



**00989/08/EN
WP150**

Opinion 2/2008 on the review of the Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive)

Adopted on 15 May 2008

This Working Party was set up under Article 29 of Directive 95/46/EC. It is an independent European advisory body on data protection and privacy. Its tasks are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC.

The secretariat is provided by Directorate C (Civil Justice, Rights and Citizenship) of the European Commission, Directorate General Justice, Freedom and Security, B-1049 Brussels, Belgium, Office No LX-46 06/80.

Website: http://ec.europa.eu/justice_home/fsj/privacy/index_en.htm

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995¹,

having regard to Articles 29, 30(1)(a) and 30(3) of that Directive, and Article 15(3) of Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002,

having regard to Article 255 of the EC Treaty and to Regulation (EC) no. 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents,

having regard to its Rules of Procedure

HAS ADOPTED THE PRESENT DOCUMENT:

1. BACKGROUND

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 communications sector ("the Proposal").

The primary objective of the Proposal is to enhance the protection of personal data and the privacy of individuals in the electronic communications sector, in particular, by strengthening security-related provisions and enforcement mechanisms.

The Article 29 WP wishes to comment on the Proposal and address some additional issues.

2. SPECIFIC COMMENTS

Notification of security breaches

Article 4

The Article 29 Working Party fully supports the proposed strengthening of Article 4 "Security" by requiring providers of publicly available communication services to notify security breaches, and underlines the importance of informing all persons concerned when their personal data have been compromised or are at risk of being compromised. However, the Working Party 29 does not consider that this Article fully addresses certain issues:

(a) The need to include providers of information society services within the scope of the obligation to notify security breaches

The Article 29 Working Party fully endorses the EDPS Opinion² that the introduction of a security breach notification system as described in Articles 4.3. and 4.4. should also

¹ Official Journal no. L281 of 23/11/1995, p. 31,
http://europa.eu.int/comm/internal_market/en/media/dataprot/index.htm

include providers of information society services such as on-line banks, on-line businesses, on-line providers of health care services etc.

Broadening the scope to include information society services in general would increase their accountability, and would contribute to raising awareness among the public. This would undoubtedly contribute to mitigating security risks.

(b) Recipients of the notices of security breaches

The Working Party considers that the scope of recipients of the security breach notification should be made wider, so as to include all persons concerned rather than only the "subscribers", by replacing, in Article 4, the word "subscribers" with "persons concerned".

The term "persons concerned" would include all persons whose data has effectively been compromised by the security breach (e.g. subscribers, but also former subscribers, and certain third parties).

This may be of special relevance, for instance, to persons who recently unsubscribed from a service and who are no longer "subscribers", but whose personal data are still retained by the data controller (i.e. the provider of a public electronic communication service). Another hypothetical situation which supports the need to broaden the scope of the addressees of the notification obligation is the case where providers of public electronic communication services retain information about a person, A, who did not subscribe to its services. This may happen if the information was submitted by a subscriber of the service who invited A to join the service. If information about A is disclosed as a result of a security breach, then A should naturally be notified of the breach.

This would also be relevant when breach notifications concern information society services. Indeed, users may interact with some information society services without subscribing to those services.

(c) Disclosure to the public

The Working Party suggests that, in certain circumstances, the national regulatory authority should be empowered, in the public interest, to inform the public of a breach or require the undertakings concerned to do so. The NRA should assess whether the case needs publication, balancing the interests of the providers against the rights of those affected.

Article 4.4.

Pursuant to Article 4.4, the Commission may, following consultation with the European Electronic Communication Market Authority and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances,

format and procedures applicable to the information and notification requirements referred to in Article 4.

(a) The choice of the “comitology” procedure

The Working Party 29 agrees with the Proposal's approach to tackle many important questions to be addressed regarding the provision of information to individuals and data protection authorities through implementing legislation rather than in the context of the ePrivacy Directive.

(b) Need for consultation with WP 29

The Article 29 Working Party should also be consulted in addition to the European Electronic Communication Market Authority and EDPS, since any measures introduced will directly affect the information to be given to persons concerned.

Concept of “personal data”

The Working Party welcomes the fact that the definition and scope of the term “*personal data*” in the Proposal is fully compatible with the corresponding definition in the Data Protection Directive, and underlines that any narrowing of the scope of the definition of “*personal data*” in the ePrivacy Directive would create a gap in the protection of individuals in a domain that lies at the heart of electronic communications – and consequently also information society and eGovernment services building on electronic services – and would thus be totally unacceptable from a privacy perspective.

Concept of “public communications network” and “electronic communications services”

The ePrivacy Directive applies to the provision of publicly available electronic communication services in public networks. However, in practice, the notions of “*public communications network*” and “*electronic communications services*” are very often unclear. Services are increasingly becoming a mixture of private and public elements and it is often difficult for regulators and for stakeholders alike to determine whether the ePrivacy Directive applies in a given situation. For example, is the provision of internet access to 30.000 students a public electronic communication system or a private one? What if the same access is provided by a multinational company, to 300.000 employees? What if it is provided by a cybercafé?

The Article 29 Working Party refers to its previous Opinions (WP 36³ and WP 126⁴) and once again calls for the definition of “*electronic communication services*” and “*public communications networks*” to be clarified, as the development of hybrid public/private networks needs to be taken into account.

The Article 29 Working Party invites the Commission to consult with it on this issue either through a Commission communication or another appropriate instrument.

³ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf

⁴ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp126_en.pdf

NRAs

Some references to the NRA (national regulatory authority) in the Proposal seem to refer to the national telecommunications regulatory authority, while some others seem to refer to the data protection authority.

The Article 29 Working Party suggests introducing wording similar to Article 3(5) of the Framework Directive 2002/21/EC, so as to ensure that the national regulatory authorities and national data protection authorities co-operate with each other effectively.

Furthermore, the proposed Article 15a (4) "*Implementation and enforcement*" suggests consultation with the European Electronic Communications Market Authority. The Article 29 Working Party insists that it be consulted as well, and that an explicit reference to an obligatory consultation process be included to that end.

Finally, the Working Party considers it necessary to ensure that the proposed harmonisation mechanism does not prevent Member States from adopting additional security requirements in order to pursue the objectives set out in the ePrivacy Directive.

Article 3

The Article 29 Working Party agrees with the above mentioned EDPS Opinion, and finds this provision positive, as it clarifies that a number of RFID applications fall under the scope of the ePrivacy Directive.

Article 13 Unsolicited communications

The Article 29 Working Party notes trends in communication technology that depart from the traditional subscriber model⁵ and suggests that the term "*subscriber*" should be changed to "*user*" throughout Article 13, and a new Recital inserted to clarify the relation and roles of subscribers vs. users.

The newly amended ePrivacy Directive should protect users of short range wireless media against unsolicited communication as defined in Article 13. A more detailed clarification could be included by way of a new Recital.

Article 13.1.

In order to cover the constant development and changes of technologies, paragraph 1 should not refer to "*automated calling systems*", but rather to "*automated calling and communication systems*" in order to maintain a technology neutral approach whilst taking into account ongoing technological changes.

Article 13.6.

In the new Article 13.6 the Commission proposes to confirm the rights of individuals and legal persons to take legal action against infringements of national provisions adopted following Article 13 of the ePrivacy Directive. The Working Party recommends

⁵ e.g. through the increasing use of technologies such as Bluetooth which allow for a form of advertising that has become just as intrusive as spam, though the technological basis is different

extending this right to Article 5(3) of the ePrivacy Directive, so as to allow a legal right of action in case of infringements of national provisions prohibiting the use of spyware.

3. OTHER ISSUES TO BE CONSIDERED

(a) Privacy by design

The Working Party 29 advocates the application of the principle of data minimisation and the deployment of Privacy Enhancing Technologies⁶ by data controllers.

The Working Party calls upon European legislators to make provision for a re-enforcement of said principle, by reiterating Recitals 9 and 30 of the ePrivacy Directive in a new paragraph in Article 1 of this Directive.

(b) IP addresses

The Working Party 29 observes that in the context of the discussion of the ePrivacy Directive the issue of whether IP addresses are personal data has been raised. The Working Party 29 recalls that, in most cases – including cases with dynamic IP address allocation – the necessary data will be available to identify the user(s) of the IP address.

The Working Party noted in its WP 136⁷ that "... *unless the Internet Service Provider is in a position to distinguish with absolute certainty that the data correspond to users that cannot be identified, it will have to treat all IP information as personal data, to be on the safe side....*" These considerations will apply equally to search engine operators (WP 148⁸).

(c) Article 5 (1)

The Article 29 Working Party recalls that this Article imposes an obligation to ensure confidentiality of communications irrespective of the nature of the network and whether the communication crosses borders to non-EU member states.

Providers of electronic communications services should step up their measures in order to strive to better protect all the individuals who are engaged in electronic communications involving parties situated in non-EU states. The review of the ePrivacy Directive is the appropriate forum to affirm civil rights in this regard, in particular to ensure transparency in the mechanisms used for the conveyance of communications.

4. FINAL REMARKS, CONCLUSION

The Article 29 Working Party calls on the European legislators to consider the issues highlighted in this Opinion.

Done at Brussels, 15 May 2008
For the Working Party
The Chairman
Alex Türk

⁶ COM (2007) 228 final

⁷ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp136_en.pdf

⁸ http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp148_en.pdf