

Deutsche Vereinigung
für gewerblichen Rechtsschutz
und Urheberrecht e.V.

Deutsche Vereinigung für gewerblichen Rechtsschutz und Urheberrecht
Konrad-Adenauer-Ufer 11 • RheinAtrium • 50668 Köln

Der Generalsekretär

European Commission
DG Internal Market & Services
Rue de la Loi 200
B-1049 Brussels
Belgium

Konrad-Adenauer-Ufer 11
RheinAtrium
50668 Köln

Telefon (0221) 650 65-151
Telefax (0221) 650 65-205
e-mail: office@grur.de
www.grur.de

2007-04-17

**Questionnaire on the Liability Regime of Information Society
Intermediaries of November 3rd 2006 (MARKT/2006/09/E)**

Dear Madams and Sirs,

1. The German Association for the Protection of Intellectual Property (GRUR) is a scientific association; its statutory purpose is both to foster the scientific training and development concerning the law of intellectual property and the support of the legislative organs with regard to legislation in the respective area. The association unites members of all occupational groups, lawyers, judges, academic scholars, the executors of the specific public authorities as well as of the competent ministries dealing with the respective questions and further representatives of businesses. We would hereby like to submit our observations in regard to the above-mentioned questionnaire which specifically raises the question as to whether the current regime on the liability of information society intermediaries provides a satisfactory framework or requires complementary measures.
2. It appears that Germany has met the basic objectives of the Electronic Commerce Directive 2000/31/EC (ECD),
 - availability of the advantages of e-commerce to small and medium-sized companies as well as to citizens and
 - information services without internal frontiers.

It appears that legal obstacles constraining the free flow of information and e-commerce between the Member States have been removed in the course of the implementation of the ECD.

While some Scandinavian countries and the UK are in the lead, Germany is well on the path towards becoming an information society. Subsequent to a recent report by the Federal Bureau of Statistics (Statistisches Bundesamt), a share of 94% of commercial entities with at least ten employees has access to the internet which is slightly above average in the European Union (92% of EU-15). A share of 54% of all commercial entities takes advantage of the internet for the purchase of goods. As for the citizens, 62% of all private households are connected to the internet and there is an increasing use of the internet for the sale and purchase of goods. The Federal Bureau of Statistics reports that already in the first quarter of 2005 46% of all private users made a purchase online. In particular, the auction house “eBay” appears to be the basic forum for e-commerce in Germany. Nowadays, eBay reports more than 20 million members of which only slightly more than 200 000 are commercial. This is roughly a quarter of the total population in Germany.

The usage of the internet as a source of information for private, professional and educational purposes is still increasing – in 2002 46%, in 2004 58% and in 2005 61% of the total German population.

3. While Germany is on a good path to develop e-commerce as a standard in the daily life of citizens and businesses, the implementation of other aims of the Directive, namely the high level of protection for consumers and public health, is under threat. The importance of such high standards of protection has been reaffirmed in the Unfair Commercial Practices Directive of May 11th 2005 (2005/29/EC).

There are namely two issues which give reason for severe concern –

- the explosion of unsolicited commercial communication and
- the volume and nature of counterfeit trade via the internet.

It appears that the strong ban of any type of unsolicited commercial communication (which has already been legally imposed by Art. 7 (2) of the German Unfair Competition Code of July 2004) is completely ineffective and lacks enforcement. German consumer protection associations report a significant increase of unsolicited telephone calls and emails to private recipients. Therefore Germany has just recently passed a bill for a new tele-media-law specifying the obligations under Art. 7 (1) ECD and imposing an administrative penalty of up to 50 000 EUR for any kind of violation.

4. As to the volume and nature of counterfeit trade via the internet, it is to be emphasized that such trade does not only affect the economic interests of trademark owners as well as of owners of other intellectual property rights and authorisations for the sale of medicinal products – to give only two examples on the suppliers’ side. Rather, product piracy, which is expanding via the internet, does and will also persistently endanger economic and health-related interests of consumers. Recent studies have shown a steady increase in product piracy and the distribution of harmful counterfeit medicines in the e-commerce sector. This may be demonstrated by giving some examples:
 - a) The OECD study “THE ECONOMIC IMPACT OF COUNTERFEITING AND PIRACY”, submitted in December 2006, revealed once more that the trade with counterfeit products and plagiarised brand products is further growing. The study

also showed that the “online environment is attractive to counterfeiters and pirates for a number of reasons” (cf. 3.5.1). In late January 2007 the World Intellectual Property Organization (WIPO), Interpol and the World Customs Organisation organised a congress in Geneva dedicated to the struggle against product and trademark piracy for the third time. All experts agreed that it would be necessary to make increased efforts to combat product and trademark counterfeiting, also in the field of e-commerce. This view is also shared by the majority of EU Member States and the EU Commission, which intends to deal with this important issue actively.

- b) Recently the Vienna-based INCB (International Narcotics Control Board), established by the WHO, warned that the flood of counterfeit medicines now available in many countries may have fatal consequences for consumers. In its Annual Report 2006, the Board stated, in pertinent part:

“Through internet pharmacies, internationally controlled drugs such as benzodiazepines, opioids, stimulants and barbiturates can be obtained without a prescription. According to estimates of the World Health Organisation (WHO), at least 10 per cent of the world’s drugs are counterfeit.”

(cf. also WHO, “Counterfeit medicines”, Fact Sheet No. 275, February 2006).

The risks involved in the illegal distribution of other prescription counterfeit medicines without medical control such as slimming products, potency products, psychotropics and products against influenza have also been repeatedly emphasized by the EU Commission and the EMEA (cf. e.g. press release of the Vice President of the EU Commission Günter Verheugen at http://ec.europa.eu/commission_barroso/verheugen/index_de.htm; EMEA-Report “Counterfeit Medicines” at <http://www.emea.eu.int/Inspection/Counterfeits.html>).

- c) Considering these facts, GRUR takes the view that it is necessary to submit a consistent legislative overall concept taking due account of the legitimate interests in the development of e-commerce, the interests of the owners of trademark and other intellectual property rights as well as the economic and health-related interests of consumers. However, a selective unilateral consideration of the liability risks of e-commerce providers alone would not be an appropriate response to this complex problem.

The liability standard applied by Germany’s Federal Court of Justice (Bundesgerichtshof) in its Rolex/Ricardo decision (BGH, GRUR 2004, 860 ff. – Rolex/Ricardo; the **attached** decision is also called “Internet-Versteigerung”) does not constitute specific e-commerce-related law. It is also applied to print media in a comparable manner (cf. only BGH, GRUR 1990, 1012 – Pressehaftung I; GRUR 1992, 618 – Pressehaftung II; GRUR 1993, 53 – Ausländischer Inserent). A check for reasonability based upon the balancing of interests is always required as a restriction to this standard. With regard to e-commerce, this corrective measure explicitly requires a review of the feasibility under technical, economic and time

aspects. It should be noted in this context that more recent studies point out that the VeRO programme offered by eBay does not exhaust the possibilities of what is technically feasible and reasonable (cf. Christianini and Shawe-Taylor, *An Introduction to Support Vector Machines and Other Kernel-Based Learning Methods*, Cambridge University Press, 2000; E. Michelakis, I. Androutsopoulos, G. Paliouras, G. Sakkis, P. Stamatopoulos (2004), *Filtron. A Learning-Based Anti-Spam Filter*, Proc. First Conference on Email and Anti-Spam (CEAS), Mountain View, CA. <http://www.ceas.cc/papers-2004/index.html>; C. Nadeau and Y. Bengio, *Inference for the Generalisation Error*, *Machine Learning*, Vol. 52 (2003), p. 239-281).

5. Both, the volume of unsolicited commercial communication and the risks caused by counterfeit trade raise the question as to whether the instruments of the ECD provide sufficient protection or require improvement:
 - a) As to the problem of unsolicited commercial communication, it appears that the rules of Art. 6 and 7 of the Directive lack enforcement. However, in Germany legislation has already responded to this threat which is in compliance with the authorisation for further sanctions in Art. 20 ECD. Subsequently, there is no need for further complimentary measures on a community level.
 - b) As for the liability of intermediaries, the alarming dimension and character of counterfeit trade via the internet require a thorough review of the current system. It threatens the high level of protection for final consumers and public health as well as the effective protection of intellectual property rights within the community.
6. In this regard, GRUR is severely concerned by the various attempts of parts of the internet industry to challenge the judgement of the Federal Court of Justice of March 11th 2004 as a violation of the current regime of articles 12 – 15 of the ECD. Such complaints are unfounded. They also aim for further restrictions of liability which necessarily will result in a further dilution of protection and in an increase of internet crime:

First of all, the Federal Court of Justice is blamed by the internet industry for having imposed a general obligation to monitor the content of internet transmissions through the back door and thus having violated the general principle of Art. 15 ECD. Such a complaint is unfounded. In its judgement in the matter *Rolex/Ricardo* (BGH, GRUR 2004, 860 ff.), the Federal Court of Justice has made it precisely clear that intermediaries are not generally obliged to monitor the content of their transmissions in order to seek facts or circumstances indicating illegal activity. Quite to the contrary, the Federal Court of Justice has emphasised that an obligation to review and monitor the content would only apply under specific circumstances and with regard to the following:

- a clear infringement of intellectual property rights of a third party;
- the infringement is easily detectable; or
- an obligation of the provider to monitor the content is reasonable with regard to a full review of the overall circumstances of each individual case.

In particular with regard to the last requirement, the Federal Court of Justice has held the auction house Ricardo liable because Ricardo was also taking advantage of the sale of counterfeit watches by receiving a fee for each purchase. In that regard, it is more than questionable whether the principles of the Rolex/Ricardo judgement can result in a comparable injunction against mere access- or cache-providers as addressed in articles 12 and 13 ECD.

In addition, it is worth mentioning that the ECD has already foreseen the possibility of injunctive orders against service providers in its Articles 12 (3), 13 (2) and 14 (3). In particular, the instrument of a notice and takedown mechanism as addressed in Art. 14 (1) lit. b may well be interpreted as an immediate obligation under the Directive to constantly disable access to unlawful information after having received respective notice. Practically, there is no difference between blocking unlawful content and disabling the access to it (see also Art. 13 (1) lit. e).

Finally, it is also worth noting that the Federal Court of Justice has only dealt with the liability of service providers with regard to the prevention of illegal content. It has on the other hand reconfirmed that this should not affect the exemption from criminal or financial (damages) liability.

7. The Federal Court of Justice has interpreted the provisions of the national law implementing the ECD as self executing; i.e. establishing respective obligations between the parties. In that regard, GRUR strongly opposes any attempts trying to submit the assessment of liability of service providers to a mandatory prior court ruling. Such a measure would not only invalidate the aims of the Enforcement Directive dated April 29th 2004 (2004/48/EC). It would also result in an unjustified workload for the national courts. It is already foreseeable that a mandatory obligation to go to court even in clear cases will invalidate the access to speedy and interim proceedings as granted under Art. 18 (1) of the ECD.
8. With regard to the question of the functioning of the current framework, complementary measures, if any, should focus on the problems of unsolicited commercial communication and the role of internet trade of counterfeits. GRUR suggests no more than two alterations/amendments of Articles 14 and 15 of the ECD which should significantly reduce the current insufficiencies of enforcement and shortcomings of protection.
9. Both suggestions are – to a certain extent – related in that that the anonymity/pseudonymity of the internet is one of the basic if not the determining factor for these two phenomenons. It is undeniable that in that regard – at least in Germany – a misconception of personal data protection laws has contributed much to the current situation. In particular, commercial communication for the sale of goods on platforms like auction houses takes unreasoned advantage from the anonymity and pseudonymity of private users. This may be illustrated by the relationship between the allegedly only 200 000 commercial members of eBay against the number of 19 800 000 allegedly private members who usually act under a pseudonym rather than under their actual name and address.

The first proposal of GRUR therefore aims for a better enforcement of Art. 6 b) of the ECD in order to make unlawful activities in the internet less attractive. Such enforcement can only be achieved by way of lifting the current veil of pseudonymity and by drawing clear lines to distinct data protection from commercial transparency.

The information required by Art. 6 b) ECD usually is – or should be – at least stored by the intermediaries. Subsequently, the ECD should clarify that the intermediaries are not obliged to keep any personal data confidential which the ECD requires to be published alongside with commercial communication on the internet. GRUR therefore suggests the following amendment to the ECD which might be worked into the framework of a new Article 15 a) as follows:

“Member states shall ensure that service providers, notwithstanding the liability exemptions under the above Articles 12, 13 and 14, shall be obliged to disclose the identity of a natural or legal person to national authorities, courts or stakeholders of intellectual property rights, if

a) the nature of a communication as commercial is clearly identifiable, and

b) the identity of the natural or legal person behind the communication is not identifiable from the communication, and

c) a severe risk of illegal activity or information is established.”

10. With regard to the issue of counterfeit trade on the internet, GRUR suggests to specify the terms of Article 14 (1) lit. b in order to underline a possible obligation of host providers to prevent further unlawful activities and thus contribute to the defense against counterfeits as follows:

“...the provider, upon obtaining such knowledge or awareness of sufficient significance, acts expeditiously to remove or to disable access to the information and to take reasonable precaution to prevent a repeated storage of the information.”

Such new wording should help to avoid the misunderstanding that the notice-and-take-down-procedure is a measure which does not go beyond an immediate response to a certain complaint. It follows already from the recitals 40 and 45 ECD that service providers may well have a duty to also prevent illegal activities. In addition, it follows from recital 44 that particularly host providers who collaborate with the recipients of their services shall not benefit from the exemptions for ‘mere conduit’ or ‘caching’.

.....
Dr. Hans Peter Kunz-Hallstein
(President)

.....
Dr. Michael Loschelder
(Secretary General)