March 2005

ETNO RD on article 29 WG working document on data protection issues relating to IPR

Executive Summary:

ETNO presents its views on the Art. 29 working document taking account of the need for clarification of the application of data protection principles in the field of DRM and enforcement of copyright.

Regarding DRM, ETNO highlights the fact that the use of new technologies to protect copyrighted works should not be detrimental to the fundamental right of protection of personal data. ETNO considers that workplace DRM systems may be operated legitimately within the context of the criteria outlined in Art. 29 WG's Opinion 8/2001.

Regarding enforcement of copyright legislation, ETNO emphasises the importance of guaranteeing fundamental data protection rights in the context of Internet communications. The EU has already established a balanced framework defining the liability of intermediaries for illegal on-line content. "Backdoor" modification of this framework through changes to rules on data protection and data retention should be avoided.

As the representative of 41 major European telecoms operators, ETNO thanks the Article 29 Group for the opportunity to comment on its Working Document. The paper deals separately with data protection issues relating to operation of DRM systems and "a posteriori" copyright enforcement activities. ETNO's comments are provided below under the same two headings.

Digital Rights Management

All ETNO Members are potential providers of DRM-based services. Some have already made significant investments in order to launch commercial operations.

In ETNO's view, deployment of DRM systems can contribute to a virtuous circle which will play a central role in the development of

eEurope. Such systems will ensure appropriate revenues for all players in the value-chain (content creators, rightholders and service providers), thereby promoting wider availability of high-quality digital content. Wider availability of such content will in turn attract more users to high-speed communications networks, thereby creating more demand for content.

Consumer confidence is one of the keys to this process. In particular, customers are more likely to take advantage of DRM-based services in the absence of fears regarding utilisation of their personal data.

Against this background, ETNO welcomes the Working Party's attempt to clarify the application of data protection principles in the DRM field. The Association fully shares the Working Document's central principle: use of new technologies to protect copyrighted works should not be detrimental to the fundamental right of protection of personal data[1].

The Association fundamentally disagrees with nothing in the Working Party's analysis. However, the reference to "workplace" applications of DRM (see section on "use of unique identifiers") does provide some cause for concern. The context of the reference (juxtaposed with the sentence "The Working Party seriously questions the use of identifiers for the purpose of tracing a priori every user in order to go back to a specific individual in case of a suspected copyright abuse") suggests some disapproval of such applications which ETNO believes to be unjustified.

Contrary to the impression given by the Working Party's document, such applications are not confined to the film and music industries. Firms ranging from car manufacturers to pharmaceutical companies may also use DRM systems to protect the IPRs and other commercially sensitive information contained in their internal documents. Such an approach can boost the competitiveness of European industry by permitting remote working on digital versions of documents which previously had to be confined in a single secure physical location.

The Working Document mentions two possible justifications for document tagging ("…if the link is necessary for the performance of the service or if the individual has been informed and has consented to it.") but workplace DRM applications seem unlikely to qualify for either of these exemptions:

a) Since no money changes hands, they may not be considered as provision of a service;

[1] The protection of personal data has been explicitly recognised as a Fundamental Right by Art. 8 of the Charter of Fundamental Rights of the EU.

b) The Article 29 Working Group has already suggested that an employee's consent generally cannot be used to legitimise processing of personal data by his/her employer since such consent will rarely be given completely freely (see Opinion 8/2001 on the processing of personal data in the employment context).

ETNO considers that workplace DRM systems may nevertheless be operated legitimately within the context of the criteria outlined in Opinion 8/2001.

Enforcement of copyright

Rightholder requests for the names and addresses of alleged copyright infringers have created serious dilemmas for many ETNO Members during recent years. On the one hand, we acknowledge that effective enforcement of copyright legislation has a crucial role to play in promoting migration of users towards legitimate digital distribution services. On the other hand, e-communications operators have an obligation to protect the privacy of their customers.

ETNO Members are also concerned by the constant pressure to overturn the provisions of the E-Commerce Directive (2000/31/EC) on ISP liability in order to create a situation where intermediaries are liable for illegal content transmitted across their networks. The Directive states very clearly that no systematic obligation of surveillance or monitoring should be imposed on ISPs. Furthermore, Article 15 of this Directive establishes that ISPs should be subject to no general obligation to actively seek facts or circumstances indicating illegal activities.

Against this background, ETNO strongly supports the Working Document's emphasis on the importance of guaranteeing fundamental data protection rights in the context of Internet communications. Failure to enforce these rights strictly will lead to a perception of growing abuse of personal data, and this can only impact negatively on the take-up of information society services. In particular, ETNO fully agrees with the Working Document's conclusion that personal data can only be transferred in very defined cases provided by Law, only to Public Law Enforcement Authorities, and not to rightholders directly.

The EU has already established a balanced framework defining the liability of intermediaries for illegal on-line content. "Backdoor" modification of this framework through changes to rules on data protection and data retention should be avoided.