

RECOMMENDATIONS
FOR INTERNET USERS

CONTENTS

1. <i>Introduction.</i>	3
2. <i>This Document's Structure.</i>	4
3. <i>Principles of Data Protection.</i>	5
4. <i>World Wide Web.</i>	5
4.1. <i>Description of the Service.</i>	5
4.2. <i>Profiling.</i>	6
4.3. <i>Global Availability of Personal Data.</i>	7
<i>Recommendations.</i>	8
5. <i>E-mail.</i>	9
5.1. <i>Description of the Service.</i>	9
5.2. <i>E-mail Address Collecting.</i>	10
5.3. <i>Privacy in Communications.</i>	100
<i>Recommendations.</i>	111
6. <i>Electronic Forums.</i>	122
6.1. <i>Description of the Service.</i>	122
6.2. <i>User Identification.</i>	133
6.3. <i>Profiling.</i>	144
<i>Recommendations.</i>	144
7. <i>Electronic Commerce.</i>	155
7.1. <i>Description of the Service.</i>	155
7.2. <i>The Electronic Money Trail.</i>	155
7.3. <i>Security in Electronic Transactions.</i>	166
7.4. <i>Profiling.</i>	166
7.5. <i>Advertising.</i>	177
7.6. <i>Mobile E-commerce.</i>	1818
<i>Recommendations.</i>	18
<i>Summary of Recommendations.</i>	199
<i>Glossary of Terms.</i>	23

1. Introduction.

Spain's Organic Law 5/1992 of 29 October regulating the computer processing of personal data created the Data Protection Agency as an independent body charged with seeing to the law's enforcement. In 1999, to conclude the transposition into Spanish legislation of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection on individuals with regard to the processing of personal data and on the free movement of such data, Organic Law 15/1999 on the protection of personal data (abbreviated as the LOPD)¹ was enacted, *'intended to guarantee and protect the public liberties and fundamental rights of natural persons, and in particular their personal and family privacy, with regard to the processing of personal data'*. The Data Protection Agency is the independent agency that remains entrusted with supervising the correct application of the law.

Because of this responsibility, the Agency takes a special interest in tracking all new technological developments that might affect the use of citizens' personal data and citizens' fundamental right to personal-data protection². The right to personal-data protection is defined in crystal-clear terms by Spain's Constitutional Court in Sentence 292/2000³, which states that the right *'is not restricted entirely to a person's private data, but includes any kind of personal data, private or otherwise, whose knowledge or use by third parties may affect the person's rights, fundamental or otherwise. This is so because the object [of the right] is not just individual privacy (for that, we have the protection furnished under article 18.1 of the Spanish Constitution), but personal data. Therefore, it also encompasses those public personal data that do not, merely because they are public, merely because they are open to being known by anyone, lie beyond the affected person's power of disposal, thanks to the guarantee afforded by the affected person's right to data protection. Also for that reason, the fact that data are personal does not mean that only data concerning the private or intimate life of the person are protected; rather, the data protected are*

¹ The full text of the LOPD and all the rest of Spain's data-protection legislation can be found at <https://www.agenciaprotecciondatos.org/datd.htm>. The Data Protection Agency provides more information and services as well over its web server, <https://www.agenciaprotecciondatos.org/>.

² In this document, the terms 'data protection' and 'privacy' are held to mean the same thing.

³ Available at <http://www.tribunalconstitucional.es/STC2000/STC2000-292.htm>.

all data that identify or enable the identification of the person, could be used to profile the person ideologically, racially, sexually, economically or in any other fashion, or serve for any other use that under certain circumstances constitutes a threat to the individual'.

So, it is this interest that drove the Data Protection Agency to publish the first version of its Recommendations for Internet Users in 1997 and has since led the Agency to update its advice here, in the second version of its Recommendations.

The situation the Recommendations were originally created to respond to has not changed; there are no legal regulations on the Internet protecting user privacy on the worldwide scale yet. It is, however, feasible, even on the globalised stage where today's new virtual society goes about its business, to minimise the risks, if we have a good understanding of how things work.

The fundamental objective of this document is therefore to make you as an Internet user aware that your personal data may be used in shady ways, and that you have in your grasp certain mechanisms that can help you get honesty and transparency in how your personal data are collected and processed.

Nevertheless, we don't want to alarm you unduly about how the Internet is used. Although there may be some problems with the Net, as we shall see, it is also an incredibly useful, versatile tool for an endless number of activities.

2. This Document's Structure.

These recommendations are designed for immediate practical use. We begin, therefore, with a short list of the principles of data protection and then go on to describe what main services the Internet provides, how to identify the possible risks to privacy that Internet use can involve and what recommendations we have for users.

At the end of the document is a summary of our recommendations and a short glossary defining the technical terms we have used.

3. Principles of Data Protection.

Spain's Data Protection Act⁴ establishes that citizens have the right to know what personal data of theirs are being held in another person's files and the right to have their data corrected or deleted under certain circumstances, especially when the data are inaccurate or false⁵.

That is why data-file controllers must inform you of their identity and address, the purpose they are collecting your data for and how you can exercise the rights mentioned in the paragraph above.

Furthermore, generally speaking, your personal data can only be processed with your consent, in pursuit of the legitimate purpose for which the data were collected. This idea is called the principle of consent, and it also applies when your data is transferred to third parties.

These foundations are also discussed in other rules and directives of the Council of Europe, the European Union, the OECD and the UN.

4. World Wide Web.

4.1. Description of the Service.

The *World Wide Web* service (known as the *WWW*), while very complex inside, is extremely simple to use. On one side, there are web servers made up of structured information in the form of documents called 'pages', which look like the pages of a book or encyclopaedia. On the other side, there are users like you, who use computer programs called *browsers* to see these pages. Each page on the Net is assigned an address that belongs exclusively to that page alone, and each page is designed and defined by means of a highly versatile language called *HTML*, which allows text, pictures, sound, video and hypertext to be placed on the page.

⁴Although, as we said before, there is no global regulation, that shouldn't make us lose sight of the fact that if Internet processing of personal data takes place on Spanish soil, it is subject to Spanish data-protection legislation, and therefore its controllers are specifically obliged to provide the information, respect the consent and facilitate the exercise of the rights established in the Organic Act on the protection of personal data.

⁵The right to consult the General Data Protection Registry, the right of access, the right of rectification or cancellation and the right of objection that appear in Title III of Organic Act 15/1999.

Hypertext is a special kind of text that links the document you are looking at with other pages all over the Net. To see one of these linked pages, all you have to do is select the text that represents the link, and the new page is transmitted automatically from the *web server* to your computer. You can do this again and again, an infinite number of times, leaping from one page to another in what is known in Net slang as surfing. In addition to retrieving information, the WWW service allows data to be exchanged between users and web servers.

Next, let's take a look at the problems the WWW service may entail from the data-protection standpoint.

4.2. Profiling.

When we visit web servers, we may be asked for all kinds of personal data before we are allowed to use a service or purchase a product. These data may range from a simple request for an e-mail address to a complete survey asking for our name, address, income, hobbies, and other personal information.

We have to be aware that these data can be used for purposes other than the ones they were gathered for, including but not limited to personalising advertisements so they will appeal especially to us, tracking our interests and hobbies and marketing our personal data to third parties.

It is also possible that the visits we make to web servers may be tracked in greater detail without our knowledge, for example, by using what are called *cookies*⁶, tracing our *clickstream* with conventional tools and *webmining*.

Another thing we have to bear in mind is that sometimes, if we refuse to allow a *cookie* into our computer, the service provider may refuse to let us use certain features of its product or service, or may even refuse to allow us to use its service altogether.

⁶All terms in cursive are defined in the Glossary.

A respectful user-privacy policy ought to inform users when *cookies* are saved or placed in their computers, how to prevent *cookies* from entering and what consequences might stem from refusing *cookies*.

In addition, in recent times a new generation of programs known as *ET applications* has begun to proliferate. These programs generally install themselves in a user's browser and, dangling as bait the offer of enhanced surfing (for instance, interesting web sites related with the one the user is looking at, more information about the site the user is visiting, recommendations about certain products or comparative advice, etc.), they send huge quantities of data about the pages the user has visited and the user's shopping habits 'home' to their owners or creators.

On other occasions, these kinds of programs install themselves surreptitiously and remain active, even when the program they used to enter the user's computer has been removed, and send information 'home' to their creators about, for instance, the advertisements their unwitting hosts click on.

4.3. Global Availability of Personal Data.

The Internet is by definition a global network. That means once data leave your computer, you have no way of knowing what route they take to get to their destination, at what points along the way they are temporarily stored or who might gain access to them, copy them, change them and use them for a purpose other than the one you volunteered them for.

For an example, when a set of data is sent from one Spanish city to another, it might easily travel through one or more foreign countries under different levels of guaranteed personal-data processing security (in some cases, no security at all).

Therefore, in a raft of cases, when the rights acknowledged in Spanish law are violated, it can prove very hard to pin responsibilities clearly to the different data-communication agents involved (*access providers, content providers, net operators, etc.*).

Recommendations

- *Be aware of what personal data you provide or post on your personal pages, and who you provide it to. You might find the information listed under 'Who we are' or 'About us' on many web pages helpful. Also, try to give only those personal data that are strictly necessary. Share this recommendation with everybody in your family who uses the Internet.*
- *Whenever you can, use the latest versions of browsers, because the new ones are starting to incorporate a number of improvements giving you more control over the personal data exchanged between the server and your computer. Consider the possibility of configuring your browser's features to provide you with more protection, and don't assume that the default values that come with the product are the best for protecting your privacy. For example, in some programs you can activate options that alert you to undesired data exchanges, especially cookies.*
- *If you like, there are several programs on the market that can help you manage the cookies that are installed in your computer and decide which ones you want to keep or throw away.*
- *Use the legally available security mechanisms within your reach (secure web servers, cryptography, electronic signatures, etc.) to protect the confidentiality and integrity of your data when you need to.*
- *When you surf the Internet, be aware that the web servers you visit may register which pages you visit, how often, and what subjects you're looking for, even if they don't inform you of the fact. If you don't want to leave a record of your activities, use tools and servers that keep your identity safe, generally by giving you a pseudonym (which some countries' laws could require the server to reveal under certain circumstances).*

- *When you download programs from the Internet, try to inform yourself, from the most reliable source you can find, about the creators and features of the programs, and don't take them if you suspect they may have their own hidden agenda.*
- *Remember that if you share your computer with other people, the pages you have visited and the data you have accessed are easily accessible to the computer's other users, unless you take certain precautions. You can use your browser's options to delete the 'History' of the sites you've visited and the 'Temporary Internet files' where the pages you've visited are stored.*

5. E-mail.

5.1. Description of the Service.

E-mail or interpersonal messaging is the most widely used Internet service. It enables net users to create and send messages to each other without having to be connected at the same time⁷.

In e-mail service, there's nothing to guarantee that messages will always reach their destination, nothing to guarantee that the sender is informed when messages fail to get where they're going and nothing to guarantee that the sender is who he or she claims to be.

Basically, anybody who wants to use e-mail needs an e-mail client program (a program installed in his or her PC), an e-mail address (e-mail account) and an Internet connection.

E-mail addresses consist of two parts separated by the @ symbol, such as juan.español@cualquiersitio.es or NC1452@cualquiersitio.com. The part to the right of the @ identifies the *domain* where the user has an account with

⁷Since e-mail service is given free by a large number of Internet servers and allows e-mail to be managed from any computer in the world that's connected to the Net, the use of e-mail service through web pages (known as *webmail*) has been spreading lately. Webmail's main advantage, apart from its universal accessibility, is that even if you change Internet access providers, you can keep the same e-mail address. Since *webmail* is based on the *World Wide Web* service, it compounds the risks inherent in the WWW with the risks of address collection and lack of message confidentiality that are discussed below.

a mail server. The part to the left of the @ is the user's own unique identification or user code; it is the name by which the e-mail server identifies the user. There is no law or technical need requiring it to be the user's real name; it could be a pseudonym chosen by the user or an arbitrary code assigned by the e-mail server when the user registers for e-mail.

There are two kinds of risks to personal data in e-mail. The first has to do with the collection of identifying data and *profiling*, and the second concerns the preservation of privacy in communications.

5.2. E-mail Address Collecting.

Remember, an e-mail address is the most common way of registering a person's 'identity' on the Internet, and it's usually employed as the foundation for accumulating information about the person. Often it contains information about the person, such as the person's surname, employer or country of residence. This address is used in a great number of spots on the Net and can be obtained easily without its owner's knowledge (Some programs include code for transmitting the customer's e-mail address without letting the customer know; some browsers have security loopholes that allow a web site to find the e-mail addresses of its visitors; there are public areas on the Internet where addresses can be obtained, etc.). When data are included in *directories* of people (like X.500 directories) without proper security measures, that data becomes vulnerable to being collected without the knowledge of the data subjects and used for other purposes.

5.3. Privacy in Communications.

At the present state of the art, all the services we have discussed so far fail to provide a generalised means of establishing the identity of the sender and the receiver, which is known as *authentication*. Exchanges of information do not ordinarily include mechanisms that guarantee *confidentiality*, either. For these reasons, you must be alert to the risks of false identity and violation of the secrecy of communications.

Recommendations

- *Whenever you can, choose an e-mail user name that does not reveal anything about you. An unstructured set of upper-case and lower-case letters, numbers and symbols would be a good choice.*
- *To access your e-mail account, in addition to giving your user code, you usually have to enter a password. Pick a password that isn't a word in the more widely-used languages (again, a random combination of upper- and lower-case letters, numbers and symbols is a good choice), and change it periodically. Don't use the 'save password' option that sometimes appears to save having to re-enter your password every time you go on line.*
- *If you don't want your e-mail address to be public, set up your browser so that it won't give your address to the web servers you access.*
- *Internet e-mail isn't secure. Messages and chat rooms can be intercepted and faked. People who send you messages can turn out to be impostors. There are encryption devices on the web, sometimes free of charge, that let you exchange information confidentially, and there are relatively reliable e-mail authentication mechanisms (PGP, the PEM standard, etc.). You can use these mechanisms to make it a lot harder for others to attack your message confidentiality and integrity and set themselves up as impostors.*
- *Before you give out data, it's a good idea to remember that both your e-mail address and the rest of the personal data (name, interests, hobbies, etc.) you give when you want to be included in a directory or mailing list could be collected and used without your knowledge for purposes different from the ones you intended.*

- *Also, remember, at least in the EU, you can ask to have your personal data left out of publicly available telecommunications service guides that list e-mail addresses, and you can ask for your personal data not to be used for direct sales. Furthermore, guides of this sort can include only the data absolutely indispensable for identifying you. They have to get your consent before they can include any additional data.*
- *Be aware that when you send e-mail to a number of persons, you're showing all the addresses you've typed in the 'To' or 'Carbon copy (CC)' field to all the recipients of your message. To avoid this, you can put the message's recipients in the 'Blind carbon copy (BCC)' field, so that nobody who receives your message can get hold of the e-mail addresses of the other recipients.*

6. Electronic Forums.

6.1. Description of the Service.

Mailing lists. These are services based on e-mail. Groups of people sharing a common interest in a specific subject get together, and they exchange information about their subject via e-mail. Any message sent to the list is automatically distributed to every member on the list and sometimes could even be made public to people not on the list.

Newsgroups, Netnews, News or Usenet . All these names refer to a global mailing system that enables discussion groups to be created about topics of interest. Each newsgroup is arranged into blocks of topics organised hierarchically, such as 'comp' (computers), 'soc' (topics of social interest), 'biz' (business topics), 'alt' (alternative groups) and other groups united by geography or sector. There are different programs for accessing these discussion groups, although the leading browsers tend to come with programs of this sort. Sometimes e-mail addresses can be accessed through them, in which case they are, in a practical sense, mailing lists.

Chatting. This is a service that lets a number of users 'talk' to each other simultaneously over the web. To chat, you connect to a server where you choose a chat group or channel. Each participant is introduced to the others by a pseudonym or *nickname*. Voice conversation and videoconferencing can be used in addition to written messages, if the program is prepared for those options.

There are three main types of chatting on the Internet: Internet relay chat (*IRC*), web page chat and *ICQ* ('I seek you') chat.

The first, *IRC*, is the original electronic chat. It uses a protocol that allows users to communicate in real time, either publicly in a forums holding an indeterminate number of people, or privately with a single person to talk to. Like newsgroups, chat rooms vary according to topics, but they're different from newsgroups because their channels are shut down when the discussion is over.

Web page chat lets people communicate with each other without having to get a separate program; the only tool they need is a modern Internet browser. Though a web page chat is very easy to use, its features are limited, because you can only exchange text and you cannot personalise the different elements of the chat interface.

ICQ is a tool that lets you know when 'your' people (a set of people you have put on your list of personal contacts) go on or off line. *ICQ* also lets you contact them and exchange messages with them while you are surfing the Net. To do this, all participants have to be using *ICQ*. You can instruct the program to tag you as 'invisible', 'away' or 'extended away'.

6.2. User Identification.

Even though you use *nicknames* while chatting, most chat servers require participants to register first. When you register, you are asked for a series of personal data (going into varying degrees of detail, depending on the specific server or forum).

The main reason participants are required to identify themselves is to cover the service provider's potential legal liability in case anyone were to

distribute illegal contents or voice opinions that could lead to legal problems in certain countries and circumstances (slander, libel, broadcasting of messages encouraging violence or racial hate, etc.). This way, if the situation arises and the authorities show the service provider the correct legal requirements (such as a court order or warrant), the service provider can identify the perpetrator. In addition, if the information people exchange while chatting (in the form of text, voice or picture) is saved and stored by the server, it can also be accessed. Under certain circumstances, this is still true even if you use a pseudonym.

In mailing lists and newsgroups, identification is mainly done through your e-mail address and the details about yourself that you include in your messages.

6.3. Profiling.

The most disturbing thing about participating in discussion forums is that somebody could create a personal profile of you (topics that interest you, your political leanings and sexual orientation, etc.) on the basis of what mailing lists you belong to or what discussion groups you participate in. You run the risk of being labelled according to the company you keep.

There are also publicly available search tools that, for instance, allow a user to find out all the contributions you've made to all the groups you've ever participated in.

Recommendations

- *When you participate in discussion forums or mailing lists, remember that what you say is public and will be accessible for a long time, so the opinions you voice could eventually be misinterpreted or misused. To avoid this problem, there are mechanisms available on the Net (primarily what are known as re-mailers) that let you use e-mail anonymously and participate anonymously in discussion groups.*

- *In addition, your discussion forums may have an option available that keeps your messages from being saved in the history files if you type X-No-archive:yes in the heading of your message. This command limits the public availability of your message.*
- *If you don't want to be identified in a chat, when you set up the chat program, leave the fields about your real self blank whenever you can.*
- *If you'd like to remain unseen by the users of other channels or change your nickname, you can use invisibility commands that block others from 'seeing' you.*

7. Electronic Commerce.

7.1. Description of the Service.

What we mean by 'electronic commerce' or 'e-commerce' here is any commercial transaction made over the Internet with individuals as a party.

7.2. The Electronic Money Trail.

Certainly one of the best ways you have of preserving your privacy in traditional commerce is to pay for the goods or services you want with cash. Cash payment deprives the seller of any need to know who you are. On the Internet, things are different. First of all, unless you buy digital goods you can download directly from the Net (such as computer programs or music or films in electronic format), you've got to give a name and address for the product to be delivered to. In addition, nowadays the most widely used means of payment is the credit card, so anonymity in Internet shopping is in practice extremely hard to get. The personalised information you provide as proof of identity can be used —by the provider or by third parties the provider transfers, rents or sells information to— for purposes that have nothing at all to do with your commercial transaction.

7.3. Security in Electronic Transactions.

Another concern you as an Internet user should have when you engage in non-anonymous commercial transactions is to make sure the data you furnish for the transaction (such as your name, address and credit-card number) are not picked up in transmission by anyone but the provider you want to do business with, so nobody can pose as you later and make improper use of your data. On the other side of the equation, the provider or vendor must make sure you are truly who you claim to be, a real end consumer or a genuine middleman.

These are the features that define a secure transaction system:

- It uses *encryption* to guarantee the *confidentiality* of electronic commercial transactions, so that the data contained in each transaction can only be accessed by the parties to that transaction.
- It uses *electronic signatures* to guarantee transaction *integrity*, so that the transaction's content cannot be changed by third parties from outside without being discovered.
- It uses *electronic signatures* and certification to guarantee the authenticity of both the owner of the means of payment and the provider. *Electronic signatures* guarantee the *integrity* of the transaction. Certification by a *TTP (trusted third party)* guarantees the identity of the parties to the transaction.

7.4. Profiling.

On the Internet, your behaviour as a consumer can be 'monitored' by a provider, who can accumulate personal information about your tastes, preferences and behaviour without your every knowing. These data are collected by recording information about what web servers you go to, what pages you spend more time at, what topics you search for regularly,

what products you buy and even what products you don't buy⁸. This way quite a complete user profile can be built up without your knowledge.

There are ways you can keep this from happening. Perhaps one of the methods that's been most successful with users is the use of servers and programs that let you surf the Internet anonymously. The system works like this: First, you go to a server that specialises in anonymous browsing, and it gives you a new identity you can use to access other servers. This way, the web servers you access cannot find out who you really are.

7.5. Advertising.

Advertising is tied in closely with all kinds of commerce, and electronic commerce is no exception. On the Internet, advertising can take many different forms, from e-mail containing *push advertising*⁹ to *banners*, *interstitials* and *pop-up windows* that appear on your screen while you are surfing the Net.

Of course, sending advertising messages by the first method, e-mail, requires a knowledge of the recipient's e-mail address. Advertisers can get addresses from users themselves who want to receive information of interest to them, or advertisers may obtain addresses without users' knowledge through:

- Mailing lists and newsgroups.
- E-mail *directories* that give out addresses.
- Sale, rental or exchange of e-mail addresses by *access providers*.
- Surrender of e-mail addresses by browsers in certain situations when they are communicating with web servers.

⁸One of the most widespread shopping systems is the metaphor of the shopping trolley: The different products you decide to buy are put into a virtual trolley like the ones you use in supermarkets. This 'virtual trolley' is a *cookie*, and sometimes the information about the products you eventually decide not to buy (the ones you would end up putting back on the shelf in real life) is kept, and those are the first products you're shown the next time you go on line.

⁹This may be in the form of solicited or unsolicited e-mail. If it is unsolicited, the message is what's so famously known as *spam*.

- Receipt of e-mail messages that require the user to answer at a given address and ask the user to 'spread the word'.

The second type of message, no matter what form it takes, is closely linked to how web pages are displayed. It may show commercial information in specific areas of the web page that's on screen, or it may open up new windows to display advertising, taking advantage of downloading time or the transition time between different pages.

Often the specific advertisement you receive when you're on line depends on what prior information (profile) the sender has on you¹⁰, which the sender can have got hold of in a variety of ways, as we've described here.

7.6. Mobile E-commerce.

In addition, a new form of commerce is appearing now, mobile e-commerce. This is shopping not from a PC in an office or a home, but over a new generation of portable mobile devices that use new protocols affording secure access to e-mail and web pages. As a result, there is the possibility that traffic and location data generated by mobile access (such as travel patterns) may be added in with the rest of the transactional and surfing data currently processed to paint a much more accurate consumer profile.

Recommendations

- *Use electronic money systems that keep your Internet shopping habits anonymous whenever they are available and you think it would be to your advantage.*
- *Don't engage in electronic commercial transactions over providers with non-secure or unreliable systems. Your browser can recognise when you've connected to a server that admits secure transactions. Check your browser's manual to find out*

¹⁰This is often not the server handling the pages you're connecting to, but a third party, generally an advertising agency that posts online advertisements.

how it reports connection to a secure web server, although in the most widely used browsers, this kind of connection is indicated by a padlock or unbroken key that appears somewhere on the screen.

- *When you put your e-mail address in a directory or mailing list, consider the possibility that third parties may get a copy and send you messages you don't want to receive.*
- *Find out the data rental, sale and exchange policy of your Internet access provider and the administrators of the directories and mailing lists you belong to.*
- *Try to volunteer only the personal data absolutely necessary for obtaining the service or product you want to receive.*
- *Carefully read the data-protection information the seller provides, and check the company's 'Data Protection or Privacy Policy' if it's available.*

Summary of Recommendations

Data Collection

- *When you give any organisation (access providers, content providers, e-commerce vendors, etc.) personal information about yourself, be aware who you are furnishing your data to and what for. Also, try to volunteer only as much personal data as strictly necessary.*
- *Try to find out what policy your providers and list and directory administrators have about selling, exchanging or renting out the data people give them. Ask them to separate your personal data from your Internet access identification.*

- *When you surf the Net, be aware that the web servers you visit can record both the pages you visit often and the topics or subjects you look for, even if you don't tell them, and then use that information to profile you. If you don't want to leave a record of your activities, use tools and servers that keep your true identity safe, generally by letting you go by a pseudonym that someday might, in certain circumstances and under certain countries' laws, have to be revealed.*

Purpose of Data Collection

- *Get suspicious if you're asked to furnish data that go beyond the stated purpose or are unnecessary for the service you're getting.*
- *Bear in mind that, when you enter your e-mail address in a directory, mailing list or newsgroup, your address could be picked up by third parties and used for a different purpose, such as sending you junk mail.*
- *Your membership in certain newsgroups and mailing lists could help others draw up a profile of you, with varying amounts of detail. If you can get access to options that prevent your contributions to newsgroups from being stored indefinitely, use them.*
- *If you don't want to leave a trail on the Net, use the mechanisms we have described above to surf anonymously.*

Security and Confidentiality

- *Whenever possible, use the latest version of browsers, because each generation incorporates better security measures. Consider the possibility of activating options that alert you to undesired data exchanges, and don't fill in any data you don't want made public (such as your e-mail address, name, etc.).*

- *Remember, if you share your computer with other people, they can easily get access to the pages you've visited and the data you've used while surfing, unless you take certain precautions. You can use your browser's options to erase the 'History' of the sites you've visited and the 'Temporary Internet files' that store the pages you've accessed.*
- *Whenever you can, choose an e-mail user name that doesn't tell anything about your personality. An unstructured set of upper- and lower-case letters, figures and symbols would be a good choice. In addition, when you have to choose a password, make sure it's not a word in any of the most widely used languages (again, we recommend a random combination of upper- and lower-case letters, numbers and symbols), change it periodically and, at least if you're not the only person using that particular computer to go online, don't use the password-saving option to avoid having to enter it every time you log on.*
- *Don't engage in electronic commercial transactions over providers with non-secure or unreliable systems. Check your browser's manual to find out how it tells you that a connection with a secure server has been established, although in the most widely used browsers, this kind of connection is indicated by a padlock or unbroken key that appears somewhere on the screen.*
- *Remember, although they're not too widely used, there are electronic money systems that keep your Internet purchases anonymous.*
- *Use the security mechanisms within your grasp to protect your data from unwanted access. The most reliable way of doing this is to encrypt your data.*

- *Except when mechanisms are used to provide integrity, authentication and certification (electronic signatures, trusted third parties, etc.), don't blindly believe that any person or organisation that sends you a message is who they claim to be, or that the contents of the message haven't been altered, even though in the immense majority of cases everything is as claimed.*
- *When you download programs from the Internet, try to inform yourself as reliably as possible about the programs' creators and features. Refuse any that you suspect might have a hidden agenda.*

Lastly

- *Whenever you're asked to give personal data that you're not obliged by law to furnish, weigh the benefits you're going to get from the asking organisation against the possible risks of irregular use of your data.*
- *If you have any questions about the legality of the way your personal data are being used, contact the Data Protection Agency (<http://www.agenciaprotecciondatos.org>).*

Glossary of Terms

ET Applications. A kind of spyware program called ET because, once the program has been installed in your computer and found the data it's looking for, it does the same as ET in the Steven Spielberg film: It calls home, that is, it contacts its creator or distributor to report the information it's collected.

Authentication. Procedure for checking a user's identity. Authentication proves that the user accessing a computer system is who they claim to be. Authentication systems are generally based on encryption using a secret, private key or password that only the genuine issuer knows.

Banner. A kind of image used on web pages to advertise some product or service.

Encryption. Transformation of one message into another message, using a key to prevent the transformed message from being interpreted by people who don't know the key.

Clickstream. The trail you leave behind, showing the different web pages you have logged onto. The name comes from the fact that you click to get from one page to another.

Confidentiality. Characteristic or attribute of information that means the information can only be revealed to authorised users at a given time in a given fashion.

Cookie. Set of data a web server sends to any browser that visits it, with information on how the browser has used the server's pages. It gives the IP address of the browser, the addresses of the pages the browser has visited, the address of the page the browser has logged on from, date, time, and so on. This information is stored in a file in the user's computer, to be used on the user's next visit to the same server. What's more, there are servers that restrict the use of certain features of their services or even deny use of their services if the user decides not to let *cookies* into his or her computer.

Cryptography. The science that uses information processing to protect information from unauthorised use and alterations. It uses complex mathematical algorithms to transform information at one end of a communication and turn it back into its original form at the other end.

E-mail Directories. Set of e-mail addresses structured so they can be searched through. An e-mail directory resembles a phone directory, but it has e-mail addresses instead of phone numbers.

Domain or Domain Name. A registered name that identifies an organisation's web site that Internet users can access. For example, **agenciaprotecciondatos.org** is the domain name of the Data Protection Agency.

Electronic Signature. Set of electronic data added to a message to enable the recipient to check the message's source and integrity, for protection against impostors and forgeries. Cryptographic techniques are generally used to generate an electronic signature.

HTML (HyperText Markup Language). Language used to write the documents you can reach over WWW browsers. HTML enables hypertext and multimedia components to be incorporated in documents.

HTTP (HyperText Transfer Protocol). Communications protocol used by WWW servers and client programs to communicate with each other.

Integrity. The guarantee that information is accurate and has not been altered, lost or destroyed accidentally or by intentional fraud.

ICQ (I Seek You). Electronic chat program that can alert you when someone from your predefined list has logged onto the Internet.

Interface. The way two programs interact, or the way people and computer applications interact. For instance, Windows is a graphic interface that makes it easy to handle a PC.

Interstitial. Advertising that appears in the middle of the screen with moving images combined with sound while you are waiting for the web page you are trying to access to download completely.

IRC (Internet Relay Chat). Protocol for simultaneous conversations that lets several people communicate with each other in real time.

PEM (Privacy Enhanced Mail) Standard. Standard applicable to the e-mail protocol used on the Internet, which lets e-mail messages be encrypted automatically before they are sent. With PEM, you don't have to run any separate procedures to encrypt your e-mail.

Net Operator. Public or private body that makes the use of a telecommunications network available.

PGP (Pretty Good Privacy). Freeware written by Phil Zimmermann that uses cryptographic techniques to prevent files and e-mail messages from being interpreted by unauthorised people. It can also be used to sign a document or message digitally and thus provide author authentication.

Pop-up Window. New window that 'pops up' on your screen, generally at a smaller scale than your main window, when you're downloading a certain page.

Push Advertising. Advertising that is sent by advertisers or on advertisers' behalf, but not at the time when the consumer has inquired about the product. It may even be sent without the consumer's ever having inquired about the product at all. One example of push advertising is the new service and product offers that any company or business e-mails to its clients.

Access Providers. Organisations that provide the necessary technical infrastructure to enable users to hook up to the Internet. For home users, the ordinary thing is to use a connection over the basic telephone system, by means of a modem.

Content Providers. People or organisations that publish information of any sort on the Internet, using their own resources or resources provided by an access provider.

Re-mailer. Internet service that uses different techniques to conceal the identity of the person who is sending e-mail.

Web Server. A program that uses http communications protocol to receive requests for information from a client program (browser), retrieve the requested information and send it to the client program to be displayed to the user.

SHTTP (Secure http). System aimed at providing secure transactions in the World Wide Web environment.

SSL (Secure Sockets Layer). The security protocol most widely used on the Internet. It uses asymmetric cryptography to generate a session key, which is used in turn to encrypt communications between the client and the server. It also provides server authentication services and, optionally, client authentication services.

Secure Web Server. A web server that uses security protocols (generally SSL or SHTTP) when transactions are executed over it. A security protocol uses encryption and authentication techniques to increase the confidentiality and reliability of transactions.

Spam. Mass mailing of unsolicited advertising e-mails. People who send spam are called *spammers*.

TTP (Trusted Third Party). Public or private body entrusted with issuing digital certificates that attest to the authenticity of the identity of the certificates' owners.

Webmail. E-mail service rendered over a *web server* using *http* protocol. Webmail is growing, because there is a multitude of service providers that furnish webmail free and because webmail is quite versatile, since you can access your webmail messages from any computer in the world that's hooked up to the Internet. Also, webmail doesn't force you to change your e-mail address when you switch Internet access providers.

Webmining. Techniques that help discover patterns in the way users access web sites. Webmining techniques are used to fine-tune activities like online marketing, the selection of advertising *banners* and *interstitials*, the division of users into segments and customer-relations management. With the support of specific databases, they handle a huge volume of data about web page accesses and *clickstream* data.

World Wide Web (WWW, W3). A distributed information system that uses http protocol to link pages together by means of hypertext mechanisms.

X.500. Standard developed jointly by ISO/IEC (the international standards organisation) and ITU-T (formerly CCITT) using OSI architecture, for the creation and maintenance of directory services in a distributed fashion.

Agencia de Protección de Datos
Data Protection Agency
C/ Sagasta, 22
28004 Madrid
Phone: +34 91 399 62 00
Fax: +34 91 448 91 65
<http://www.agenciaprotecciondatos.org>
e-mail: atencion.ciudadano@agenciaprotecciondatos.org