European DPAs adopt integrated approach to online data protection

Report by Diana Alonso Blas

ON JANUARY 10TH 2001 the European Parliament organised a seminar on the proposed Directive on processing personal data and protecting privacy in the electronic communications sector.

Peter Hustinx, Chairman of the Dutch Data Protection Authority and the Internet Task Force (ITF) of the Article 29 Working Party, presented a document on Privacy on the Internet which the Working Party had adopted on November 21st 2000. This comprehensive document outlines the European Union Commissioners' integrated approach to on-line data protection. The word "integrated" underlines that this analysis departs from the texts of both the general data protection directive (Directive 95/46/EC) and the privacy and telecommunications directive (Directive 97/66/EC). It also reflects and assembles all opinions and documents adopted to date by the Working Party on certain critical issues related to this subject.

All chapters start with a basic technical description of the Internet service being examined, and then provide a legal analysis of the related issues. The document examines in detail the roles of the different actors and the privacy risks involved, as well as the privacy enhancing measures related to that service. One chapter is also dedicated to measures and technologies that increase the privacy of the Internet users.

TELECOMMUNICATIONS DIRECTIVE 97/66

The ITF document pays special attention to the proposed review of Directive 97/66/EC. In general, the ITF concludes that the review (outlined in the July 12th 2000 draft proposal) encompasses several substantial improvements. The following points are especially important.

The terminology in Directive 97/66/EC cast some doubt on its application to the Internet since most of its provisions use terms such as "calls", which allude to traditional and ISDN telephony. The review has made it clear that this Directive covers new services and technologies, thus avoiding possible ambiguities and facilitating the consistent application of data protection principles on the Internet.

The proposal no longer refers to "telecommunications services" but to "electronic communications services", as defined in the proposed directive establishing a common framework for electronic communications services and networks. This new definition distinguishes clearly between regulating content and transmission.

Article 5 of Directive 97/66/EC (on confidentiality) referred to the content of the communication. Distinguishing between traffic data and content, however, is not easy in the context of the Internet, and certainly not when considering "surfing". The behaviour of an Internet user (navigation data) surfing different websites in itself reveals much about the communication. Knowing which websites were visited paints a fairly accurate picture of the communication. Extending the scope of Article 5 to cover not just the content of the communication but also the related

The Internet Task Force (ITF) of the Working Party, which prepared the document, was created in 1999 to deal systematically and efficiently with Internet-related data protection issues. The ITF brings together resources and interdisciplinary expertise from different national Data Protection Authorities. It is a joint European investment in e-privacy.

The ITF's work was co-ordinated by Peter Hustinx, Chairman of the Dutch Data Protection Authority, and involved delegates from the data protection authorities of Belgium, Denmark, France, Germany, Spain and The Netherlands. ITF appointed an internal Drafting Group to prepare the consolidated version of the document. The group is composed of Diana Alonso Blas (from the Dutch Data Protection Authority) and Anne-Christine Lacoste (from the Belgian Data Protection Authority).

The ITF first studied individually the most common services available on the Net and then prepared a synthesis paper on all these services. The Drafting Group prepared a consolidated version of the complete document, paying particular attention to the structure and coherence of the document as a whole, the integration and further development of additional legal issues and technical information. The Working Group also took into account comments from other delegations and developed the glossary of technical terms and the document's conclusions.

traffic data has led to major improvements. By giving equal protection to content and related traffic data the (sometimes difficult) distinction between these concepts assumes less importance.

THE DOCUMENT'S APPROACH TO INTERNET PRIVACY

The working document first offers a technical description of the Internet. This description is written in clear language and seeks to provide readers with the basic tools to understand the privacy issues. The document pays special attention to the different groups involved in the Internet, the most commonly used services, the importance of the protocols used and the economic aspects of the Internet as a business. Where necessary, more detailed technical explanations are included in the footnotes and in the glossary.

A second chapter deals with general legal issues. It pays particular attention to the increasing amounts of personal data processed on the Internet and the various groups involved. The chapter explains generally the main data protection rules (both European Directives) and other instruments such as the e-commerce Directive.

The core of this document deals primarily with the Internet services commonly used by an average Internet user: e-mail, surfing and searching, newsgroups, chat-rooms and electronic transactions. A separate chapter addresses each service, including one on "cybermarketing."

While the Working Party welcomes the draft Directive having taken the new issues into account, some of its proposals could still be addressed more effectively.

TRENDS, RISKS, GUIDELINES AND RECOMMENDATIONS

The document contains two sets of conclusions: first, it summarises the trends and privacy risks observed in all the different aspects of Internet use; second, it provides guidelines and recommendations for possible action. The main trends and risks are:

• The Internet is growing exponentially.

• The number of available services and their complexity is increasing, making it difficult for users to understand the services and the differences between them.

• Companies try to attract users and distinguish themselves by offering personalised services. These services require the users' personal data, which companies obtain through different sources.

• New technologies (often using a statistical analysis of IP addresses) and the new generation of software and hardware products make it easier to monitor users in real time without their knowledge. Anonymity becomes increasingly difficult to achieve on the Internet.

These new capabilities embody new risks for Internet users' privacy, especially when data are concentrated in the hands of one or a few controllers. Such risks also arise because some data are preserved on-line for considerable time. The long-term availability of data facilitates unexpected secondary uses that are often incompatible with the purpose for which the data were originally collected.

THE CONCLUSION PROPOSES FOUR FUTURE POLICIES:

1. Increase privacy awareness of Internet users

Given the increasing risks for the privacy of Internet users, it is especially important to ensure users have all the information they need to make an informed choice. Several groups have a role to play in providing this information:

(a) Any controller (whether a public authority or private company) collecting personal data on-line must give the data subject all the necessary information. This information (cited in article 10 of Directive 95/46/EC) must always be given when collecting the data. Posting a privacy policy on the website is a good way of providing general information to the public. However, data controllers must also provide information to the data subject in a simple and accessible way each time the data are collected – for example, on the same screen where the data subject must supply data, or through a box prompt.
(b) Privacy associations and advocates have traditionally performed public awareness activities.
(c) Consumer associations are also increasingly involved in the privacy aspects of consumer activities.
(d) Professional associations can inform their members about their legal obligations.
(e) Individuals must then use all available means to ensure respect for their rights. They might also want to make clear that they will not accept services or products that do not comply with the existing legal framework.

2. Apply existing legislation in a coherent and co-ordinated way

Sufficient on-line data protection can occur only if the existing legal framework is respected. Given the international character of the Internet, data controllers must be able to depend on a coherent and co-ordinated interpretation and application of the European data protection rules. The Working Party and revision of the Telecommunications Directive 97/66/EC are especially important.

Interpretation and application of the legislation is not only the task of public authorities. The private sector can make a useful contribution by self-regulation or by developing codes of conduct to address specific issues in their particular sector.

3. Develop and use privacy compliant, privacy friendly and privacy enhancing technologies

The processing of personal data on the Internet is heavily dependent on the configuration of the hardware and software, as well as the protocols and technical standards used to transmit information. Therefore it is particularly important to take privacy requirements into account at the earliest stage of developing these tools.

Continued on page 18