Privacy

Antonia Paniza Fullana

October 14, 2009

Contents

1 Introduction **2**

2 Regulation **5**

3 Directive on Privacy and Electronic Comunications and Comparative Law **6**

4 Rules about Personal Data Protection **9**

5 Privacy versus Search Engines and On Line Social Networks **11**

Chapter 1

Introduction

The dangers to our privacy are becoming increasingly sophisticated and invisible by the technology progress, so that makes it very difficult to detect for most users. It is almost impossible to know if certain kinds of software capable to obtain information have been installed on our computer. Only with the installation of an specific software you can know if there were a spyware or web bugs, mail bugs... in your computer.

Some words about this kind of software are new, for instance: cookies in flash (or local shared objects). They are a specific type of cookies that are stored on the user's hard drive through applications of flash when visiting a particular website. These cookies, unlike the traditional, can not be viewed or managed browser settings by the user such as cookies that can be called "traditional" nor are stored with them and there are not deleted when you delete the other cookies.

User should be informed about the installation in the computer, as well as how to access the information gathered for possible correction or to delete it. It also raises another problem with regard to privacy: cookies not eliminated, it could collide with the requirements of Laws about data protection, according to which the data will be cancelled when no longer needed for the purpose for which they were collected.

In general, spyware is software that aids in gathering information about a person or an organization without their knowledge. Spyware may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge [1]. In order to know its operation, it is important to answer some of the frequently-asked questions: How they install spyware at our computer? How do they settle? Frequently,

[1] "The Federal Trade Commission, which probably carries the most potent regulatory authority to control spyware, defines it as software that aids in gathering information about a person or organization without their knowledge, and that may send that information to another entity without user consent [Urbach and Kibel, 2004]. Spyware, essentially, is software that asserts control over a user's computer without his/herconsent" (Stafford, Th. F. y Urbaczewski, A.: Spyware: the ghost in the machine. Communications of the Association for Information Systems (Volume14, 2004), 292).

the user is not conscious that he has an installed spy file in his computer that can have installed with free software or after to have visited some web sites. A major concern in all cases is that users are very often not aware of the fact that others gain access to their PCs and store information or programs on it. Many spyware are introduced in the system once the user accepts, without previously reading the license agreement. In the case of free software which has been installed, the spy program even continues working when the program that had been unloaded has let work. What are the consequences for the user? Once installed, what can it do? These programs can copy information, to generate specific publicity for this concrete user, to know the e-mail address, web sites that the user has visited, etc. These e-mail addresses can later be used to send commercial communications. It leads to another problem involving consumer protection and spam (article 21 Electronic Commerce Act in Spain and article 13 Directive on Privacy and Electronic Communications) [2].

Adware, unlike spyware, do not collect information about your computer only shows advertising while the user is using a certain application. Adware is entered into the computer and the application is self each time you start a session and you can record the pages you visit, send information to external servers, which in turn will send advertisements to the user.

Moreover, web bugs are small images embedded in web pages. Its operation is similar to the bars ad as the display of the image causes the execution of an action. These web bugs go unnoticed (can be limited to pictures one pixel transparent) and can obtain to collect usage statistics, operation of bars advertising, etc. The information stolen can be found the user's IP address, the browser used or the information collected by cookies.

Mail bugs are similar to the web bugs, but this time associated with the email. When viewing the email, the image is downloaded from the server. Being embedded in the email, sent information indicating that the message it contains has been opened, verify that the recipient address is real. After this verification, this address may be used for sending unsolicited commercial email. If the mail bug contains a unique identifier may be used to determine whether a message is forwarded.

All these technologies, as set out above, are capable of seeping into the computer without a user account that it is necessary to install certain software to detect and can be particularly interesting to obtain user's tastes, preferences will possible to send a personalized advertising, much more effective than the traditional one. These techniques, known as spyware, could be more aggressive than the use of cookies and its operation is different. While the cookies are deposited in the net server of the client, which the user will be able to recognise

[2] About spyware, e-trust guidance says: "From there, the program would work invisibly, sending key logs, or log files of the characters you have punched on your keyboard, to someone else on a remote terminal. This is why spyware is also called as a key logger program. Eventually, spyware evolved into more damaging forms. Today, you would have invisible scripts redirecting you to certain websites which you have not chosen to view, or pop-ups that keep sprouting left and right even if you're viewing a pop-up free website". (`http://www.etrust.org/guidance/spyware.html`).

in later accesses, spyware settles in the computer of the user, without the users consent. The user is not conscious that a web bug or mail bug is gathering information about him. In cookies, we have a function of security in the navigator which can warn the user of his use; however, in the case of spyware, there is no warning of any type and installing a certain program one only knows if really they are catching our data. The technical panorama is advancing very fast in this aspect. Are current laws adequate to deal with these emerging problems?

Chapter 2

Regulation

- Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
- Directive 2002/58/CE on Privacy and Electronic Communications.
- Directive 2000/731/EC on Electronic Commerce.
- Spanish Data Protection Act: L.O. 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Spanish Electronic Commerce Act: Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Chapter 3

Directive on Privacy and Electronic Comunications and Comparative Law

Cookies, spyware, web bugs or mail bugs are techniques used to successfully obtain information about Internet users. It can damage their privacy. This problematic subject is already reflected in whereas 24 and 25 and in the article 5.3 of Directive 2002/58/CE on Privacy and Electronic Communications:

"(24) Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms. So-called spyware, web bugs, hidden identifiers and other similar devices can enter the user's terminal without their knowledge in order to gain access to information, to store hidden information or to trace the activities of the user and may seriously intrude upon the privacy of these users. The use of such devices should be allowed only for legitimate purposes, with the knowledge of the users concerned.

(25) However, such devices, for instance so-called 'cookies', can be a legitimate and useful tool, for example, in analysing the effectiveness of website design and advertising, and in verifying the identity of users engaged in online transactions. Where such devices, for instance cookies, are intended for a legitimate purpose, such as to facilitate the provision of information society services, their use should be allowed on condition that users are provided with clear and precise information in accordance with Directive 95/46/EC about the purposes of cookies or similar devices so as to ensure that users are made aware of information being placed on the terminal equipment they are using. Users should have the opportunity to refuse to have a cookie or similar device stored on their terminal equipment. This is particularly important where users other than the original user have access to the terminal equipment and thereby to any data containing privacy-sensitive information stored on such equipment. Infor-

mation and the right to refuse may be offered once for the use of various devices to be installed on the user's terminal equipment during the same connection and also covering any further use that may be made of those devices during subsequent connections. The methods for giving information, offering a right to refuse or requesting consent should be made as user-friendly as possible. Access to specific website content may still be made conditional on the wellinformed acceptance of a cookie or similar device, if it is used for a legitimate purpose".

Besides article 5.3 Directive on Privacy and Electronic Communication states: *"Member States shall ensure that the use of electronic communications networks to store information or to gain access to information stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned is provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia about the purposes of the processing, and is offered the right to refuse such processing by the data controller. This shall not prevent any technical storage or access for the sole purpose of carrying out or facilitating the transmission of a communication over an electronic communications network, or as strictly necessary in order to provide an information society service explicitly requested by the subscriber or user".*

The regulation applicable to the cookies, spyware, mail bugs... (it does not refer expressly to the spyware but to *"electronic communications networks to store information or to gain access to information stored in the terminal equipment"*) in Spain is article 22.2 of the Electronic Commerce Act.

According to these articles: to use electronic communications networks to store information or to gain access to information stored in the terminal equipment of user is only allowed if:

- the user is informed in a clear and comprehensive manner on the use and purpose of the processing information and
- the right to refuse such processing is offered by the data controller with a free and easy manner.

In the USA there are specific rules about Spyware. It is the case of Spyware Control Act of Utah. This Act establishes: *"(1) A person may not: (a) install spyware on another person's computer; (b) cause spyware to be installed on another person's computer; (c) use a context based triggering mechanism to display an advertisement that partially or wholly covers or obscures paid advertising or other content on an Internet website in a way that interferes with a user's ability to view the Internet website".* (`http://www.le.state.ut.us`). In California, Consumer Protection Against Computer Spyware Act establishes: "*It is the intent of the Legislature that this Act protect California consumers from the use of spyware and malware that is deceptively or surreptitiously installed on their computers. Because the threats posed by these practices change over time, it is the intent of the Legislature to revise the provisions in this act as needed to fully protect consumers from additional unfair and deceptive practices and to address future innovations in computer technology and practices".*

Main issues in the USA rules are: software that taking control of a computer; modifying settings without authorization; collecting personally identifiable information; preventing reasonable efforts to block the installation of software; misrepresentation that the software will be uninstalled or disabled; and removing or rendering inoperative antispyware software.

It is necessary the previous information (in a clear and comprehensible manner) and consent of the user to install spyware in his computer. It is the case of the rules of Indiana, Massachusetts, New Hampshire, Tennesse, etc. (`http://www.benedelman.org/spyware/legislation`. Y para obtener información sobre litigios en EE.UU referentes a estos temas:
`http://www.benedelman.org/spyware/threats/`).

Chapter 4

Rules about Personal Data Protection

Besides the Directive on Privacy and Electronic Communications, in these cases rules about data protection must be applied. Specifically, the Directive on Data Protection and its implementing regulation: in Spain the Data Protection Act (LO 15/1999). Cookies, spyware and other system can obtain personal data of the users, for instance: IP address or e-mail address among others.

Personal data mean: any information relating to an identified or identifiable natural person ('data subject'). An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Specially, Spanish Agency of Data Protection in its reports 327/2003 and 0391/2007 qualified IP address and e-mail address as personal data. So in the cases of personal data are processed it is necessary to fulfil the rules of the Data Protection Act about consent, right of access, right to object, etc.

The processing of personal data is legitimate only when they are adapted, pertinent and not excessive as regards the certain, explicit and legitimate purposes for those who have been obtained (article 4.1 Spanish Data Protection Act). Besides, the Directive on the protection of individuals with regard to the processing of personal data establishes that any processing of personal data must be lawful and fair to the individual concerned; in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed and such purposes must be explicit and legitimate and must be determined at the time of collection of the data. The purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified. So, the information object of treatment will not be able to be used for incompatible purposes with those for that the information had been gathered (in this case: the protection of the copyright?). The information about personal data will be accurate and informed so that they answer with veracity

to the current situation of the affected one and it will be cancelled when they have stopped being necessary for the purpose for the one that they had been obtained.

In the same way, the article 4.3 of the Electronic Communications Act of Luxembourg (may 30th, 2005) or the article 5 of the data Protection Act in Portugal.

If it is a question on personal data, the controller will have to fulfil the requirements established by the law. They are very important: the duty to inform and the data subject's consent. This consent in European Directive on Data Protection (article 2) and in Spanish Data Protection Act (article 3) is defined as a freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed. And the controller must inform about: the identity of the controller; the purposes of the processing for which the data are intended; the recipients of the data, the existence of the right of access and the right to rectify the data concerning him in so far as such further information is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject.

Chapter 5

Privacy versus Search Engines and On Line Social Networks

However, there are other dangers to privacy of the users. There are other services that, although they do not break the rules themselves, sometimes they are in the limit that regulation permits. This is the case of search engines (and search histories and personal data) or social networks. A lot of problems about privacy can arise during people use on line social networks and a lot of times people are not conscious of these dangers.

In the case of search engines, they can get our personal data; they may obtain search histories that could obtain data on the tastes, interests of users. On this, the Opinion 1/2008 on data protection issues on April 4th, 2008 of the Working Group Article 29 about search engines:

- "If search engine providers use cookies, their lifetime should be no longer than demonstrably necessary. Similarly to web cookies, flash cookies should only be installed if transparent information is provided about the purpose for which they are installed and how to access, edit and delete this information.
- Search engine providers must give users clear and intelligible information about their identity and location and about the data they intend to collect, store or transmit, as well as the purpose for which they are collected".

About the right of users in these cases:

- "Users of search engine services have the right to access, inspect and correct if necessary, according to Article 12 of the Data Protection Directive (95/46/EC), all their personal data, including their profiles and search history.

- Cross-correlation of data originating from different services belonging to the search engine provider may only be performed if consent has been granted by the user for that specific service".

Besides, search engines often contain hyperlinks to advertisers. On the other hand, social Networks are very popular nowadays. But a lot of information and personal data is on the Internet. So, a lot of people can access to them, for instance marketing enterprises. Participation in social networks is very interesting but privacy issues are concerned (This is an example in the clauses about privacy of Facebook: *"When you publish content or information using the "everyone" setting, it means that everyone, including people off of Facebook, will have access to that information and we may not have control over what they do with it")*.

Cookies are often used in the social networks. This is a clause of Facebook: *"In addition, we store certain information from your browser using "cookies." A cookie is a piece of data stored on the user's computer tied to information about the user. We use session ID cookies to confirm that users are logged in. These cookies terminate once the user closes the browser. By default, we use a persistent cookie that stores your login ID (but not your password) to make it easier for you to login when you come back to Facebook. You can remove or block this cookie using the settings in your browser if you want to disable this convenience feature..."*. Or in the case of Myspace: *"Cookies are small bits of information that MySpace places on your computer. MySpace uses cookies to identify your Internet browser, store Users' preferences, and determine whether you have installed the enabling software needed to access certain material on the MySpace Services. Data in cookies may be read to authenticate user sessions or provide services"*. Or: *"MySpace may use cookies and similar tools to customize the content and advertising you receive based on the Profile Information you have provided"*.

In fact, Canada has already raised a complaint against a popular social network for violation of Canadian law on data protection. Data of a group of students were used by to send personal advertisers. They say that this action is against data protection rules in Canadá.

Another clause of the general terms of Facebook establishes that: *"...may also collect information about you from other sources, such as newspapers, blogs, instant messaging services, and other users of the Facebook service through the operation of the service (e.g., photo tags) in order to provide you with more useful information and a more personalized experience"*. This is not possible in Spain without the prior consent of the user because Internet are not a "public source"(in the terms of the Data Protection Act) of personal data.