I

(Resolutions, recommendations and opinions)

OPINIONS

EUROPEAN DATA PROTECTION SUPERVISOR

Opinion of the European Data Protection Supervisor on the Proposal for a Directive of the European Parliament and of the Council amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)

(2008/C 181/01)

THE EUROPEAN DATA PROTECTION SUPERVISOR,

Having regard to the Treaty establishing the European Community, and in particular its Article 286,

Having regard to the Charter of Fundamental Rights of the European Union, and in particular its Article 8,

Having regard to 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 ([1]),

Having regard to Directive 2002/58/EC of the European Parliament and of the Council of the 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector ([2]),

Having regard to Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, and in particular its Article 41 ([3]),

Having regard to the request for an opinion in accordance with Article 28(2) of Regulation (EC) No 45/2001 received on 16 November 2007 from the European Commission,

HAS ADOPTED THE FOLLOWING OPINION:

I. INTRODUCTION

1. On 13 November 2007, the Commission adopted a Proposal for a Directive amending, among others, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communication sector (hereinafter 'Proposal' or 'proposed amendments'). The current version of Directive 2002/58/EC is usually, also in this Opinion, referred to as the ePrivacy Directive.

([1]) OJ L 281, 23.11.1995, p. 31.
([2]) OJ L 201, 31.7.2002, p. 37.
([3]) OJ L 8, 12.1.2001, p. 1.

2. The Proposal aims at enhancing the protection of individuals' privacy and personal data in the electronic communications sector. This is done not by entirely reshaping the existing ePrivacy Directive but rather by proposing *ad hoc* amendments to it, which mainly aim at strengthening the security-related provisions and improving the enforcement mechanisms.

3. The Proposal is part of a wider reform of the five EU telecom Directives ('the telecoms package'). In addition to the proposals for the review of the telecoms package ([1]) the Commission has also adopted at the same time a Proposal for a Regulation establishing the European Electronic Communications Market Authority ([2]).

4. The remarks contained in this Opinion are limited to the proposed amendments to the ePrivacy Directive unless such proposed amendments rely on concepts or provisions contained in proposals for review of the telecoms package. In addition, some comments contained in this Opinion refer to provisions of the ePrivacy Directive which have not been amended by the Proposal.

5. This Opinion addresses the following topics: (i) the scope of the ePrivacy Directive, in particular, the services concerned (proposed amendment to Article 3(1)); (ii) the notification of security breaches (proposed amendment creating Article 4(3) and 4(4)); (iii) the provisions on cookies, spyware and similar devices (proposed amendment to Article 5(3)); (iv) the legal actions initiated by electronic communication services providers and other legal persons (proposed amendment creating Article 13(6)); and (v) the strengthening of the enforcement provisions (proposed amendment creating Article 15a).

Consultation with the EDPS and broader public consultation

6. The Proposal was sent by the Commission to the EDPS on 16 November 2007. The EDPS understands this communication as a request to advise Community institutions and bodies, as foreseen in Article 28(2) of Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data (hereinafter 'Regulation (EC) No 45/2001').

7. Prior to the adoption of the Proposal, the Commission informally consulted the EDPS on the draft Proposal, which the EDPS welcomed as it gave him an opportunity to make some suggestions on the draft proposal prior to its adoption by the Commission. The EDPS is glad to see that some of his suggestions have been reflected in the Proposal.

8. The adoption of the Proposal was preceded by a wide public consultation exercise, a practice valued by the EDPS. Indeed in June 2006 the Commission launched a public consultation on its Communication on the Review of the telecoms package where the Commission described its views on the situation and put forward some proposals for amendments ([3]). The Article 29 Data Protection Working Party ('WP 29'), of which the EDPS is a member, used this opportunity to provide its views on the proposed amendments in an Opinion adopted on 26 September 2006 ([4]).

([1]) The proposed amendments to the telecoms Directives are put forward in the following Proposals: (i) proposal for a Directive of the European Parliament and of the Council amending Directive 2002/21/EC on a common regulatory framework for electronic communications networks and services, Directive 2002/19/EC on access to, and interconnection of, electronic communications networks and services, and Directive 2002/20/EC on the authorisation of electronic communications networks and services, 13 November 2007, COM(2007) 697 final; (ii) proposal for a Directive of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on consumer protection cooperation, 13 November 2007, COM(2007) 698 final.

([2]) Proposal for a Regulation of the European Parliament and of the Council establishing the European Electronic Communications Market Authority, 13 November 2007, COM(2007) 699 final.

([3]) Communication on the EU Regulatory Framework for electronic communications networks and services (SEC(2006) 816) adopted on 29 June 2006. The Communication was complemented by a Commission Staff Working Document (COM(206) 334 final).

([4]) Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, adopted on 26 September 2006.

EDPS overall views

9. On the whole the EDPS views on the Proposal are positive. The EDPS fully supports the aims of the Commission in adopting a Proposal enhancing the protection of individuals' privacy and personal data in the electronic communications sector. The EDPS particularly welcomes the adoption of a mandatory security breach notification system (Amendment to Article 4 of the ePrivacy Directive, adding paragraphs 3 and 4). When data breaches occur, notification has clear benefits, it reinforces the accountability of organizations, is a factor that drives companies to implement stringent security measures and it permits the identification of the most reliable technologies towards protecting information. Furthermore, it allows the affected individuals the opportunity to take steps to protect themselves from identify theft or other misuse of their personal information.

10. The EDPS welcomes other amendments in the Proposal such as the ability for legal persons with legitimate interest to have a cause of action against those who infringe some of the provisions of the ePrivacy Directive (Amendment to Article 13, adding paragraph 6). Also positive is the strengthening of the investigatory powers of national regulatory authorities as it will enable them to assess whether or not any processing of data is carried out in compliance with the law and to identify infringers (Addition of Article 15a(3)). To be able to stop unlawful processing of personal data and infringements of privacy as soon as possible is a necessary measure in order to protect the rights and freedoms of individuals. To this end the proposed Article 15a(2) which recognizes the national regulatory authorities' power to order the cessation of infringements is much welcomed as it will enable them to bring seriously unlawful processing to an immediate halt.

11. The approach of the Proposal and most of the proposed amendments are in line with the views on the future data protection policy which were put forward in previous EDPS Opinions such as the Opinion on the implementation of the Data protection Directive ([1]). Among others, the approach is based on the belief that while no new data protection principles are necessary, there is a need for more specific rules to address data protection issues raised, by new technologies such as the Internet, RFID, etc, as well as tools that contribute to enforce and make effective data protection legislation such as enabling legal entities to initiate actions for violation of data protection and obliging data controllers to notify security breaches.

12. Despite the overall positive approach of the Proposal, the EDPS regrets that the Proposal is not as ambitious as it could have been. Indeed, since 2003 the application of the provisions contained in the ePrivacy Directive as well as careful analysis of the subject has shown that some of its provisions are far from clear, generating legal uncertainty and compliance problems. For example, this is the case regarding the extent to which semi-public providers of electronic communication services are covered by the ePrivacy Directive. One would have hoped that the Commission would have made use of the review of the telecom package, and in particular of the ePrivacy Directive, to resolve some of the outstanding problems. Furthermore, in dealing with new issues, such as the setting up of a mandatory breach notification system, the Proposal only offers a partial solution, not including within the scope of the organizations obliged to notify security breaches, entities that process very sensitive types of data such as on-line banks or providers of on-line health services. The EDPS regrets this approach.

13. The EDPS is hopeful that as the Proposal makes its way through the legislative process, the legislator will take into account the comments and proposals contained in this Opinion towards solving the issues that the Commission's Proposal has failed to address.

([1]) Opinion of the European Data Protection Supervisor of 25 July 2007 on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1).

II. ANALYSIS OF THE PROPOSAL

II.1. Scope of the ePrivacy Directive, in particular, services concerned

14. A key issue in the current ePrivacy Directive is the question of its scope of application. The Proposal contains some positive elements towards defining and clarifying the scope of the Proposal, particularly, the services concerned by the Directive, which are discussed below under Section (i). Unfortunately, the proposed amendments do not solve all existing problems. As discussed under Section (ii) below, the amendments unfortunately do not seek to broaden the scope of application of the Directive to include electronic communication services in private networks.

15. Article 3 of the ePrivacy Directive describes the services concerned by the Directive, in other words, the services to which the obligations set forth in the Directive apply: '*This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communication services in public communications networks*'.

16. Therefore, the services concerned by the ePrivacy Directive are the providers of public electronic communication services in public networks ('PPECS'). The definition of a PPECS is provided under Article 2(c) of the Framework Directive ([1]). Public communication networks are defined under Article 2(d) of the Framework Directive ([2]). Examples of PPECS include providing access to the Internet, transmission of information through electronic networks, mobile and telephone connections, etc.

(i) *Proposed amendment to Article 3 of the ePrivacy Directive: Services concerned to include public communication networks supporting data collection and identification devices*

17. The Proposal amends Article 3 of the ePrivacy Directive by specifying that public electronic communication networks include '*public communication networks supporting data collection and identification devices*'. Recital 28 explains that the development of applications entailing the collection of information, including personal data, using radio frequencies, such as RFID, must be subject to the ePrivacy Directive when they are connected or make use of public communication networks or services.

18. The EDPS finds this provision positive as it clarifies that a number of RFID applications fall within the scope of the ePrivacy Directive, thus removing some uncertainty on this point and definitively removing misunderstandings or misinterpretation of the law.

19. Indeed, under the current Article 3 of the ePrivacy Directive certain RFID applications are already covered by the Directive. This happens for several cumulative reasons. Firstly, because RFID applications fall within the definition of electronic communication services. Secondly, because they are provided over an electronic communication network insofar as the applications are supported by a transmission system that conveys signals in a wireless way. And finally, the network may be public

([1]) Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services (OJ L 108, 24.4.2002, p. 33). The Framework Directive delimits what should be understood by electronic communication system, namely: (i) An 'electronic communications service' is a service that is normally provided for a fee and consists of conveying signals on networks and includes telecommunications and transmission services in networks. (ii) Services that provide content transmitted using electronic communications networks and services are excluded from the definition of electronic communications services. (iii) Provision of services means the establishment, operation, control, or making available of a network. (iv) Electronic communications services do not include information society services, which are defined in the E-Commerce Directive as service[s], normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

([2]) Public communications network means an electronic communications network used wholly or mainly for the provision of publicly available electronic communications services.

and private. If public, RFID applications will be deemed as 'services concerned' and thus fall within the scope of application of the ePrivacy Directive. However, the proposed amendment will eliminate any remaining doubt about it and thus provide more legal certainty.

20. Of course, as pointed out in a previous EDPS Opinion on RFID ([1]), this provision does not preclude the possible need to enact additional legal instruments as far as RFID is concerned. However, such measures should be adopted in another context, not as part of this Proposal.

(ii) *Need to include electronic communication services in private or semi private networks*

21. While the EDPS welcomes the clarification described above, he regrets that the Proposal has not tackled the issue of the increasingly blurred distinction between private and public networks. Furthermore, the EDPS regrets that the definition of services covered by the ePrivacy Directive has not been broadened to include private networks. As it currently stands, Article 3(1) of the ePrivacy Directive applies only to *electronic communication services in public networks*.

22. The EDPS notes the tendency of services to increasingly become a mixture of private and public ones. Think for example of universities allowing thousands of students to use Internet and e-mail. The ability of this semi-public (or semi/private) networks to impinge on individuals' privacy is obvious and therefore calls for this type of services to be subject to the same set of rules as apply to purely public networks. Furthermore, private networks such as those of employers providing employees with Internet access, hotels or apartment owners providing guests with telephone and e-mail as well as Internet cafes have an impact on the data protection and privacy of their users which suggests that they should also be covered by the scope of application of the ePrivacy Directive.

23. In fact, case law of some Member States has already held electronic communication services provided in private networks under the same obligations as those provided in public ones ([2]). Also, under German law, data protection authorities have found that allowing private email usage within a company can cause the company to be deemed as an operator of public telecommunications services, and thus to fall under the ePrivacy Directive's provisions.

24. In short, the rising importance of the mixed (private/public) and private networks in everyday life, with the risk to personal data and privacy increasing accordingly, justifies the need to apply to such services the same set of rules that apply to public electronic communication services. To this end, the EDPS considers that the Directive should be amended to broaden its scope to include such type of private services; a view that is shared by the Working Party 29 ([3]).

II.2. **Notification of Security Breaches: Amendment to Article 4**

25. Article 4 of the ePrivacy Directive is amended with the inclusion of two new paragraphs (3 and 4) which set forth an obligation to notify security breaches. Indeed, according to Article 4(3), PPECS are compelled to, on the one hand, notify national regulatory authorities, without undue delay of any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed in connection with the provision of electronic communications services (collectively 'compromise of data'); on the other hand, PPECS are also compelled to notify their customers.

([1]) Opinion of 20 December 2007 on the communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Radio Frequency Identification (RFID) in Europe: steps towards a policy framework, COM(2007) 96.

([2]) For example the Paris Court of Appeal judgment in *BNP Paribas* v *World Press Online* delivered on 4 February 2005 found that there was no distinction between Internet service providers who offered Internet access on a commercial basis and employers who gave Internet access to their staff.

([3]) Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive, adopted on 26 September 2006.

Benefits of this obligation

26. The EDPS welcomes these provisions (Article 4(3) and 4(4)) introducing a mandatory notification of security breaches. The notification of security breaches carries positive effects from the perspective of the protection of personal data and privacy, which have already been tested in the United States where breach notification legislation at state level has been in place for several years already.

27. Firstly, breach notification legislation enhances the accountability of the PPECS regarding the information which has been compromised. Under the data protection or privacy policy framework, accountability means that each and every organization is responsible for the information that is under its care and control. The obligation to notify is tantamount to a re-statement, on the one hand, that the data which have been compromised were under the control of the PPECS and, on the other hand, that it is the responsibility of this organization to take the necessary measures *vis-à-vis* such data.

28. Secondly, the existence of a security breach notification has proved to be a factor that drives security investment at organizations that process personal data. Indeed, the simple fact of having to publicly notify security breaches causes organizations to implement stronger security standards that protect personal information and prevent breaches. Furthermore, the notification of security breaches will help to identify and carry out reliable statistical analysis regarding the most effective security solutions and mechanisms. For a long time there has been a shortage of hard data about information security failures and the most appropriate technologies to protect information. This problem is likely to be solved with the security breach notification obligations, as was the case with the US security breach reporting laws, because notification will give information on the technologies more favourable to breaches ([1]).

29. Finally, the notification of security breaches makes individuals aware of the risks they face when their personal data are compromised and helps them to take the necessary measures to mitigate such risks. For example, if bank details have been compromised, the individual who is informed may decide to change his/her access details to his/her bank account to prevent someone from taking this information and using it for an unlawful purpose (usually referred to as 'identity theft'). In sum, this obligation reduces the likelihood of individuals becoming victims of identity theft and also may help victims to take the actions necessary to resolve problems.

Shortfall of the proposed amendment

30. While the EDPS is pleased with the security breach notification system set forth under Articles 4(3) and 4(4), he would have favored their application at a wider scale to include providers of information society services. This would mean that on-line banks, on-line businesses, on-line providers of health services, etc would also be covered by the law ([2]).

31. The reasons that justify imposing the security breach notification upon providers of public electronic communication services, i.e. PPECS, also exist regarding other organizations which also process massive amounts of personal data, the disclosure of which may be particularly harmful to data subjects. This includes on-line banks, data brokers and other on-line providers such as those who process sensitive data (which includes health data, political views, etc.). The compromise of information held by on-line banks and on-line business which may include not only bank account numbers but also credit card details may trigger identity theft, in which case it is essential for individuals to be made aware in order to take the necessary measures. In the latter case (on-line health), if not financial damage, surely individuals are likely to suffer non-economic damage when sensitive information is compromised.

([1]) See report '*Security Economics and the Internal Market*', commissioned by ENISA to by Prof. Ross Anderson, Rainer Böhme, Richard Clayton and Tyler Moore. The report is available at: http://www.enisa.europa.eu/doc/pdf/report_sec_econ_&_int_mark_20080131.pdf

([2]) Providers of information society services are defined in the E-Commerce Directive as service[s], normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services.

32. Furthermore, by broadening the scope of the obligation, the benefits described above, expected from the imposition of this obligation, will not be limited to one sector of activity, that of providers of publicly available electronic communication services, but will be expanded to information society services in general. Indeed, the imposition of security breach notification obligations upon information society services such as on-line banks will not only increase their accountability but also motivate such actors to strengthen their security measures and thus avoid future potential security breaches.

33. There are other precedents where the ePrivacy Directive already applies to entities other than PPECS, such as Article 5 on the confidentiality of communications and Article 13 on spam. This confirms that in the past the legislator, very wisely, took the decision to broaden the scope of application of certain provisions of the ePrivacy Directive because it felt that it was appropriate and necessary. The EDPS hopes that currently the legislator will not hesitate to take a similar sensible and flexible approach and broaden the scope of application of Article 4 in order to include providers of information society services. To this end, it would be sufficient to insert in Article 4(3) a reference to the providers of information society services as follows: 'In case of a breach of security leading to the accidental or … the provider of publicly available communication services and the provider of information society services, shall … notify the subscriber concerned and the national regulatory authority of such a breach'.

34. The EDPS views this obligation and its application to both PPECS and information society service providers as a first step of a development which may eventually be applied to all data controllers in general.

Specific legal framework for security breaches to be addressed through comitology

35. The Proposal does not address a number of questions related to the obligation to provide notification on security breaches. Examples of issues that need to be addressed are the circumstances of the notice, the format and the procedures applicable. Instead, Article 4(4) of the Proposal leaves these decisions for adoption through a 'comitology' committee ([1]), namely the Communications Committee set up by Article 22 of the Framework Directive, pursuant to Council Decision of 28 June 1999. In particular, such measures would be adopted in accordance with Article 5 of the Council Decision of 28 June 1999 which set up rules for the Regulatory procedure, as regards '*measures of general scope designed to apply essential provisions of basic instruments*'.

36. The EDPS does not oppose the choice of leaving all these issues to implementing legislation. Adoption of legislation through comitology is likely to shorten the legislative procedure. Also, comitology will help to ensure harmonization which is a goal that should be definitively sought.

37. Taking into account the large number of issues that will need to be addressed in the implementing measures and their relevance, as highlighted below, it seems appropriate to tackle them altogether in a single piece of legislation rather than in a piecemeal approach whereby some of the issues would be addressed in the ePrivacy Directive whereas others would be left to implementing legislation. Thus, the Commission's approach consisting in leaving these decisions to implementing legislation, to be adopted after consulting the EDPS, and hopefully other stakeholders (see point below), is to be welcomed.

Issues that will need to be addressed through implementing measures

38. The relevance of the implementing measures is highlighted if one foresees with some level of detail the issues that will need to be addressed by the implementing measures. Indeed, implementing measures may determine the standards under which notices must be delivered. For example, they will specify what constitutes a security breach, the conditions under which notices to individuals and to the authorities must be delivered, the timing for the notice and notification.

([1]) Law-making procedures in the EC which involve committees composed of the representatives of the governments of the Member States at the level of civil servants.

39. The EDPS considers that the ePrivacy Directive and particularly Article 4 should not contain any exception to the obligation to notify. In this regard, the EDPS is glad with the Commission's approach embodied in Article 4 which sets forth an obligation to notify and does not foresee any exception to it but allows this and other questions to be dealt with by implementing legislation. Although the EDPS is aware of arguments that might justify the setting up of some exceptions to the obligation, the EDPS favors this and other questions to be carefully addressed through implementing legislation, after a thorough and global debate of all the issues at stake. As indicated above, the complex nature of the questions related to the obligation to provide notification on security breaches, including whether exceptions or limitations are appropriate, calls for its treatment in a unified way, i.e. in a single piece of legislation which exclusively deals with this issue.

Consultation with the EDPS and the need to broaden the consultation

40. Taking into account the extent to which the implementing measures will affect the protection of the personal data of individuals, it is important that prior to the adoption of these measures the Commission engages in a proper consultation exercise. For this reason, the EDPS welcomes Article 4(4) of the Proposal which explicitly establishes that prior to adopting implementing measures, the Commission will consult the European Data Protection Supervisor. Such measures will not only concern but have an important impact on the protection of personal data and privacy of individuals. It is important therefore to seek the advice of the EDPS as required under Article 41 of Regulation (EC) No 45/2001.

41. In addition to consultation with the EDPS, it may be appropriate to include a provision establishing that draft implementation measures will be subject to public consultation, in order to obtain advice and encourage the sharing of experience of best practices in these matters. This will provide a proper channel not only to industry but also other stakeholders, including other data protection authorities and the Article 29 Working Party to put forward their views. The need for public consultation is reinforced if one takes into account that the procedure for adoption of legislation is comitology, with limited intervention of the European Parliament.

42. The EDPS notes that Article 4(4) of the Proposal foresees that the Commission will also consult the Electronic Communications Market Authority prior to adopting implementing rules. In this regard, the EDPS values the principle of consulting the Electronic Communications Market Authority as depositary of ENISA's experience and knowledge on network and information security issues. Until the Electronic Communications Market Authority is created it may be appropriate as an interim solution to foresee in the proposed amendment (Article 4(4)) the consultation of ENISA.

II.3. **Provision on cookies, spyware and similar devices: Amendment to Article 5(3)**

43. Article 5(3) of the ePrivacy Directive addresses the issue of technologies that permit the access to information and the storage of information in the users' terminal equipment, via electronic communication networks. An example of the application of Article 5(3) is the use of cookies ([1]). Other examples include the use of technologies such as spyware (hidden espionage programs) and Trojan horses (programs hidden in messages or in other apparently innocent software). The aim of such technologies and purposes varies enormously, whereas some are perfectly harmless or even useful for the user, other objectives are clearly very harmful and threatening.

([1]) Cookies are placed by ISSP (websites) in users' terminal equipments, for different purposes, including recognizing a visitor when he/she revisits a website. In practice when a cookie is sent to an Internet user by a website, the user's computer is assigned a unique number (i.e. the computer that received cookies from website A become 'computer holder of cookie 111'). The website keeps this number as a reference. If the user/s of the computer that received the cookie 111 does not delete the cookie file, the next time he/she visits the same website, the site will be able to identify the computer as the holder of cookie 111. The website naturally deduces that this computer has visited on previous occasions. The mechanism that allows a website to recognize a computer as a repeat visitor is simple. When the visiting computer holds cookies, such as cookie 111, and visits the site that on an earlier visited generated that cookie, it will search the hard disk of the user for the cookie file number. If the user's browser finds a cookie file to match the reference number kept by the website, it informs the website that the computer holds a cookie 111.

44. Article 5(3) of the ePrivacy Directive sets forth the conditions that apply when gaining access to or storing information on the terminal equipment of users using, among others, the technologies mentioned above. In particular, pursuant to Article 5(3): (i) Internet users must be provided with clear and comprehensive information in accordance with Directive 95/46/EC, *inter alia* about the purposes of the processing; and (ii) Internet users must be allowed to refuse such processing, i.e. to opt out from the processing of information retrieved from his/her terminal equipment.

Benefits of the proposed amendment

45. The existing Article 5(3) of the ePrivacy Directive limits its scope of application to situations where access to information and the storage of information in the users' terminal equipment is carried out via *electronic communication networks*. This includes the situation described above regarding the use of cookies as well as other technologies such as spyware delivered via electronic communication networks. However, it is far from clear whether Article 5(3) applies in situations where similar technologies (cookies/spyware and the likes) are distributed through software provided on external storage media and downloaded into the users' terminal equipment. Given that the threat to privacy exists independently of the communication channel, the limitation of Article 5(3) to one communication channel only is unfortunate.

46. The EDPS is therefore pleased with the Amendment to Article 5(3) which, by removing the reference to 'electronic communication networks', in fact, broadens the scope of application of Article 5(3). Indeed, the amended version of Article 5(3) encompasses both situations where access to information and the storage of information in the users' terminal equipment is carried out via electronic communication networks but also via other external data storage media such as CDs, CD-ROMs, USB Keys, etc.

Technical storage for the purpose of facilitating the transmission

47. The last sentence of Article 5(3) of the ePrivacy Directive remains unmodified in its amended version. Pursuant to the last sentence, the requirements of the first paragraph of Article 5(3) '*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 communication network or as strictly necessary in order to provide an information society service …*'. Thus, the mandatory rules of the first sentence of Article 5(3) (the need to provide information and offer the possibility to refuse) will not apply when access to the terminal equipment of the user or the storage of information has the sole purpose of *facilitating* a transmission or when it is strictly necessary for providing information society services requested by the user.

48. The Directive does not describe when the access or storage of information has the sole purpose of facilitating a transmission or providing information. One situation that would clearly be covered by this exception is the establishment of an Internet connection. This is because to establish an Internet connection is necessary to obtain an IP address ([1]). The computer of the end user will be asked to disclose to the Internet access provider certain information about itself and in return the Internet access provider will provide him an IP address. In this case, information stored in the end user terminal equipment will be transferred to the Internet access provider for the purpose of providing the user with access to the Internet. In this case, the Internet access provider is exempted from both the obligation to announce this collection of information and to provide the right to refuse insofar as it is needed to provide the service.

49. Once connected to the Internet, if a user wants to view a given website, he/she must send a request to the server where the website is hosted. The latter will respond if it knows where to send the information, i.e. if it knows the user's IP address. Because of how this address is stored, it again requires the website which the user wants to visit to access information on the Internet users' terminal equipment. Clearly this transaction would also fall within the scope of the exception. Indeed, in these cases it seems appropriate to be outside the scope of application of the requirements of Article 5(3).

([1]) An IP address (Internet Protocol address) is a unique address that certain electronic devices use in order to identify and communicate with each other on a computer network utilizing the Internet Protocol standard (IP) — in simpler terms, a computer address. Any participating network device — including routers, switches, computers, infrastructure servers (e.g. NTP, DNS, DHCP, SNMP, etc.), printers, Internet fax machines, and some telephones — can have its own address that is unique within the scope of the specific network. Some IP addresses are intended to be unique within the scope of the global Internet, while others need to be unique only within the scope of an enterprise.

50. The EDPS considers appropriate to exempt from the need to inform and give the possibility to refuse in situations as those illustrated above when technical storage or access to a user's terminal equipment is *necessary* for the sole purpose of carrying out the transmission of a communication over an electronic communication network. The same applies when the technical storage or access is strictly necessary in order to provide an information society service. However, the EDPS does not see the need to exclude from the obligation to provide information and offer the right to refuse in those situations where the technical storage or access has the purpose of merely *facilitating* the transmission of a communication. For example, pursuant to the last sentence of this Article a data subject may not benefit from information and the right to oppose the processing of his/her data if a cookie collects his language preferences or his location (e.g. Belgium, China) as this kind of cookies could be presented as having as objective the facilitation of the transmission of a communication. The EDPS is aware that at the level of software, the possibility is given in practice to data subjects to refuse or modulate the storage of cookies. However this is not backed-up clearly enough by any legal provision that would formally entitle the data subject to defend his rights in the context described above.

51. To avoid this outcome the EDPS suggests making a minor amendment to the last part of Article 5(3) which consists in deleting the word 'facilitating' from the sentence: '*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 communication network or as strictly necessary in order to provide an information society service …*'.

II.4. **Legal actions initiated by PPECS and legal persons: Addition of paragraph 6 to Article 13**

52. The proposed Article 13(6) provides civil law remedies for any individual or legal person with a legitimate interest particularly for electronic communication service providers, having a business interest to fight those who infringe Article 13 of the ePrivacy Directive. This Article deals with the sending of unsolicited commercial communications.

53. The proposed amendment will allow, for example, Internet access providers to tackle spammers for abusing their networks, to sue entities counterfeiting sender addresses or hacking servers for use as spam relays, etc.

54. The ePrivacy Directive was not clear on whether it allowed PPECS the right of action against spammers and on a very few occasions PPECS have brought actions before courts for infringement of Article 13 as implemented in Member State legislation ([1]). By recognizing a cause of action for electronic communications service providers to protect their business interests the Proposal confirms that the ePrivacy Directive intends not only to protect individual subscribers, but also the providers of electronic communication services.

55. The EDPS is satisfied that the Proposal introduces the possibility for electronic communication service providers having a business interest to bring actions against spammers. Save in exceptional circumstances, individual subscribers have neither the money nor the incentives to initiate this type of court action. Conversely, Internet access providers and other PPECS have the financial strength and technological capability to investigate spam campaigns, to identify the perpetrators and it only seems appropriate that they have the right to take legal actions against spammers.

56. The EDPS values particularly the proposed amendment insofar as it would also permit consumer associations and trade unions representing the interest of spammed consumers to take legal action on their behalf before courts. As outlined above, the damage inflicted upon a data subject who has been spammed, individually considered, is usually not sufficient in itself for him/her to initiate legal action before courts. In fact, the EDPS already proposed this measure as to privacy and data protection infringements generally speaking in his Opinion on the follow-up of the Work Programme for better

([1]) One case when this happens is the case Microsoft corporation v Paul McDonald t/a Bizards UK (2006 All Er (D) 153).

implementation of the Data Protection Directive ([1]). In the EDPS view, the Proposal could have gone further and propose class actions, empowering groups of citizens to jointly use litigation in matters concerning protection of personal data. In the case of spam, where a large number of individuals are receiving spam, the potential exists for classes of individuals to join together and launch class actions against spammers.

57. The EDPS especially regrets that the Proposal limits the possibility for legal persons to take legal actions to situations where there is an infringement of Article 13 of the Directive, i.e. situations where there is a violation of the provision on unsolicited email communications. Indeed, under the proposed amendment, legal persons would not be able to take legal actions about infringements of the other provisions of the ePrivacy Directive. For example, the current provision does not enable a legal person such as a consumer association to take legal action against an Internet access provider who had disclosed personal data of millions of customers. The enforcement of the ePrivacy Directive as a whole, not only of a given Article, would be greatly improved if the provision of Article 13(6) was made general to enable legal persons to take legal actions for infringement of any provision of the ePrivacy Directive.

58. To fix this problem the EDPS suggests converting Article 13(6) into a separate Article (Article 14). In addition, the language of Article 13(6) should be slightly amended as follows: Where it says '*pursuant to this Article*' it should say 'pursuant to this Directive'.

II.5. **Strengthening enforcement provisions: Addition of Article 15a**

59. The ePrivacy Directive does not contain explicit enforcement provisions. Instead, it refers to the enforcement Section of the Data Protection Directive ([2]). The EDPS welcomes the new Article 15a of the Proposal, which explicitly addresses enforcement issues under this Directive.

60. Firstly, the EDPS notes that an effective enforcement policy in this field assumes, as required under the proposed Article 15a(3), that national authorities have investigative powers in order to gather the necessary information. Very often the evidence of infringement of the provisions of the ePrivacy Directive will be of electronic nature and may be stored on different computers and devices or networks. In this context, it is important for enforcement agencies to be given the possibility to obtain search warrants conferring powers of entry, search and seizure.

61. Secondly, the EDPS particularly welcomes the proposed amendment, i.e. Article 15a(2), pursuant to which national regulatory authorities must have the power to order injunctions, i.e. the cessation of infringements and have the necessary investigation powers and resources. National regulatory authorities, including national data protection authorities, should have the power to impose injunctions requiring wrongdoers from continuing an activity that infringes the ePrivacy Directive. Injunctions or the power to order a cessation of an infringement is a useful tool in case of an ongoing course of conduct that violates individuals' rights. Injunctions will be very useful in order to stop infringements of the ePrivacy Directive such as for example the violation of Article 13 on unsolicited commercial communications which by its very nature is an ongoing course of conduct.

62. Thirdly, the Proposal enables the Commission to enact technical implementing measures to ensure effective cross border cooperation in the enforcement of national laws (proposed amendment Article 15a(4)). Experience of cooperation until now includes the agreement set up at the initiative of the Commission establishing a common procedure for handling cross-border complaints on spam.

([1]) Opinion of the European Data Protection Supervisor on the Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive (OJ C 255, 27.10.2007, p. 1).

([2]) 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.

63. The EDPS considers that, if legislation supports regulators to assist their counterpart in other countries, it will undoubtedly assist the cross border enforcement. It is therefore appropriate for the Proposal to enable the Commission to create the conditions to ensure cross-border cooperation, including the procedures for sharing information.

III. **CONCLUSIONS AND RECOMMENDATIONS**

64. The EDPS fully welcomes the Proposal. The proposed amendments strengthen the protection of individuals' privacy and personal data in the electronic communications sector and this is done with a light touch, without creating unjustified and unnecessary burdens upon organizations. More specifically, the EDPS considers that for the most part the proposed amendments should not be modified insofar as they fulfill properly their pursued objective. Point 69 below lists the amendments that the EDPS would hope to remain unmodified.

65. Notwithstanding the overall positive consideration of the Proposal, the EDPS considers that some of its amendments should be improved to ensure that they effectively provide for a proper protection of the personal data and the privacy of individuals. This is particularly true regarding the provisions on security breach notification and for those that deal with the legal actions initiated by electronic communication service providers for violation of spam provisions. In addition, the EDPS regrets that the Proposal fails to tackle some issues, not properly dealt with in the current ePrivacy Directive, missing the opportunity of this review exercise to resolve the outstanding problems.

66. To solve both problems, i.e. issues not properly addressed in the Proposal and those not dealt with at all, this Opinion has put forward some drafting proposals. Points 67 and 68 summarize the problems and propose specific language. The EDPS calls upon the legislator to take them into account as the Proposal makes its way through the legislative process.

67. The amendments contained in the Proposal where the EDPS would strongly favor modification, include the following:

(i) **Security breach notification**: As formulated, the proposed amendment adding *Article 4(4)* applies to providers of public electronic communication services in public networks (ISPs, network operators) who are compelled to notify national regulatory authorities and their customers of security breaches. The EDPS fully supports this obligation. However, the EDPS considers that the obligation should also apply to providers of information society services which often process sensitive personal information. Thus, on-line banks and insurers, on-line providers of health services and any other on-line business would also have to comply with the obligation.

To this end, the EDPS suggests inserting in Article 4(3) a reference to the providers of information society services as follows: 'In case of a breach of security … the provider of publicly available communication services *and the provider of information society services*, shall … notify the subscriber concerned and the national regulatory authority of such a breach'.

(ii) **Legal actions initiated by providers of public electronic communication services in public networks**: As formulated, the proposed amendment adding *Article 13(6)* provides civil law remedies for any individual or legal person particularly for electronic communication service providers to fight infringements of Article 13 of the ePrivacy Directive which deals with spam. The EDPS is satisfied with this provision. However, the EDPS does not see the rationale for this new capability to be limited to the infringement of Article 13. The EDPS suggests enabling legal persons to take legal actions for infringement of any provision of the ePrivacy Directive.

To achieve the above, the EDPS suggests converting Article 13(6) into a separate Article (Article 14). In addition, the language of Article 13(6) should be slightly amended as follows: Where it says '*pursuant to this Article*' it should say 'pursuant to this Directive'.

68. The scope of application of the ePrivacy Directive which is currently limited to providers of public electronic communication networks is one of the most worrisome issues that the Proposal has failed to address. The EDPS considers that the Directive should be amended to broaden its application to include providers of electronic communication services also in mixed (private/public) and private networks.

69. The amendments that the EDPS would strongly favor to remain unmodified include the following:

(i) **RFID**: The proposed amendment to *Article 3* according to which electronic communication networks include '*public communication networks supporting data collection and identification devices*' is fully satisfactory. This provision is very positive as it clarifies that a number of RFID applications must comply with the ePrivacy Directive, thus removing some legal uncertainty on this point.

(ii) **Cookies/spyware**: The proposed amendment to *Article 5(3)* is to be welcomed because as a result the obligation to inform and give the right to oppose to have cookies/spyware stored in one's terminal equipment will also apply when such devices are placed through external data storage media such as CD-ROMs, USB Keys. However, the EDPS suggests that a minor amendment be made to the last part of Article 5(3) which consists in deleting the word 'facilitating' from the sentence.

(iii) **Choice of comitology with consultation to the EDPS and conditions/limitations to the obligation to notify**: The proposed amendment adding Article 4(4) regarding security breach notification leaves up to comitology, after having sought the EDPS's advice, the decision of complex questions regarding the circumstances/format procedures of the security breach notification system. The EDPS strongly supports this unified approach. Legislation on security breach notification is a topic on its own that needs to be addressed, after a careful debate and analysis.

Linked to this matter is the call by some stakeholders to draw up exceptions to the obligation to notify security breaches in Article 4(4). The EDPS strongly opposes this approach. He rather favors that the overall subject of the notification, how to notify, in which circumstances the notification may be shortened or somehow limited, to be analyzed holistically, after undertaking a proper debate.

(iv) **Enforcement**: The proposed amendment adding *Article 15a* contains many helpful elements to be kept which will contribute to ensuring effective compliance, including the strengthening of the investigatory powers of national regulatory authorities (Article 15a(3)) and the creation of the national regulatory authorities' power to order the cessation of infringements.

Done at Brussels, 10 April 2008.

Peter HUSTINX

European Data Protection Supervisor