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

OLIS : 23-Dec-1998
Dist. : 04-Jan-1999

Or. Fre.

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

DSTI/ICCP/REG(98)6/FINAL
Unclassified

Group of Experts on Information Security and Privacy

PRACTICES TO IMPLEMENT THE OECD PRIVACY GUIDELINES ON GLOBAL NETWORKS

73163
Ta. 19301 - 20.08.98 - 02.09.98

Or. Fre.

FOREWORD

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 processing of personal information, and its technologically neutral principles are included in a large number of national and international instruments.

Given its history in developing the Privacy Guidelines, its continuing experience in issues related to privacy protection, and its ongoing work in the area of the global information infrastructure, the global information society (GII/GIS), and electronic commerce, the OECD Committee for Information, Computer and Communications Policy (ICCP) decided in September 1997 to undertake a work programme on how to implement the Privacy Guidelines in an online environment.

In this context, the present report, prepared by Mr. S. Gauthronet, consultant, analyses current privacy practices on Global Networks and contains, in an annex, suggestions for a privacy-friendly Web site design.

The report was submitted to the Working Party on Information Security and Privacy in May 1998 and to the ICCP Committee in September 1998 which agreed to declassify it under the authority of the Secretary-General. The report reflects the views of the author and not necessarily those of the OECD or of the governments of Member countries.

TABLE OF CONTENTS

INTRODUCTION

This summary report is based on a flash survey carried out by the OECD Secretariat during the month of April 1998 on some 50 Web sites, mainly commercial sites open to the general public, a summary of which is presented in Annex 2. The aim of the study was to analyse the extent to which, and how, the OECD Guidelines on data protection were put into practice on these different Web sites. The severe constraints arising from the need to adhere to the OECD Programme of Work meant that the study had to be completed on a very short deadline and could cover only a restricted sample.

The choice of Web sites which were surveyed for this study is not statistically significant, nor is it representative of the full range of online services. In selecting the Web sites for the study, we endeavoured instead to select commercial sites with existing privacy policies as examples of "best practices" regarding data protection and respect of users' privacy. The selections were made with the informal help of contacts in a number of countries. The sample includes 3 sites in Australia, 5 in Canada, 1 in Denmark, 2 in Finland, 6 in France, 1 in Germany, 2 in Italy, 2 in Japan, 1 in Mexico, 2 in Spain, 2 in the United Kingdom and 23 in the United States.

The aim of the study was to observe exactly how the principles of the OECD Guidelines are put into practice by these sites through: specific references they may make to the body of governing rules (national legislation, internal policies or professional codes of conduct); implementation of those rules, whether through registration procedures -- subscription contracts for example -- or through additional technical solutions; and, lastly, the privacy protection obligations to which the operators of these sites are subject or which they impose upon themselves.

1. For the purpose of this report, to which we wanted to add suggestions presented in Annex 1, the findings of the survey of Web sites are discussed in the following five sections corresponding to the eight fundamental principles of the OECD Guidelines:

- ***Limitation of data collection***: this point is dealt with in the initial part of the first section through a presentation of the different techniques used for collecting personal data.

- ***Data quality***: this point is dealt with in the second part of the first section, where we endeavour to restate the concept of the relevance of the data collected in relation to the objectives of the site; we thus note what requested information is optional and what is obligatory; in addition we identify what sensitive data these sites may record in their files.

- ***Specification of the purposes:*** the application of this principle is studied in the second section, where we distinguish data processing according to whether it is a matter of targeting consumers for marketing purposes or navigational analysis.

- ***Limitation of use:*** the implementation of this principle, in particular the question of passing data on to third parties and the opt-out possibilities offered to users, are presented in the last parts of the second section.

- ***Security guarantees:*** this question is dealt with in the initial part of the fourth section with respect to online payment procedures.

- ***Transparency:*** the transparency of the practices employed by the Web sites is analysed in the third section through the various references made to national legislation, internal policies or professional codes of conduct. This analysis also includes an examination of the visibility of these guiding principles through the pages of the sample sites as well as a typology of the content of the privacy statements or the contracts accessible online.

- ***Individual participation:*** this concerns the individual rights of the user as they are acknowledged by the sites in the study vis-à-vis their visitors or their subscribers; these are examined in the last two paragraphs of the fourth section.

- ***Responsibility:*** the application of this principle is analysed in the fifth section through an examination of redress procedures offered by site operators and an evaluation of their compliance with the rules they set themselves.

THE COLLECTION OF PERSONAL DATA BY ONLINE COMMERCIAL SITES

Methods of collection and nature of the personal data collected

The Web sites studied collect data mainly in two ways: by placing "cookie" files on users' PCs and collecting information from various forms completed by users.

Cookie files

A majority of sites attempt to set cookies[1]. In some cases, in particular in the press and media sector or on search engine sites, cookies are connected with the placement of "Ad-banners" managed by a marketing agency (or "Rep Agency") such as DoubleClick or FocalLink. If the browser is set up in a certain way, the user is notified by a dialogue box that appears superimposed on the user's screen indicating that the site wishes to place a cookie. In this case, it can be considered that the data collection is done openly and fairly and that by clicking on the acceptance button the visitor consents to the operation. However, this does not mean that that the user is, at this stage, informed of the purpose of the collection and processing that this will permit. If, on the other hand, the browser is set up to accept cookies without systematically displaying the warning box, the user will not see a notification and the circulation of the cookies will operate without his knowledge.

The dialogue box, the content of which is standardised, makes it possible to identify the name of the file which will be recorded in the ad hoc directory, the origin of the cookie (name of the URL), and its expiration date. The majority of the cookies sent by the sample sites have expiration dates set for the end of 1999, or a life-span of almost 20 months. Two cases extend the life of the cookie beyond the year 2000 (2010 for the one, 2020 for the other).

In order to follow a user's navigation through different pages, Web sites may need to place cookies on a user's machine a number of times throughout the interaction. The number of times cookies are set may be very high: in many cases it is greater than five, and several of the sample sites set cookies more than ten times. The risk here is that Internet users will tire of the cookie warning and set their browsers once and for all to accept cookies to avoid the too-frequent appearance of the warning box.

---

1. A "cookie" is a mechanism which "server side" connections can use to both store and retrieve information on the "client side" of a Web-based connection. In practical terms, a cookie is a text file that a Website places on a user's computer when the user visits the site, which can later be accessed and read by the Website's server each time the user visits the site. The file contains information about the user that allows the Website to recognise the user and recall user preferences, for example to check the user's password or to direct the user to a preferred destination page within a given site. Cookies can also be used to register articles to be purchased in an electronic shopping mall (in which case the cookie would serve as a "shopping cart" until the final phase of a transaction) or to personalise the site according to the user's identity. They can also be used to collect data about the site audience, for instance by tracking user behaviour within the site or tracking return visits.

With the exception of one site, none of the Web sites surveyed made entry to and navigation on the site, or a section of it, conditional upon the acceptance of the cookie. Indirectly this means that at this level there is no conditional relationship between the supply of personal data and access to an Internet site.

Where a Web server sends out information which is stored by the user's browser software and retrieved on a subsequent connection to the server ("cookies"), the system can indicate that the visitor has been there before, but without revealing his identity. Identification requires matching the data collected by cookies with other information, and as a result, when linked to the identification file incorporated into the browser and transmitted to a server, the information recorded in cookies can yield valuable user profiles. However it is to be noted that some browsers offer an option which stops a cookie being sent: this option is often unsatisfactory and more or less user-friendly.

Forms

As most of them offer commercial services, all of the sample sites submit forms that visitors must complete in order to register, subscribe, take part in a discussion group housed on the site, make suggestions and, in particular of course, to book a service or order an article and initiate the purchase procedure.

The data most often collected include the user's name, address, home or work telephone number and e-mail address. Additional identifying data is also sometimes requested, such as age, sex, marital status, occupation and in some cases income, the size and sector of activity of the enterprise or personal interests (sports practised, reading habits, etc.). The order forms all require the type and number of the credit card and its expiration date, and they also provide for different delivery and invoicing addresses. These data are collected in the context of registration, voluntary participation in a survey, or payment procedures, which means that for the most part they are relevant to the user activity.

Although for the most part information is collected through cookies, some sites ask their users to state what operating system they have on their PC and the version of the browser they use to connect to the Internet, as well as the transmission speed of their modem. Certain sites include online questionnaires connected with their activity and ask for precise data concerning, for example, in the case of computer hardware manufacturers or software producers, the characteristics of the computer used; and for travel agencies, the preferences for airline cabin services (seat location, meals).

Automatic data collection

It is well known that two of the basic technical components present in browsers (Java or ActiveX) at one time had serious anomalies which threatened the security of the personal data and files present on users' PCs. More precisely, in versions 2 and 3 of Netscape Navigator it was possible for a Web site intent upon doing so, to capture visitors' e-mail addresses without their knowledge. Subsequent versions of the browser software have resolved this problem. To eliminate any question, several of the US Web sites in the study explicitly state in their privacy policy that they do not collect the e-mail address other than when it is voluntarily supplied by visitors.

However the means of automatic collection still exist through the Internet Protocol (IP) address which contains, in particular, the name of the domain to which a user belongs and his access provider. Only two of the sample sites make reference to this type of data collection, which is somewhat technical and does not reveal much with respect to identity. It is also possible to collect data from the identification

form that a PC user is invited to complete in the configuration options of his browser which is the equivalent of a personal identity card. This optional form contains several "click-buttons" and many fields for the user's name, e-mail address, home and work addresses, different telephone and fax numbers, occupation and even an open text zone. If the browser is not configured so that a dialogue box appears to notify the user that a site wishes to access the information stored in the user's browser profile, the transfer of data takes place automatically without the user's knowledge. This being said, there is nothing to oblige a user to personalise his browser, or even to enter his e-mail address. None of the sites studied mention this method of collecting personal data.

Lastly, there is still another very simple way of collecting an electronic address, without the visitor necessarily being aware of it, which is to use the heading of electronic mail or the various forms that are transmitted by e-mail. In all, only one French site, which offers a share portfolio management service, mentions this risk by activating a browser dialogue box which is displayed prior to the visitor's transmission of an information request form.

Quality and relevance of the data

Data collected and the purposes of collection

On the whole the data collected by the sites surveyed appear relevant to the purpose of their eventual use.

It is however, fairly rare for the user to be informed of the purpose at the time of the collection process. This remark applies in particular to the cookie files: the dialogue box appears unexpectedly during the navigation and contains no indication as to the purpose of the cookie. To learn about the purpose of the cookies set by the site, a user must go to a public service area of the site where the "cookie policy" is explained. In the case where a cookie policy is given, the three most often stated purposes are fairly neutral:

- automatic recognition of the visitor when he connects, which avoids having to ask him to identify himself; this is a principle of ease and convenience for the user;

- analysis of the clickstream data to detect the pages most often visited, in order to develop the content of the site in a way that best responds to user demand; and

- keeping track of articles selected during the purchase session up to the completion of payment during the session, or during a new session if the first is interrupted for any reason.

However, it is remarkable that none of the sites openly explains that one of the objectives for the use of cookies is to be able to send "one-to-one" advertising communications by precisely targeting visitors according to their individual profile. Perhaps some Web site operators believe that such processing is not their concern, since it is generally done by specialised agencies, and their sites play only a supporting role. If they do think in this way, it would raise issues for further examination. What is more, it is clear that other sites carry out their own impact studies: one site thus explains that it contributes information to anonymous studies that enable it to tell its advertising clients that "12 000 people clicked on ad-banner X or Y today and among them 35 per cent had previously told us that they were interested in sport." The paradox is that nowhere does this site explain that it carries out clickstream analysis and that

at the time when the processing itself is done, the input data are not anonymised; only the output results are reported.

On the other hand, there is more chance of finding an acceptable explanation for the purposes associated with the collection process when questionnaires are involved. The site operators make considerable efforts to explain at the beginning of the questionnaire that the information requested is intended, for example, to record participation in a competition, or to carry out socio-demographic studies on visiting habits. The sites also explain that the data will be processed in an aggregated and anonymous fashion and, to clarify this, there is often an illustration such as: "40 per cent of our members are in the 20 to 30 age group."

Optional and obligatory information

In nearly two-thirds of the sites, some of the information requested in the various registration forms, feed-back forms and above all the questionnaires, is optional. To make it clear to visitors which information is optional, several sites have adopted the practice of separating the optional information in an independent box. This practice is clearer than that frequently adopted by sites where the optional fields are marked with an asterix. Still other sites display labels corresponding to the obligatory fields in bold type or preceding them by the word "Required." "Optional" data often include a request for an e-mail address, a telephone number, age, sex, occupation, and certain personal preferences and habits. In one case, a Japanese shopping centre offers visitors the benefit of acquiring points towards gifts where they replied to the optional questions, and another site gives entry to a competition in exchange for providing optional data. In yet another case, an online bookshop gives visitors stating their preferred types of reading materials the right to free monthly information (sent to their electronic mailbox) giving details on recent books corresponding to the personal tastes marked on the questionnaire.

The obligatory information, for its part, generally corresponds to the identification and payment data essential for subscribing or making a transaction. In this context certain data may be checked against tables and verified online. For example, in the case of information provided about address, postal code, and credit card data, these checks may be made either directly by the site itself or through an instant connection to an authorisation server.

The collection of sensitive data

The study revealed that at least three sites collect information of a sensitive nature. Two of these sites are online bookshops. One gives visitors the option of marking preferred types of reading material in a long list which includes subjects that may indirectly reveal the sexual inclinations of the visitors who select them ("gay studies", "lesbian studies") or their religion ("Eastern religions", "Judaeo-Christian books"). This site has no particular arrangement to safeguard the confidentiality of these data. The other bookshop, however, is more prudent and states that the sensitive data that it may collect (social security number, mother's maiden name, salary, ownership of a share portfolio, medical data, data concerning children) will be handled with "extra care." The policy states that information will not be passed on outside the organisation, and the site offers users the opportunity to "opt-out" to prevent these data being shared even with other business units within the organisation itself.

The third site that collected such data was for an Australian travel agency which, in the course of registering its members, collects data that may be qualified as indirectly sensitive, connected with the stating of service preferences when making flight reservations. These SSR preferences ("Special Services

Requirement") have been codified and standardised at the international level under the aegis of the IATA (International Association of Travel Agents) in a table known as AIRIMP, and are commonly used by travel agencies all over the world during the creation of the PNR ("Passenger Name Record"). The AIRIMP includes almost 100 four-letter codes, some of which define food requirements (diabetic meals, vegetarian meals, Muslim meals, kosher meals, etc.) and the passenger's physical condition (e.g. blind passenger, deaf passenger, wheelchair in cabin, etc.). The collection of this data is offered on the Internet site so that the data can be taken into account during the online reservation process.

THE PROCESSING OF PERSONAL DATA BY ONLINE COMMERCIAL SITES

Nature of the data processing

Virtually all of the sample sites clearly state their procedures for the processing of personal data. A distinction must be made between two categories of processing: processing for the purpose of targeted marketing and the processing of navigational data (clickstream data):

- Processing for marketing purposes is intended to establish the profiles of visitors to sites who have registered and supplied certain data through which they can be identified. It is usually stated that this processing will lead to targeted commercial offers being made to visitors by three types of communication: ordinary mail, electronic mail and (more rarely) by telephone. Fewer than five sites practise "host-mailing" and they explain that they may themselves implement a marketing campaign for outside partners, which are always described as reputable and rigorously selected companies.

- Processing of clickstream data makes it possible to match two sources of information:

  – the visitor identification and profile data which is collected during the initial registration of site users; and

  – the data generated either on the basis of the log analysis software[2] present on the server platforms, or with the aid of cookies, which will make it possible to follow step-by-step the specific pages consulted by users and the articles placed in their shopping basket.

Only three sites admit that they engage in this type of data "matching" process, which clearly makes it possible to refine the user profiles and, above all, to determine which parts of the site are visited most often by a given category of user. With respect to one-to-one marketing, this information is obviously a high "value-added" commodity for advertising agencies, space purchasers and advertisers. The small number of surveyed sites which practice relative transparency in this respect have the common characteristics of all being of North American origin and belonging to the TRUSTe label. These sites explain in their privacy statement that they are financed primarily through advertising revenue and that freedom of access for visitors depends on their ability to provide precise targeting data. These sites also state that they do not make connections between individual identities and site navigation data. However beyond their stated intentions, admittedly nothing prevents this processing technically, to the extent that

2. "Log Analysis Software" is server-side software used by a Website to analyse data about users collected through the use of cookies by putting it together with information collected by the server in a "standard server log file". The log file data is obtained when a user connects to the Website, including IP address, connection date, type of transaction, name of files transferred to the user's browser, the protocol used, the page from which the user has arrived at the server, and/or the type of browser used. Log analysis software can be used for in-depth analysis of Website traffic.

the cookies set by these sites contain a permanent user ID that is easy to connect with identification and profile data collected during the process of visitor registration.

Transfer of data to third parties

Two families of sites can be distinguished at this stage: sites which explicitly and categorically declare through their privacy statement that they do not intend to pass on any personal data to third parties other than aggregated and anonymous statistics; and sites which, in generally careful terms, explain that they may have occasion to provide subsidiaries or outside partners with personal data with a view to advancing commercial offers. All of the sites which cede data to third parties acknowledge the respect of privacy by giving people the opportunity to "opt out".

Opt-out possibilities

Half of the sites analysed give visitors the opportunity to refuse to have their personal data processed for commercial purposes or transmitted to third parties ("opt-out"). The visitor has the opportunity to express his refusal in four different ways:

- by marking a specific box: usually provided on the registration form, this option appears to be the simplest and most natural way for a person to exercise his right of refusal;
- by mail: here it should be noted that not all sites make the provision of indicating their postal address at the same place where this notification appears; visitors are generally requested at this point to give their precise name and address so that their request can be taken into account;
- by e-mail; and
- by telephone (however, only a few sites provide a free call number).

A number of sites claim to offer the possibility for users to opt-out without specifically stating the procedure as to how this right can be exercised. In practice, after a fairly lengthy search, such explanations were found as part of the privacy statement. There, users were informed that upon receipt of subsequent commercial e-mail, he or she has the opportunity to send a reply asking not to be sent any more such mail. Thus, it is more a case of deferred opt-out.

It is very important to note that the opt-out arrangements as set out in the sample sites only apply with respect to commercial approaches or advertising operations that may be aimed at the visitor. Only the sites in the press sector include in the opt-out the satisfaction surveys that might be sent to subscribers by e-mail. In addition, the opt-out procedure makes no distinction between marketing initiated by the site itself, or that initiated by third parties to which a file of prospective clients may have been communicated. In none of the sites analysed did users have the possibility to opt-out of the processing of clickstream data or those relating to their purchasing behaviour. Only one of the surveyed sites offers what might be called a non-commercial opt-out procedure. This particular site is a Canadian Web site that permits subscribers to post "jobs-wanted" ads. For obvious reasons of confidentiality, the job-seekers have the opportunity to transmit, via a free text zone, a list of enterprises to which they do not want their applications to be sent. Indirectly, and even if it is complex, this example shows that sites are capable of treating opt-out requests in different ways.

Only one of the surveyed sites makes reference to a procedure for obtaining the consent of its visitors prior to the use of personal data. This particular site is a large American technological site which offers its visitors several mechanisms for providing feed-back. The site receives a variety of information and views from users which the site operators consider they have an unlimited and irrevocable right to use, which raises some issues for consideration. In cases where these texts are to be published however, the site undertakes not to name their authors except after prior notification or with consent.

Lastly, special mention should be made concerning the possibility of exercising a global and centralised opt-out with the agencies that exploit advertising information on the Internet, a possibility which is, in fact, offered by the DoubleClick agency among others. Specifically, the activation of the procedure involves connecting to the agency site and selecting the "privacy" section: here the user can read a general declaration by the enterprise concerning its practices with respect to the protection of privacy and choose the opt-out option. At that point, the identification number specific to DoubleClick contained in the user's cookie file is erased and replaced by "ID = OPT OUT". There is virtually no public knowledge of the existence of this procedure; of 17 million cookies set about a year ago, DoubleClick declared that it received at the time scarcely more than 5 to 10 opt-outs per day. One likely explanation could be the fact that none of the Web sites that market their advertising space via an agency of the DoubleClick type make reference, by hyper-link for example, to the existence of this possibility.

TRANSPARENCY OF THE WEB SITES WITH REGARD TO THE PROTECTION OF PRIVACY

The Web site survey makes it possible, to some extent, to assess the degree to which sites implement the principle of transparency with respect to their privacy protection policies. Here we sought to identify the body of rules to which the sites make reference and the terms in which they do so. It turns out that none of the sites make reference to any of the international instruments referred to in the inventory (OECD Guidelines, Council of Europe Convention, United Nations Guidelines, European Union Directive). Three categories of site can be distinguished according to whether they refer to national legislation, internal policy, or a sectoral code of conduct.

Reference to national legislation

On the whole the European Web sites in the study make reference to their respective national legislation in the field of data protection, however some sites did not include any such specific reference. When available, the reference most frequently appears in a public service section of the site which deals with the right of access and the correction of personal data, a "Frequently Asked Questions" (FAQ) section, a subscription contract (e.g. the press sites), or again, as part of the privacy statement when there is one, which is not always the case with the European sites.

Rather than national legislation on data protection, the two American sites operating in the credit reporting sector refer to a sectoral Act in the field of credit (FCRA: *Fair Credit Reporting Act* — 1970, amended Sept. 30, 1996) which comprises a set of provisions on the right of access and correction of data, their duration of storage, and restrictions concerning their transmission to third parties; one of the two sites offers a hyper-link giving access to the full text of the Act. It should be noted, however, that the reference to this Act concerns the protection of the privacy of the consumers whose data are contained in the files, much more than the protection of the privacy of the subscribers to the Web site who access the data. The subscription contracts for these sites are very elaborate, which is an indication of the very particular sensitivity of American society with respect to Credit Bureaus. Thus in subscribing to the site, the clients of the system, who both consult and enrich the data base of consumer credit reports, agree to respect the obligations imposed by the FCRA, while specific clauses of the contract remind them in particular of the obligation to respect the purposes for which they use the data ("legitimate business") and the obligation to divulge sources of data on demand.

One Canadian site specialising in job vacancies protects the confidentiality of the personal data stored in its databases by invoking the national legislation on copyright; it cites the sanctions applicable to acts of piracy and encourages, by means of a reward of Can$500, the denunciation of any fraudulent use, reproduction or redistribution of the data.

The presence of Privacy Policy Statements

Three-quarters of the sample Web sites studied have a policy for the protection of privacy intended for their visitors and accessible online. It can be seen that there is not, strictly speaking, any connection between the fact that the sites have made the effort to adopt a specific policy, and the fact that at the broader national level there are legal provisions on data protection. Eleven out of 19 sites of European origin have their own privacy policy; logically enough the proportion is 22 out of 23 for the American sites. None of the sites seek explicitly to exploit the fact that they provide privacy statements to enhance their image or boost visitor trust. In evaluating the transparency of these policies, particular attention was paid to the accessibility of this information, the guarantees offered, and the possibilities for recourse available to users.

Accessibility of the Privacy Policy Statements

The situation is very mixed regarding the ease with which visitors can access the privacy statements on Web sites. The operation is easy on a little over half of the sites looked at in the study, but it is more complicated on at least ten of them, where it takes a fairly long time to find the privacy statement. For some sites it is even necessary to be quite far advanced in a registration process or in a transaction -- i.e. the user has to have started to transmit personal data -- before a link with the site's provisions regarding personal data and privacy appears. The simplest procedure is of course when the section title "privacy" appears on the homepage; this is most often the case and the interested user can satisfy his curiosity very quickly. Lastly, it can be noted that only five sites included the term "privacy" in the keyword catalogue of their internal search engine.

Typology of the policies

It was not within the scope of the study to include an in-depth legal analysis of the content of the privacy statements displayed by the different sample sites, but they can be classified in three broad categories:

- *Provisions included in FAQ sections:* these are usually fairly brief sections (one to five paragraphs) often dealing with only part of the question; some focus on cookies, others on the capture of e-mail addresses, or the opt-out procedure, and others on secure data transmission protocols. One of the features common to these sites is that perhaps they are new to the Web. Also, they often skip over the issue by stating that they can invoke the national legislation of the countries where they are established. The only somewhat exceptional case in this group is that of Netscape where there are no less than four or five pages of fairly technical questions and answers on privacy protection issues. But this site also has a section in its Terms Of Service, which precisely defines the data collection practices and the opt-out conditions.

- *Privacy Statements* in the form of guidelines: these are often entire sections, generally accessible from the homepage. In terms of volume, these guidelines vary between a single page and ten densely filled pages, the average being estimated at about three or four pages. The sites differ first of all in their content. Certain sites adopt a policy that is consistently favourable to visitors: no export of cookies (in particular on sites targeting children), traffic analysis limited to login statistics, reduced duration of data storage, reference to the right of access to data, opt-out procedures, and non-transmission of data to third parties. At the other extreme, the sample included a number of sites which set out in detail their data collection

and processing practices, which might be characterised as extensive, but which at the same time do not affect the possibility of exercising individual rights.

It is clear that the presentation of privacy statements on Web sites tends to be a North American practice. The sites that have adopted it are generally well-established in the online world, are among the architects of the World Wide Web, are close to the technology, and they carry out a strategic activity on the Internet. They are the ones that present the most detailed provisions and indeed, it must be recognised that they take the transparency principle quite a long way. These sites also provide various links to further information on privacy protection, usually internal links for technical questions, and in one case a link to outside bodies such as the EFF (Electronic Frontier Foundation) or EPIC (Electronic Privacy Information Center). All the sites which state that they belong to TRUSTe are in this group. The sites of the two Credit Bureaus present in the sample also have very detailed privacy provisions, but this arises partly out of a different rationale (FCRA).

- *Contractual arrangements:* this is the case of sites whose provisions concerning privacy are integrated in the form of clauses in the contractual conditions; these conditions generally include registration with a discussion forum, a "push" information service, a subscription to the electronic edition of a newspaper, or an online purchase. They are found in two forms:

  – In a condensed version, generally in the form of one or two paragraphs at the top or bottom of a form into which the visitor is about to enter personal data; in particular the French sites surveyed tend to favour this style and in a few words they make reference to both the national legislation and the right of access and correction.

  – In a detailed form through the Terms of Service; the provisions concerning privacy then appear together with other branches of the law: the applicable commercial law, civil liability, compensation, or copyright. The provisions describe the data collected, the processing and any transfer to third parties that the Web site might effect, or on the contrary, refrain from. The restrictions that a site imposes on itself have the appearance here of a real commitment on major privacy issues; it is through a clause of this type that one sample site, specialising in tourism and affiliated to the American SABRE CRS (Computer Reservation System), agrees not to communicate to third parties that are not parties to the transaction, data relating to flight reservations provided by clients of the site.

Shortcomings in the content of privacy statements

On the whole, and considering the selective choice of the sample sites, the conclusions we can draw regarding the content of the privacy statements are fairly mixed. At least one third of the sites surveyed are not very explicit about the data collected, and over half do not address the question of clickstream data and the processing to which they are subject. Another third of the sites do not provide opt-out possibilities or a right of access. Lastly, almost one-quarter of the sites surveyed do not give any physical address permitting the visitor to know something about who he is dealing with in order to seek redress through traditional forms of communication, if necessary.

Reference to codes of conduct

Three of the sample sites make reference to professional codes of conduct specifying a certain number of guarantees and commitments concerning the protection of consumers' privacy. The three sites

in the survey are commercial sites in Canada, the United States, and France, and all three refer to the code of conduct of their national association of direct marketing professionals. Our aim was not to pass judgement on whether these codes of conduct are adequate or not, but rather to look at whether the provisions contained in these codes are correctly applied by the Web sites which claim to respect them. This analysis leads us to make the following observations:

- The Canadian site is a commercial server; it refers explicitly (with a hyper-link) to the code of ethics of the CDMA (Canadian Direct Marketing Association: Code of Ethics & Standard of Practice) which has recently been amended to integrate specific provisions concerning online commerce. This code contains, in particular, fairly protective provisions on obtaining the consumer's consent for the transmission of commercial offers by e-mail, and the obligation to provide information on the processing of clickstream data. While it is very clear that this second principle is remarkably well handled by the site in question through a very detailed FAQ concerning cookies, it is equally clear that, in the light of the study, the first principle is silently over-looked and no opt-out procedure is offered.

- The American site, which is one of the two Credit Bureaus selected in the sample, states that it belongs to the DMA (Direct Marketing Association)[3] and provides a link with the Web site of that organisation. The principles of the American DMA are significantly different, and appear to be less restrictive, than those drawn up by the neighbouring association in Canada. They are, on the whole, correctly applied by the Credit Bureau to its Web site, which does not use the cookies technique. Two reservations must be expressed however: first, the information on the processing carried out on the basis of the login files is not sufficiently detailed, and second, while the principles of the DMA particularly stress the need to place the information notice on data collection and processing practices on the page where the information is collected, it was seen in the study of the site that this recommendation is not correctly implemented. Furthermore, the use of the opt-out choice online is strongly encouraged by the DMA, whereas this site offers only the possibility of opting out by ordinary mail, and without this possibility being restated during the data collection procedure. It should be noted however that once the opt-out is recorded by this Credit Bureau, it becomes definitive, whereas the DMA standards only call for a five year limit on the duration.

- The French site is a large store specialised in the sale of books and CDs. It states on its site that it adheres to the national professional code of the *Syndicat des Entreprises de Vente par Correspondence* (SEVPCD). This code of good conduct takes up certain provisions of the French legislation on data protection and develops a whole code of practice for the processing of requests to be removed from files, prior information for prospective clients, explanation of the purposes, making data available to third parties, etc. A quick examination reveals that the site does not perfectly comply with the recommendations, in particular with regard to article 3.4 which stipulates that the processing must be regularly notified to the national data protection authority (in France, the CNIL -- Commission nationale de l'informatique et des libertés). No specific steps have been taken by the store in this regard, since it may consider that it is within the rules by making a global declaration at group level for all of its direct marketing activities.

3. C.f. The DMA's Marketing Online Privacy Principles and Guidance.

SECURITY AND PRIVACY ENHANCING TECHNOLOGIES

Making payments secure

Security of systems

Of the 34 sample sites that sell products or services through their Web site, a very large majority use the SSL (Secure Socket Layers) payment protocol installed on secure servers. This point is easily verifiable in so far as the entire purchasing process takes place on the user's browser, with the security icon in the locked position. Some sites have additional features:

- one Italian site, for example, uses the Verisign certification system; and
- all the French sites use the centralised national architecture for the remote authorisation of payment by card; thus during the online payment process there is a re-routing of the connection to one of the dedicated computer centres which then provides the site operator with an authorisation number and validates the transaction. The system is designed in such a way that the financial establishments do not know the content of the shopping basket, which is probably not the case with the co-branded card payment systems between VISA and AOL or Yahoo!.

One site specialising in compact disc sales offers the opportunity to transmit the credit card number via an encrypted e-mail using the Pretty Good Privacy (PGP) system[4] which can be triggered at the moment of payment.

Security of procedures

Some sites propose solutions which are simple to use and help to ensure the confidentiality of online payments. Two or three sites for example ask the visitor, either during registration or at the time of payment, to give the mother's maiden name; the collection of this information may appear curious or disproportionate, but in reality it serves to authenticate a client who has forgotten a password and who nevertheless wants to access his customer account. It should be noted that there is nothing exceptional about this procedure, which is used in particular by the big credit card operators when a declaration of card loss is made by telephone.

Another site, specialising in the management and the valuation of share portfolios provides basic but pertinent advice to its visitors who wish to maintain a certain level of confidentiality regarding their

4. PGP is a software programme that uses encryption to protect the privacy of electronic mail and data stored on a computer harddrive. It can also be used to "digitally sign" data to provide evidence about the authenticity and/or integrity of the data.

online navigation. It advises them, for example, to close the browser at the end of their session and empty the directory cache in order to remove any trace of the personal financial information that has been displayed.

Lastly, three sites offer a system which should be strongly encouraged for all electronic commerce aimed at the general public: this is an option that the client can choose which allows him to request that the site copy and store his credit or charge card number(s) in a personal portfolio. In this way, when the client returns to the site to make a purchase, he only has to choose one of his cards which are presented to him by revealing the last four digits of the card number. Thus the card number will have been transmitted on the network only once, during the first purchase. These sites state that they take special precautions in storing the card number by using a database that is maintained on a non-networked computer.

Exercise of the right of access

The exercise of the right of access by visitors to Internet sites can be seen both as a way of checking the personal data collected, and also ensuring that the data are kept up to date and, if necessary, providing the opportunity to correct the data. Over half of the sites studied provide an individual right of access, and for a quarter of the sites this right can be exercised online in other words the request and the response are executed in real time during a connection through a dialogue between the browser and the server platform. Since this procedure is technically not very complicated to set up, it is rather surprising that it is not more widespread. Lastly, it seemed that, among the sites surveyed, the US sites were the ones which least often offered their visitors the opportunity to exercise their right of access.

Privacy enhancing technologies (PETs)

The inventory identifies several technological mechanisms that can be made available to Internet users to help protect the confidentiality of their personal data or their navigational data. These techniques, mainly OPS (Open Profiling Standard) and P3P (Platform for Privacy Preferences), are still in an embryonic stage of development, which probably explains why only one of the sample sites explicitly uses one of these solutions. That site is an American online bookshop which uses the Firefly system. Firefly is based on a “collaborative filtering” technique, to which, it should be acknowledged, scarcely 30 sites belong at present. It is noteworthy that the Firefly company was very recently taken over by Microsoft. Specifically, the system currently operates on the basis of a trustworthy third party, where the Internet user supplies the Firefly site with his personal data (identification and interests) and defines a private or public status for each. This constitutes his “passport”. When he connects to a site belonging to the Firefly network all he has to do is enter the Firefly password and the site automatically retrieves the public data from his passport. The visitor benefits from the confidentiality commitments defined in Firefly’s privacy statement (right of access, right of online correction of data, prior consent for the transmission of the e-mail address to third parties, prohibition of “reverse searches” to identify the owner of an e-mail address, right of reply, claims). However, the visitor also benefits from expressing his personal preferences, because the site, on the basis of his profile and the definition of his preferences, will then be able to send him targeted information. In the case of the online bookshop in the sample, this results in the display of a personalised welcome page and the transmission by e-mail of information about new books and authors. It is curious, however, that the site does not draw attention to the fact that it uses Firefly, except through a minute icon at the bottom of a screen.

CLAIMS AND RESPONSIBILITIES

Redress mechanisms

In the last section of the inventory we noted the different national mechanisms, based on legislation or self-regulation, aimed at ensuring that Web sites respect their obligations concerning the processing of personal data and the protection of privacy. Some of these instruments also offer possible redress mechanisms enabling visitors to Web sites who consider that they have suffered injury to institute an action.

It emerges from the analysis that scarcely ten sites out of the 50 studied in the sample offer their visitors or clients possibilities for recourse in the case of disagreement. A distinction should be made between four types of redress mechanisms:

- Claims by e-mail: aimed at dealing with any problem that may arise with a delivery, for example, the quality of the product or invoicing. Applying a world standard for distance selling, the majority of the sites have a purchase return policy. Generally speaking, since all sites give their e-mail address, it can be considered that this means of communication is always open to visitors to ask questions or to express their disagreement with this or that practice.

- Financial recourse: one Italian commercial site agrees to compensate a client up to US$50 in the case of fraudulent use of his payment card as the result of an online purchase on the site and where the institution which issued the card maintains that the client bears part of the responsibility.

- Claims before an arbitrator: the Web site of a French bank has a page dedicated to the amicable settlement process available via its customer service department for settling any disagreement that may arise with a client. This offer is broad and is not limited only to possible disagreements that could result from the use of its Web site.

- Claims before the courts: lastly, some Web sites, online newspapers in particular, have in their contracts a clause of attribution of jurisdiction which designates the legal institution competent to deal with any dispute between the two parties.

Responsibility and liability regarding the respect of privacy

The sample sites which explicitly agree to hold themselves responsible for the application of their privacy policy statement are very few -- seven in all. Here again it should be pointed out that this acceptance of responsibility frequently concerns only the limitation of the transmission of data to third parties.

This seems to raise the question of the value of these commitments. This study of Web sites does not allow for an answer to the question at this stage, but an awareness about certain practices provides a perspective on the scope of the site operators' pledges, and even in some cases their contractual commitments.

Recent examples seem to indicate that certain sites, under pressure to find any way to balance finances, may be willing to embark on marketing operations contrary to their commitments vis-à-vis their subscribers. The best known case is that of a telephone campaign that a major service provider planned to launch last summer. The project provided for the disclosure to direct marketing firms of a list of several hundred thousand personal telephone numbers of subscribers to the service, whereas according to the contract the collection of these numbers was intended exclusively to make it possible to warn subscribers rapidly in the case of fraudulent use of their access and of their means of payment. At the same time, this service provider discreetly and unilaterally modified its Terms Of Service in order to add telephone numbers to the list of data that it authorised itself to transmit to third parties for the purposes of commercial canvassing. This operation clearly infringed the established principles in two ways: it was both an alteration of purpose, and a failure to inform the persons concerned directly and honestly[5]. This particular case showed an indication of the effect market pressure can have, i.e. the anger of members and their threat to cancel their subscriptions, and the criticism of some commentators, forced this large operator to abandon the plan.

5. Cf. Serge Gauthronet: "*Les services en ligne and la protection de la vie privée* -- Rapport n° 2 -- Etudes de cas" - Commission of the European Communities — ETD/96/B-3000/142 - Brussels - December 1997 — (in print).

CONCLUSION

The most striking conclusion that can be drawn from this study is that there is a marked discrepancy between the world of the various institutions and organisations that develop ideas and instruments for data protection on the one hand, and the world of Web sites on the other. The latter, or the great majority of them, whatever their sincerity or their good intentions with regard to their visitors, actually give the impression today that they pay too little attention to the issues involved in the protection of privacy and transborder data flows, and, most importantly, that they lack precise and consistent direction for privacy protection applicable to online networks.

It therefore seemed useful to draw up a set of generally applicable suggestions corresponding to some of the “best practices” that were highlighted by the survey or which, on the contrary, can be derived from the shortcomings or gaps that can be seen in the Web sites analysed.

Without claiming to be exhaustive, and without implying any kind of ranking in their classification other than that stemming from the chronology of this report, we can thus formulate, in the spirit of both the proper application of the OECD principles and the promotion of a climate of confidence for electronic commerce, the ten series of suggestions attached in Annex 1.

ANNEX 1

SUGGESTIONS FOR A PRIVACY-FRIENDLY WEB SITE DESIGN

1. Cookies

- The visitor to a Web site should be informed of the purpose of the collection and processing of data relating to cookies at the moment when these are placed in the corresponding file of his browser.

- The duration of storage of cookies, and more generally any personal data, should be defined and should not be excessive. A "life-span" of two years would seem to be acceptable and longer periods could be admissible depending on the duration of the contract between a user and an online service to which he connects regularly. In this case, the duration of storage should be proportional to the period during which the service is provided, plus a period of about one year for the settlement of any disagreements concerning invoicing or for trying to win back the client.

- The placement of multiple cookies provoking a saturation effect for the visitor should be strongly discouraged.

- Once a user has expressed his refusal to accept a cookie, the Web site should definitively stop its attempts to place them on the user's hard drive.

- There should be no link between the acceptance of a cookie—or more broadly the transmission of personal data—and the ability to navigate freely through the public pages and sections of a Web site.

- Information on the purpose of the cookies placed by a site should be factual and complete. In particular, sites should make it possible to differentiate the purposes and the processing of data according to whether the cookies are placed by the sites themselves or by advertising agencies.

- This information should also include precise details on the existence of data matching processes between the identification data (see Suggestion 8) and the clickstream data collected through the cookies.

2. E-mail

- Any message sent to request information from a site indirectly reveals the sender's e-mail address; in the context of an obligation to advise, sites have the responsibility to warn their visitors of this.

3. Forms

- Optional information collected by means of the various forms (registration, surveys, feed-back, payment) should be clearly separated from the obligatory information and grouped in a distinct block.

- If sensitive data are legitimately collected, the site should undertake to respect the highest degree of security and confidentiality for them.

4. Transfer of data to third parties and opt-out

- Any site that collects personal data should give its visitors the opportunity to opt out online.

- The opportunities to opt-out should be available to users at the time of data collection by means of marking a box on the data collection form itself.

- The exercise of the opt-out, where this is necessary, should indicate the processing that it applies to: commercial processing by the site itself, clickstream analysis, extraction of lists destined for third parties and the data matching processes to which these lists could subsequently be subject.

- It should also be possible to opt-out from the one-to-one targeting done by advertising agencies; to this end Web sites should be able to register the opt-out information for transmission to the agency or provide a hyper-link for the user to connect directly to the appropriate page of the advertising agency and carry out the procedure himself.

- Any site which, after agreeing not to provide personal data to third parties, nevertheless wishes to do so, must obtain prior consent from those concerned. Unilateral modification of the terms of service cannot in any case be sufficient.

5. Education/information

- Any Web site referring to application of an international or regional data protection instrument is encouraged to make explicit reference to that instrument and provide a hyper-link to the site of the organisation concerned.

- Any Web site operating out of a country which has national legislation on data protection should make formal reference to it and, in the context of its general user education and information policy, provide a hyper-link to the administrative authority responsible for the proper implementation and enforcement of the legislation. In this context, it is imperative

that every existing data protection authority be present on the World Wide Web through relevant, well-documented and interactive sites.

- Any Web site claiming to adhere to a professional or sectoral instrument should provide a hyper-link to the text of the code referred to, as well as to the site of the professional organisation responsible for its proper implementation and enforcement.

6. Transparency of sites

- Whatever the international or national instrument to which they claim to adhere, sites should, because they operate on a global level, have privacy statements accessible online to their visitors.

- Privacy statements accessible online should, as a minimum requirement, be explicit about the data collected, in terms of their justification for collecting data, the use of the clickstream data and the processing to which they are subject, as well as the opportunity to opt out.

- The reference to the privacy statement should be explicit and visible on the homepage of each site concerned.

- Any site established in a country where the national legislation requires prior declaration of processing should indicate the receipt number issued by the competent authority.

- Any site claiming to apply a sectoral code of conduct should scrupulously respect all of its provisions.

7. Security

- Commercial sites which offer online payment procedures should be required to upgrade their server platform so as to be able to integrate the most secure methods as soon as they become available and have been tested.

- Commercial sites which offer for sale products or services that can be bought for small sums should accept anonymous means of payment.

- In the context of their duty to inform visitors, sites that process confidential data should warn their visitors of the risks of the data which exists on their local hard drive of their PC (such as tracking or cache files), being disclosed.

- In the absence, for now, of absolute security in terms of authentication of payments and transmission of data over networks, commercial sites which accept online payments by card could configure their systems in such a way that they only need to ask for the card details once, on the imperative condition that they store this information in highly secure files on non-networked computers.

8. Individual rights

- All sites involved in electronic commerce should offer their clients procedures for seeking redress by e-mail.

- All sites collecting personal data should provide identified visitors with the opportunity to exercise their right of access online; failing this, the right of access should be able to be exercised offline, and in this case the postal address of the site should feature prominently.

- It should be possible for the right of access to data to be exercised in full and this right should not be limited to the data supplied by visitors to the site. If data are collected or generated elsewhere -- for example where clickstream or purchasing profiles are created -- visitors exercising their right of access should also have this information communicated to them, and in particular the behavioural segment in which they are classified.

- Where it is physically impossible to transmit the information requested by exercising the right of access, the site must give reasons in a way that is precise and intelligible to the layman.

9. Privacy enhancing technologies

- Web sites should undertake to implement on their server platform, as soon as they are available and have been tested, privacy enhancing technologies (PETs) integrated in the browsers wherever these solutions can ensure compliance with the above suggestions and permit users to define and correct on a case-by-case basis, the delivery of their personal data according to the different categories of possible recipients.

10. Responsibility

- All Web sites collecting personal data should formally state their acceptance of full responsibility for the security and confidentiality of the data, and for statements of intent or contractual commitments with regard to the data and the processing of that data.

ANNEX 2

STUDY ON PRIVACY PROTECTION PRACTICES CARRIED OUT ON A SAMPLE OF WEB SITES IN VARIOUS OECD MEMBER COUNTRIES

Methodology of sample selection

Given the conditions in which the study was carried out and the time available to do it (1 month), it was not possible to compile a sample of Web sites that was statistically significant and representative of sites world-wide.

The approach adopted was therefore completely different from previous or on-going initiatives in the same area, in particular the Electronic Privacy Information Center (EPIC) study, which focused on 100 hot sites, and the review currently being conducted by the Federal Trade Commission (FTC) in the United States of 1 200 Web sites.

It was decided that the study should focus on commercial sites that exhibited satisfactory data protection practices, with a view to achieving three objectives:

- to show that there is no inherent conflict between on-line commerce and privacy protection;
- to illustrate and give prominence to the good practices identified;
- to analyse shortcomings and to suggest an ad hoc level of protection that should be generally achievable.

The first problem was to decide the minimum criteria for including a site in the sample. Given the tight deadline, some very popular sites cited by the Top 100 Web Sites (100hot Web Sites, Web21) were included in the sample, as well as sites proposed by specialists (data protection experts or authorities) from OECD Member countries which were of particular interest from the standpoint of personal data collection and processing.

Three criteria were adopted:

Criterion No 1: commercial sites

The study focused on private-sector commercial sites which offer on-line sales or collect personal data on-line, irrespective of the type of goods or services offered.

Criterion No 2: sites located in various areas of the OECD

Although the majority of commercial sites are still North American, [one of]the aim[s] of the study was to show how the approaches to data protection in various OECD Member countries were or were not reflected in the design of the sites and in the nature of the customer relationship. It was therefore essential to incorporate in the sample commercial sites from different OECD Member countries.

Fifty sites were therefore selected according to the following geographical breakdown:

United States:	23 sites
Canada	5 sites
European Union, of which: - Germany 1 - Denmark 1 - Spain 2 - Finland 2 - France 6 - Italy 2 - United Kingdom 2 -	16 sites
Japan	2 sites
Australia	3 sites
Mexico	1 site

Criterion No 3: sites offering various goods and services

Most commercial sectors, even the most unexpected ones, are to be found on the Internet, and the study does not purport to cover all of them. Instead, it focused on four main categories of site:

- Commercial sites which have enjoyed spectacular growth thanks to the Internet, and for which the Internet is becoming the main means of doing business. These very busy sites were the most likely to have put in place privacy protection arrangements for their customers. Three sectors were picked out:

  – computer equipment sales
  – software sales
  – book and record sales.

- Sites with significant commercial potential on the Web, and which have traditionally used sophisticated direct marketing techniques. Three sectors were picked out:

  – tourism
  – air travel ticket sales and reservations
  – finance.

- Sites offering products or services, the nature of which may be more or less indicative of the customer's personal situation. Three series of commercial sites were selected:

  – on-line newspapers and magazines
  – games
  – Internet services such as e-mail and on-line advertising.

- Shopping sites (usually malls) open to the general public. Two sectors were picked out:

  – textiles, clothing and accessories
  – sports goods and toys.

Selected Samples

Country	Name	URL	Description	Language
Australia	Fairfax@Market	http://www.market.fairfax.com.au/	Classified ads	Engl
Australia	Qantas	http://www.qantas.com.au/	Airline	Engl
Australia	Traveland	http://www.ansett.com.au/traveland.html	Travel services	Engl
Canada	Royal Bank	http://www.royalbank.com/	Bank	Engl Fr
Canada	Globe & Mail Employment service	http://careers.theglobeandmail.com/	Newspaper employment service	Engl
Canada	Mountain Equipment Co-op	http://www.mec.ca/	Outdoor equipment supplier	Engl
Canada	Hudson's Bay Co.	http://www.hbc.ca	Trading	Engl Fr
Canada	CANOE (CANadian Online Explorer)	http://www.canoe.ca	News, entertainment	Engl Fr
Denmark	Lego	http://www.lego.com	Toys	Engl German Danish Fre
Finland	Iltalehti	http://www.itlalehti.fi	Newspaper	Finnish
Finland	VIP Hiusklubi	http://www.hairstore.fi/~vip/	Hair products	Finnish
France	Decathlon	http://www.decathlon.com	Sporting goods	Fre Engl
France	CPR Bourse	http://www.cprbourse.tm.fr/	Financial svcs.	Fre Engl (only welcome)
France	Société Générale	http://www.socgen.com	Banking svcs.	Fre Engl (incomplete)
France	FNAC	http://www.fnac.fr		Fre
France	CNP	http://www.cnp.fr	Insurance / savings inst.	Fre
France	Les Echos	http://www.lesechos.fr	Newspaper	Fre
Germany	Der Spiegel	http://www.spiegel.de	News	German
Italy	Mollificio Lamperti Srl	http://www.lamperti.it/	Coil springs manufacturer	Italian
Italy	Ego	http://www.ego1997.com	Clothing	Engl
Japan	Japan Catalogue (Mitsubishi)	http://www.japan-cata.com	Japanese products	Japanese
Japan	G-Square	http://www.gsquare.or.jp	Info. svc. provider; on-line shopping	Japanese
Mexico	Infosel	http://www.infosel.com.mx/	News service	Spanish
Spain	Banesto	http://www.banesto.es/	Bank	Spanish Engl
Spain	El Corte Inglés	http://www.elcorteingles.es	Retail	Spanish
United Kingdom	Financial Times	http://www.ft.com	Newspaper	Engl
United Kingdom	Economist	http://www.economist.com		Engl
United States	3M	http://www.mmm.com		Engl
United States	Amazon	http://www.amazon.com	Book seller	Engl
United States	ATT	http://www.att.com/	Telecom	Engl
United States	Barnes and Noble	http://www.BarnesandNoble.com	Book seller	Engl
United States	Nashbar	http://www.nashbar.com	Bikes / volleyball eqpt.	Engl
United States	CDNow	http://www.cdnow.com	Music	Engl
United States	CNet	http://www.cnet.com/		Engl
United States	Double Click	http://www.doubleclick.net/	Internet advertising	Engl Jap Span Fre Port Ital Swed
United States	Excite	http://www.excite.com/	Search	Engl Dutch Fre German Swed Jap
United States	First Virtual	http://www.firstvirtual.com/	E-messaging	Engl
United States	Galoob	http://www.galoob.com	Toys	Engl
United States	IBM	http://www.ibm.com/		Engl
United States	Infoseek	http://www.infoseek.com	Search engine	Engl Fre Port Dan Ger

				Spa Ital Jap Dutch Swe
United States	Intel	http://www.intel.com	Microprocessors	Engl (+ others)
United States	McGraw-Hill	http://www.mcgraw-hill.com/index.html	Publishing	Engl
United States	Microsoft	http://www.microsoft.com		Engl
United States	National Credit Information Network	http://www.social-security-number.com/ncihome.htm	Credit reporting	Engl
United States	NBC	http://www.nbc.com	TV	Engl
United States	Netscape	http://www.netscape.com		Engl
United States	Travelocity	http://www.travelocity.com/	Travel services	Engl
United States	HotWired	http://www.hotwired.com		Engl
United States	Yahoo	http://www.yahoo.com	Search engine	Engl Jap Ger Swe Dan Fre Kor
United States	Experian	http://www.experian.com	Credit reporting	Engl

	YES	NO	No answ.
1) DOES THE SITE REFER TO OR UTILISE ANY OF THE FOLLOWING:	**24**		
Specific Laws And Other Legal Instruments			
International Instruments (e.g. EU Directive)			
National Laws			
Contractual Agreements			
Self Regulation And User Empowerment Technologies			
Compliance with Specific Codes of Conduct or Guidelines:			
Government Model Codes			
Industry Codes			
Auditing and Certification			
TRUSTe			
Audits by Accounting Firms			
BBBOnline			
Personal Preference Settings and Labelling			
P3P (formerly OPS)			
PICS			
Personal Data Control Technologies			
Digital certificates			
2) DOES THE SITE SET "COOKIES"?	**31**	**19**	**0**
If so:			
a) Are the cookies being set by the site itself or by an advertising entity?	*Itself: 22. Both: 7.*		
b) What is the [average] expiration date of the cookie(s)?	*End 1999 (20 months)*		
c) How many times does the site attempt to set cookies?	*10 or more (often at each link).*		
d) Can you enter the site if you refuse the cookie?	29	1	1
3) DOES THE SITE ASK VISITORS TO SUPPLY PERSONAL DATA THROUGH THE USE OF REGISTRATION FORMS, ORDER FORMS, MAILING LISTS, QUESTIONNAIRES OR SURVEYS, AND/OR REQUESTS FOR FEEDBACK OR COMMENT?		**3**	
a) What specific personal information is requested?	*Name, address, e-mail.*		
b) Does the site offer free information or services in exchange for personal data?	28	18	4
c) Is the information requested proportional in value to the information or services received or necessary to complete a specific transaction (e.g. home address for delivery)?	32	7	11
d) Is any of the information requested optional?	29	7	14

	YES	NO	No answ.
4) DOES THE SITE HAVE A PRIVACY POLICY?	**38**	**11**	**1**
If so,			
a) Is information about the Privacy Policy available online? (Please print a copy.)	38	2	10
b) Is it easy to find?	28	10	12
i) is it accessible from the homepage?	21	17	12
ii) if not, is it found as a "key word" using the site's search engine?	5	8	37
5) IS NOTICE GIVEN CONCERNING THE TYPES OF PERSONAL INFORMATION COLLECTED?	**28**	**17**	**5**
6) IS NOTICE GIVEN REGARDING THE COLLECTION OF E-MAIL ADDRESSES OR OTHER PERSONAL INFORMATION COLLECTED AUTOMATICALLY FROM A VISITOR'S BROWSER?	**15**	**33**	**2**
7) IS NOTICE GIVEN CONCERNING THE USE OF THE PERSONAL INFORMATION COLLECTED?	**39**	**9**	**2**
8) CAN VISITORS REFUSE AND/OR "OPT-OUT OF" CERTAIN USES OF THEIR PERSONAL INFORMATION?	**26**	**18**	**6**
9) CAN INDIVIDUALS ACCESS THEIR PERSONAL INFORMATION FOR VERIFICATION AND CORRECTION ?	**28**	**17**	**5**
If yes, briefly describe how (i.e. online mechanisms; off-line contact information)			
10) DOES THE SITE OFFER GOODS OR SERVICES FOR PURCHASE?	**34**	**15**	**1**
If so,			
a) Does the site offer a secure electronic payment mechanism?	28	7	15
Mostly secure server.			
b) What specific personal data is requested during the payment process?	*Name, address, e-mail, credit card (# and expiration date).*		
11) DOES THE SITE MENTION THE USE OF SECURITY MEASURES, EITHER AT THE POINT OF PAYMENT, OR AS PART OF A PRIVACY POLICY OR A SEPARATE "SECURITY STATEMENT"? (This could include operational or managerial measures, the use of encrypted data storage or transit, or securing payment).	**27**	**16**	**7**
12) DOES THE SITE DISPLAY A PRIVACY ICON OR TRUSTMARK?	**4**	**43**	**3**
13) DOES THE SITE GIVE INFORMATION ABOUT INTERNAL OR EXTERNAL AUDITING PROCEDURES?	**4**	**41**	**5**
14) DOES THE SITE REFER OR LINK TO A DATA PROTECTION REGISTRATION BODY OR OTHER INDEPENDENT REGULATORY BODY?	**7**	**40**	**3**
	1/4 of European sites; 1/8 for US.		

	YES	NO	No answ.
15) DOES THE SITE CLEARLY GIVE INFORMATION ABOUT RECOURSE IN THE CASE OF DISAGREEMENT? (If so, briefly describe.)	**10**	**34**	**5**
16) IS RESPONSIBILITY FOR COMPLIANCE WITH PROVISIONS OF THE PRIVACY POLICY SPECIFIED?	**7**	**34**	**9**
17) IS A PHYSICAL ADDRESS GIVEN FOR CONTACTING THE SITE?	**36**	**12**	**2**
18) IS AN EMAIL ADDRESS GIVEN FOR CONTACTING THE SITE?	**50**	**0**	**0**