patchwork of privacy laws."

The TRUSTe program will focus on addressing privacy issues concerning data collection on the Internet. With an emphasis on allaying consumer fears surrounding electronic commerce, the program will utilise Web site icons (trustmarks) to alert online consumers to the uses of their personal information.

Referencing a Boston Consulting Group consumer study, which revealed that privacy of personal information on the Internet is a consistent, significant concern for consumers, Susan Scott, Executive Director of TRUSTe, said that as much as $6 billion in additional electronic commerce could be gained by the year 2000 if consumers' privacy issues were addressed.

"Online consumers fear what happens to their personal information after they give it out," said Scott. "Our program, which focuses on the heart of privacy issues, is crucial to the success of the electronic commerce industry."

Web sites to disclose personal information usage

To further consumer privacy the TRUSTe program will utilise a standardised method of informed consent. A branded system of "trustmarks" or logos, representing the Web site's information privacy policy for users' personal information, will alert consumers to how the information they reveal online will be used. The three trustmarks will be:

No Exchange - no personally identifiable information is used by the site.

One-to-One Exchange - data is collected only for the site owner's use.

Third Party Exchange - data is collected and provided to specified third parties but only with the user's knowledge and consent.

"This system is important both in itself, and as a model of how the industry can effectively regulate itself rather than waiting for government action. It provides for flexible, decentralised enforcement and allows a maximum of choice to customers," Said Esther Dyson, Chairman of EFF.

The trustmarks are backed by an assurance process which guarantees compliance with TRUSTe guidelines. This accreditation procedure will make use of self-assessment, community monitoring and professional third-party auditing, in addition to TRUSTe's review of every Web site. A widespread awareness and education program for consumers and merchants, extensive targeted marketing, media communications, and PR campaigns are among the methods used to spread awareness and educate consumers and merchants on privacy issues and the benefits of TRUSTe's privacy program.

Also announced today, Coopers & Lybrand L.L.P. and KPMG Peat Marwick L.L.P. have been selected as the official auditing firms of TRUSTe. To help ensure that TRUSTe guidelines are adhered to, Coopers & Lybrand and KPMG will conduct random on-site compliance audits and provide due diligence reporting for violations of the TRUSTe licensing agreement.

With its new name, officially announced today, TRUSTe will be spinning off from EFF and CommerceNet and incorporating into its own non-profit entity.

Companies can license the trustmarks by downloading an online licensing agreement and invoice from the TRUSTe Web site at http://www.truste.org. After the agreement and payment have been received the licensee will have access to TRUSTe's technology that verifies the places on the site that collect information and assists with trustmark determination and placement. Licensing costs, ranging from $500 to $5,000, are dependent on the size of the company and the sensitivity of the information.

The eTRUST initiative was launched in July 1996 by the EFF and a group of pioneering Internet companies. CommerceNet and the EFF then partnered in October 1996 to move forward in implementing the initiative.

TRUSTe

TRUSTe is a global, non-profit initiative to establish trust and confidence in electronic communication by creating an infrastructure to address online privacy issues. Comprised of premier members from the electronic commerce industry, the program assures consumer privacy through a progressive policy of informed consent utilising a branded system of "trustmarks" which represent a company's online information privacy policy.

More information about the programme can be found at its Web site address: http://www.truste.org/.