1611/06/EN
WP 126

Opinion 8/2006 on the review of the regulatory Framework for Electronic Communications and Services, with focus on the ePrivacy Directive

Adopted on

26th September 2006

Set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

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

having regard to its Rules of Procedure, and in particular Articles 12 and 14 thereof,

has adopted the following Opinion:

1. Background

The European Commission has adopted its Communication on the Review of the EU Regulatory Framework for electronic communications networks and services {SEC (2006) 816} {SEC (206) 817} on 29 June 2006. The Communication reports on the functioning of the five directives of the regulatory framework for electronic communications networks and services[1], explains how the framework has delivered its objectives, and identifies areas for change.

The Communication is complemented by a Commission Staff Working Document {COM (206) 334 final}, where proposed changes are implemented. Prior to drawing conclusions presented in the Communication, the Impact Assessment captures the broader range of options considered. These above mentioned documents launched a formal public consultation on the future of the electronic communications regulatory framework on which comments are requested by 27 October 2006 at the latest.

As a following step, the Commission will draw up legislative proposals for modification of the regulatory framework, while taking into account comments received. The legislative proposal will then be presented to the Parliament and the Council.

The Review also includes the ePrivacy Directive, which belongs to the electronic communications package. The Working Party 29 wishes to contribute to the public consultation with focus on the ePrivacy Directive as follows.

2. General comments

The Article 29 Working Party's main concerns relate to personal data processing over and via electronic communications and its security as it raises a number of data protection issues which the Article 29 Working Party would like to address in the present Opinion.

[1] Directives 19/2002/EC OJ L 108, 24.4.2002, p.7, 20/2002/EC OJ L 108, 24.4.2002 p. 21, 21/2002/EC OJ L 108, 24.4.2002, p. 33, 22/2002/EC OJ L 108, 24.4.2002, p. 51, 58/2002/EC OJ L 201, 31.7.2002, p. 37

While evaluating the Communication with focus on the ePrivacy Directive and possible changes to be introduced therein, the Working party 29 would like to refer to its Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector[2]. Various proposals suggested in that Opinion however were not reflected and therefore the Working party wants to enumerate them again:

(1) In the mentioned Opinion the Working Party 29 emphasised that the fact that provisions of the ePrivacy Directive only apply to provision of publicly available electronic communications services in public communication networks is regrettable because private networks are gaining an increasing importance in everyday life, with risks increasing accordingly, in particular because such networks are becoming more specific (e.g. monitoring employee behaviour by means of traffic data). Another development that calls for reconsideration of the scope of the Directive is the tendency of services to increasingly become a mixture of private and public ones.

(2) The Working Party notes that both definitions 'electronic communications services', and 'to provide an electronic communications network' are still not very clear and both terms should be explained in more details in order to allow for a clear and unambiguous interpretation by data controllers and users alike. The unclear definitions give rise to several questions such as for instance "can a cyber café be considered as a provider of an electronic communications network"? Although such questions should be easy to answer, this is not always the case.

(3) Furthermore, the Article 29 Working party in its previous Opinion 7/2000 referred to Recital 25 of the ePrivacy Directive, regarding the use of cookies. In Recital 25 it is mentioned that the users should have the possibility to refuse the storage of a cookie on their personal computers. The Article 29 Working party fully supported this point of view. However, the last paragraph of Recital 25, stipulating that access to specific website content may be made conditional on the acceptance of a cookie, might be contradictory with the position that the users should have the possibility to refuse the storage of a cookie on their personal computers and therefore may need clarification or revision.

3. Specific Comments related to various paragraphs

Staff working document, Section 5.8 Improving enforcement mechanisms under the framework

This section concerns the need to adjust the enforcement mechanisms and powers available to authorities implementing the ePrivacy Directive.

The document states that fines for failing to comply with regulatory measures have proved inadequate: *"fines for breaches of the ePrivacy Directive are too light and enforcement uneven"*.

[2] http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2000/wp36en.pdf

It might be the case that the perceived varying levels of enforcement are caused not by provisions of the ePrivacy Directive but by differences in transposition into national laws. For example, Member States have enacted different interpretations of Article 13 (2) as well as different maximum penalties for a breach of this Directive.

In this respect, while increased and harmonised penalties may be a more effective deterrent, they alone may not address the perceived unevenness of enforcement. In addition, it is not necessarily the penalties available that determine the frequency with which enforcement powers are exercised. The nature of those powers and the mechanisms by which they are exercised may be a more important factor.

In some Member States DPAs have limited investigatory powers which, for example may not give them a right of access to the communications data needed to establish evidence of breaches of the Directive.

If in several Member States current enforcement powers do not enable the regulators to take swift action, this should be addressed. Another difficulty for enforcement is the fact that many spammers fall outside the jurisdiction of authorities within the EU. This should be resolved by close co-operation with regulators in other countries.

As regards the explicit right of action against spammers mentioned in the Staff working document, it is not clear how this would be any different to the current situation where the relevant authority can take enforcement action against those breaching the current Directive.

Staff working document, Section 7 Security

This section has a key proposal to extend and strengthen security provisions. The provisions in the ePrivacy Directive will be merged with those in the Universal Service Directive and form one specific chapter in the Framework Directive dedicated to security provisions.

While the strengthening of security provision is likely to be of benefit to consumers' privacy interests, it is unclear what benefit there is in formulating a specific hybrid chapter. Indeed, it could be argued that rather than, as the Staff working document puts it, highlighting the importance of the subject, removing the security provisions from the ePrivacy Directive would send the message that security merely concerns networks, competition and network providers, whereas in fact it also regards protecting the fundamental right to privacy as expressed in the ePrivacy Directive.

The Article 29 Working Party wishes to add that instead of addressing 'security' in its broadest sense, the attention should be given to specific aspects of security - not only 'continuity' and 'confidentiality', but 'integrity' of data as well, and in particular issues that have to do with authentication vs. anonymity. As a lack of adequate authentication procedures might lead to the creation of fraud schemes and reduce users' confidence in electronic communications, a subsection 'Identity Fraud' could be added to the introductory text of Chapter 7. In this subsection it may be argued that both confidentiality and timely deletion of excessive personal data contribute to the prevention of identity theft.

However, when addressing authentication issues, it has to be kept in mind that, in principle, individuals must be able to use public e-services anonymously. Therefore, before any proposal or change that relates to authentication issues is made, a thorough analysis of the accessibility of e-services must be carried out, since free communication is pivotal. This might reveal that various

forms of fraud will be countered by mandating authentication by service providers. Research in this area would be welcomed.

Staff working document, Section 7.1 Obligations to take security measures, and powers for NRAs to determine and monitor technical implementation

This section puts forward the idea that the present framework allows too much room for service providers to assess the adequacy of their own security measures. In the light of increased security threats, the document proposes clarification of the terms expressed in Article 4 of the ePrivacy Directive for the purpose of increasing the effectiveness of security measures.

This clarification would take the form of new obligations such as: measures to address security incidents; requirement to respect guidance issued by regulators; contractual provisions informing consumers of actions to be taken in the event of a security breach.

Firstly, it is unclear how any of the above proposals add anything to the existing framework other than to codify what most regulators would already expect to be in place. It is unlikely, for example, that a regulator would entertain the notion that a service provider whose security measures did not include procedures to address security incidents and minimise the impact on consumers was in compliance with the ePrivacy Directive.

Secondly, it must already be the case that whether a service provider ignores guidance from the regulator would go some way to determining whether that service provider was in breach of Article 4 of the ePrivacy Directive. It is therefore difficult to see how obliging providers to follow such guidance goes any further than a responsible regulatory approach to existing provisions.

Thirdly, it is unclear how contractual provisions informing customers of action they could take in the event of a security breach would be any more than a cosmetic exercise.

By mandating such provisions, the proposals also risk increasing the regulatory burden not just on industry but on the regulator. Because of the nature of the industry it is not feasible for a DPA to set out security provisions in the form of binding instructions. The measures have to be industry specific, they change too quickly for an authority to monitor the whole industry and there are, of course, large numbers of specialised security experts who are better equipped to consult on security matters and to perform audits.

Clarification and binding instructions should come from an industry specific authority rather than data protection specialists. It is also important to avoid heavy handed regulation as mentioned in the Staff working document itself (footnote 30) *"addressing security requires looking beyond regulation"*.

Staff working document, Section 7.2 Notification of security breaches by network operators and ISPs

In the light of the last comments made above, the Article 29 Working Party welcomes the proposal to require notification of security breaches; however, it has to be pointed out, that the Communication does not envisage any sanction if a network operator or ISP fails to inform the NRA.

The Article 29 Working Party also anticipates industry concerns that this might appear 'special treatment' for one industry when others have no such requirement to notify. However, the Article 29 Working Party recognises that such requirements are a current 'hot topic' and, more importantly, that this is more 'light-touch' regulation with little extra burden for those service providers who implement appropriate measures and a real market-led deterrent to those who wish to cut corners.

On the other hand, it has to be pointed out that none of the security breaches which recently hit the news in the US (Choicepoint, LexisNexis, Bank of America, Time Warner, etc.) involved ISPs. The Article 29 Working Party would like to suggest that obligation to notify should also be considered for "data brokers", banks or other online service providers. Even if they are not per definition Internet Service Providers they are the ones most concerned by any security breaches.

According to the proposal, the ISP shall notify only their customers' victim of any breach of security. However in case of important breaches, (the Communication does not intend to define different levels of breaches or when a breach is subject to notification) all the customers of the ISP shall be informed and not only the "victims". The legislative proposal should set up rules for classifying different levels of breaches.

Providers of access infrastructure and providers of services

The Communication distinguishes between providers of access infrastructure and providers of services. Article 3 of the current ePrivacy Directive defines the processing of data to which regulations apply. Whereas it used to be clear who was to be considered a provider of a publicly available electronic communications service, developments in the realm of eCommunications may make it more difficult for consumers to know who actually is rendering a service. Indeed, they may access a service via a portal and the service may involve several parties.

When issues like providing information and giving consent are concerned, it may not always be clear who is responsible for informing users or to whom consent is to be given. At the same time there might be a risk that service providers erroneously redirect users to an access or network provider, if that is the one that takes care of specific aspects of the service in a technical sense.

Anticipating the specific roles providers of access infrastructure and providers of services may have, it may be worthwhile to investigate whether regulations on the processing of personal data and the protection of privacy in the electronic communications sector need accentuation to prevent any misunderstanding concerning at whom the regulations aim. Therefore the legislative proposal should lead to the clarification and not create more confusion.

4. Conclusion

The Article 29 Working Party welcomed the opportunity to comment on the review of the eCommunications package, with focus on the ePrivacy Directive. The Article 29 Working Party wishes first of all to recommend improvement of security measures and wants to emphasize that protection of users and creating their trust into eCommunications should also be seriously taken into account while improving the security of infrastructure.

The Article 29 Working Party also suggests that the issues surrounding online applications should be addressed. These include security concerns, responsibility by the operators as well as clarification of both legal status and of the data controller.

The Article 29 Working Party wants to underline that while supporting improvement of security measures, it does not support any measure that leads or might lead to more surveillance or content blocking.

The Working Party reserves the possibility to comment on the Directive as it evolves.

Done at Brussels, on 26 September 2006

For the Working Party

The Vice-Chairman
Jose Luis Piñar Mañas