Brussels, 29 December 2009

The signatories of this paper (contact information and ID numbers page 8) represent companies that produce, and distribute movies, home entertainment and television programs in Europe and internationally. Over the past decade, these companies have been working to embrace new technologies and to license exciting new digital services[1]. We understand that the 1995 EU Data Protection Directive may be subject of a review, and appreciate the opportunity given by the European Commission to provide our views. This Directive provides a sound framework and many of its rules are still very relevant. But there are complex challenges which the drafters of the Directive could not have considered more than fourteen years ago. This submission addresses:

- The respect of privacy - and the respect of the rule of law in general in order to promote a responsible Internet.
- Our experience and the legal research conducted over past years on the interface between privacy and copyright enforcement.
- The fragmentation of the rules between the Member States and the legal and practical difficulties for legitimate parties to enforce their rights.
- Those who "play" with privacy rules (example: web site providers who manipulate/misuse the IP addresses of others to facilitate illegal activities).

Section IV includes proposals. There are already helpful legal provisions/court cases to which this submission makes extensive reference, but solutions must be encouraged by the European Commission to ensure the protection of privacy and other rights. The Commission should ensure appropriate implementation of the existing provisions of the Directive that are meant to help legitimate parties to protect their rights. An Interpretative Communication clarifying how certain provisions of the Directive can be used to ensure that privacy is protected while other rights are also safeguarded could also be helpful. If not progress is made, we would strongly encourage the Commission to propose a legislative amendment. We are certain that solutions can be formulated to address the current complexities and the issues raised in this submission, and would very much appreciate an in-depth discussion with the European Commission on this specific subject.

[1] See for example a very interesting website in the UK www.FindanyFilm.com that helps direct consumers to legal offerings (other countries are looking at similar initiatives). More generally, recent figures from the European Audiovisual Observatory refer to some 700 VOD (broadly defined) services in Europe of which over half are online. In the US, the MPAA offers a list of legal services which users can access on the MPAA website.

I. General comments on Directive 95/46/EC:

There are three main EU privacy "Directives"[2] - and the one adopted on 24 October 1995 provides a general framework. It is intended to protect the right to privacy and to ensure the free flow of personal data between Member States (Article 1 of the Directive). As is clear from this latter point, it is also very much an Internal Market Directive - meant to advance the EU's single market objective. It covers all types of processing and is THE general, basic data protection instrument in the EU.

This instrument provides a sound framework with its principles and exceptions, and both its general approach and its flexibility ensure that this legislation is still up to date in many respects. The 1995 Privacy Directive in general terms provides the conditions for legitimate data processing, information to be given to the data subject, the possibility to access and correct data, conditions for the disclosure of data to third parties and transfer of data to non-EU countries, provisions on security, as well as a limited number of exceptions. Many of its principles (and exceptions) remain fully relevant fourteen years later. However, it is regrettable that the Directive has led to the negotiation of only one code of conduct in all these years. Another major concern relates to the differing interpretations of the Directive by national courts and authorities. Such differences make it extremely difficult to anticipate how the rules will be applied in practice and result in a market that remains in reality fragmented, complex, with an inconsistent application of the rules.

The challenges that have appeared in the past decade are very much due to the rapid development of new services and their attractiveness for Internet users (it is interesting in this respect to note a certain paradox: Internet users care about their privacy, but they do not hesitate to knowingly and freely provide a lot of information about themselves in the online environment). In this new context, data privacy has taken on a major role. The day to day reality however also reveals that many civil wrongs and criminal acts occur online, and that measures must be taken to combat these illegal acts in order to ensure that the Internet is a trusted and reliable medium for communication and commerce. In other words, privacy needs to be respected – and the rule of law in general needs to be respected. Recently, the ECJ stressed the need for Member States to strike a fair balance between the fundamental right to privacy and other fundamental rights[3]. This is an important statement - and it is an essential challenge.

Solutions need to be found to ensure the enforcement of other fundamental rights and to ensure a means of redress for victims whose rights have been abused online. In the context of the development of new services, it seems essential to protect privacy but

[2] The EU Framework Directive on Data Protection (95/46/EC), the EU Data Retention Directive (2006/24/EC), and the Directive on Privacy in the Electronic Communications Sector (2002/58/EC) which was very recently updated by the telecoms package

[3] Promusicae v Telefonica, C-275-06, 29 January 2008.

also to question for which purpose. In other words, privacy is essential to protect individuals and their personal data. But privacy should not be used to protect criminals or those who have been involved in illegal or harmful activities.

II. A new environment with new challenges:

In the context of digital technologies, it has become even more relevant to protect citizens' identities as they surf the Internet, engage in file-sharing, participate in social networks, access e-government services, and make e-purchases. In the digital landscape, several types of cybercrime have appeared or have adapted themselves to the new environment: ID theft, defamation, phishing, selling of illegal medicines online, cyber-bullying and other offences against minors, etc. Again, protecting privacy (name, birth dates, bank accounts, etc.) is essential but as mentioned in *KU v Finland* in December 2008[4], although a right is fundamental, the guarantee of its application cannot be absolute and its application *"must yield on occasion to other legitimate imperatives".*

Here are a few practical examples:

- Shall a blogger be able to hide behind a right to anonymity in case of defamatory statements that have caused significant damage? More generally, does freedom of expression allow one to make any comments about anyone with complete anonymity? This question has been the subject of several commentaries and court cases at the national level[5].
- How to deal with the dramatic increase of ID theft? In March 2009, the OECD published a report on online identity theft which shows the extent to which such risk has been increasing, its impact on users' mistrust and the need for the States to have adequate legislation[6].

Every day, we read in the news about people who have suffered different types of online fraud, and there has generally been a substantial increase in cybercrime. Also, criminals have "learnt' to manipulate, change digital data. They have used these methods either to obfuscate their whereabouts, or to make potential victims believe that they are dealing with a legitimate entity. Many cybercriminals whose "business models" thrive on the theft of personal data in blatant violation of data protection and other laws hide behind these same rules to shield themselves from the authorities and their victims.

[4] KU v Finland ECHR judgment on 2 December 2008 (Application no. 2872/02)
[5] For example, in the Netherlands, Hoge Raad, November 25, 2005, Lycos/Pessers,
[6] http://www.oecd.org/document/44/0,3343,en_2649_34223_42420716_1_1_1_1,00.html

One of the most famous Internet writers/commentators, *Andrew Keen*[7], recently stressed[8] the need to promote a "*responsible Internet*" – this cannot be done if those who do not respect the rules, the "*social contract*", hide behind complete anonymity[9].

There have always been limitations to the principle of privacy in order to deal with specific and legitimate situations. Article 13 of the 1995 Directive gives Member States room to maneuver and to provide derogations to the general provisions of the Directive. It refers *inter alia* to the protection of the "*rights and freedoms of others*" - but there are also other grounds in the Directive that ensure the respect for privacy while protecting other interests (see in particular Articles 7 c), 7 f), and Recital 30). Article 8.2 of the ECHR also provides that there are specific situations where derogations are necessary to the privacy principle. Article 52 of the European Charter of Fundamental Rights also notes that limitations may be made (under specific conditions) "*if they are necessary and genuinely meet objectives of general interest recognized by the Union or the need to protect the rights and freedoms of others*".

Several court cases (of the ECJ and the ECHR) also recognize the need for a balance. For example, in *KU v Finland* (mentioned above): the ECHR noted that "*although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others*".

However, there is still huge uncertainty, divergence and even inconsistencies as to how Member States achieve this interface between fundamental rights in practice - this is a very important issue and a problem for all stakeholders[10] including for copyright owners.

III. What about rights-holders?

The companies we represent produce and distribute creative stories. Stories that make people escape from their everyday life, make them laugh, challenge society and even, on occasion, that help change the world. The development of online technologies has

[7] Andrew Keen, *"The Cult of the Amateur"* (2007) – A. Keen concludes *"let's use technology in a way that encourages innovation, open communication, and progress, while simultaneously preserving professional standards of truth, decency, and creativity" (p.205).*

[8] Andrew Keen was invited at an EIF event on 8 December 2009. His comments are available online at http://www.eifonline.org/en/articles/news/news.cfm

[9] See also in this context the EIF report 'The Digital World 2025". See also an interesting article in Der Spiegel 10/08/2009 of Thomas Darnstädt, Frank Hornig, Martin U. Müller; Marcel Rosenbach and Hilmar Schmundt.

[10] ISPs themselves use all kinds of technologies to protect their network infrastructure against spam, spyware, viruses etc. Inevitably, the use of such technologies will require the processing of IP addresses.

created fantastic opportunities to reach new audiences. At the same time, copyright holders are suffering from ever increasing levels of piracy. This is a global phenomenon. Europe is no exception, with local interests suffering substantial losses[11] .

The first court case that dealt with the interface between privacy and copyright protection at the EU level is *Promusicae (ECJ - 29 January 2008).* This case dealt with the following question: are Member States allowed to exclude the possibility of disclosing data relating to copyright infringers in civil cases? The Court ruled that Community law neither forces Member States to allow the disclosure of data to private parties for civil enforcement purposes, nor does it preclude Member States from doing so. It also stressed that there must be a balance between privacy and other fundamental rights (such as the fundamental right to property, which includes copyright). The ECJ noted that Member States can adopt measures to restrict the obligation of confidentiality "*where that restriction is necessary inter alia for the protection of the rights and freedoms of others*" (Paragraph 53 of the judgment)[12].

This case recognizes the need for a balance between rights - it also gives the possibility for Member States to allow such disclosure. The problem however is that it sends the issue back to the national level for diverging resolutions in parliaments and the courts, which shows that on this specific question of communication of data in the context of civil proceedings, there is NO harmonization and a fragmentation of the EU's single market.

Several other cases have recognized the need for a balance specifically in the field of copyright[13]. In addition the recently adopted e-privacy Directive includes a recital which codifies the *Promusicae* approach[14] (Recital 62). But as mentioned above, there is no specific harmonization and still uncertainty at the national level as to whether data can be communicated in particular in the context of civil proceedings to entitle copyright owners to protect their rights – and this despite existing grounds in the 1995 Privacy

[11] Independent research has been commissioned by the local industry bodies in a number of European countries, including in the UK, Spain and France. In the UK, for example, the impact of piracy on the film industry due to illegal downloads amounts to £53 million. In France, last year the local anti-piracy organization commissioned research which, over a given period, established that there were approximately 440,000 illegal downloads of movies each day.

[12] See Comments of Christopher Kuner, EIPR issue 5 (2008) *"Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of justice".*

[13] LSG v. Tele2 (ECJ - 19 February 2009), Judgment of the Solna District Court (Sweden) on 25 June 2009, a Swiss Federal Administrative Court judgment of 27 May 2009 (Swiss Federal Data Protection Commissioner v. Logistep).

[14] Recital 62 states that *"When implementing measures transposing Directive 2002/58/EC (Directive on privacy and electronic communications), the authorities and courts of the member States should not only interpret their national law in a manner consistent with that Directive, but should also ensure that they do not rely on an interpretation of it which would conflict with fundamental rights or general principles of Community law, such as the principle of proportionality*".

Directive (Article 13.1g) but also Article 7c) and 7f)) which provide criteria for making the processing legitimate, as well as in other EU Directives (on privacy and on copyright).

Why this issue is important and which problems do we face?

For creators, copyright is the basis on which the work is exploited, on which investment is recouped in order to remunerate various participants in the creative process and to finance new works. In the film sector, many films are illegally made available on the Internet while still in theaters (sometimes even before their release!). And this is the result of the "work" of very organized "release" groups. As a consequence, there is a direct negative impact on the film distribution channels, on the possibility for film producers to recoup their investments, and to invest in future works. This means also a direct negative impact on the level of employment in the film sector and other sectors that the film industry employs.

In theory, several remedies could be available to tackle the various forms of copyright infringements on the Internet, but in practice, it is very different[15]:

- Criminal action is sometimes possible - but often budgetary pressures and lack of resources means that the police and law enforcement officials do not have the possibility to deal with these complex cases.
- Civil relief could be possible against web sites that are providing or facilitating access to illegal material but in many cases it is complicated/expensive/lengthy to obtain the data of those who are engaged in these infringing activities i.e., the operators of the sites. If they want to launch civil proceedings against a web site, one of the first things rights-holders will have to do is to gather evidence that this web site has been providing or facilitating the dissemination of illegal content, which means that at some point, data will have to be processed. This procedure is often complicated, and in some cases it cannot be carried out due to strict interpretations of data protection rules.

In this context, rights-holders have suggested using less formal procedures to enforce their rights ("notice and takedown" procedures to facilitate the takedown or blocking of access to an illegal web site i.e., one on which the vast majority of the content is infringing; content filtering systems to prevent the uploading of infringing content on these sites; system of "graduated response" to deal with the illegal use of peer-to-peer services). But none of these approaches can work without the cooperation of the parties involved.

The reality - and problem - is that there are huge differences between the Member States on the approach to the interface between privacy and copyright enforcement.

[15] See Comments of Christopher Kuner in the EIPR issue 5 (2008) *"Data Protection and Rights Protection on the Internet: The Promusicae Judgment of the European Court of justice".*

We have done in-depth research and found major divergences between countries and even sometimes divergence of views between the courts and the data protection authorities (differences as to the definition of IP addresses, as to the existence of a special procedure between ISPs, rights-holders and the data protection authority; as to the existence of a specific procedure to compel ISPs to disclose the identity of infringers; as to the disclosure of details to rights-holders to enable them to bring civil proceedings etc.).

It is at this stage extremely difficult, expensive, and uneven for our members and copyrights holders in general to enforce their rights – national anti-piracy organizations are doing their best at the national level but they often face difficult and inconsistent situations. What we need is more cooperation from those involved - and such solutions should be found. At this stage there is a huge risk of forum shopping by rogue service providers and no enforcement of the rules against them. In other words, it seems easier for a rogue ISPs to hide behind/play with privacy rules rather than for legitimate users to protect their rights granted by existing laws. Here are just a few examples of the consequences of today's inconsistencies:

- Some rogue ISPs (generally hosting providers) do not hesitate to intentionally use the rules/use technologies to hide who is behind a website – making it impossible to file a complaint or even send a cease and desist letter because there is no possibility to locate the operators of the site, who may be in several countries. These same websites that are protected by privacy rules are engaged in the daily theft of personal data.
- Much information is made available freely by users. People can see many things on a P2P network merely by logging on including the IP addresses of those involved. It is very easy for the operator of a P2P portal site or other types of sites (cyberlocker, video linking, usenet) as well as other users to obtain and use this data for illegal purposes. Some pirates even very proudly make their own picture/ID details publicly available. In this context, why in some countries is it so difficult for legitimate organizations charged with the defense of specific rights to deal with this information which, again, is being made freely available?
- Some criminals have been misusing the IP addresses of others to facilitate their illegal activities. Some web site providers and "talented" Internet users have also been "faking" IP addresses in order to mislead people as to the true whereabouts of a particular site – whether it is actually being hosted where it appears (this also shows how far IP addresses can be manipulated - and how it is difficult to assimilate them to personal data).

IV. Facing this challenge:

This position paper speaks about the research we have made in the past years, and our experience with data protection issues and the very specific issue of online piracy. We

have many materials (studies on data privacy and online enforcement, presentations on piracy with practical examples of the problems we face) at your disposal. Current efforts to deal with the interface between privacy and other rights in order to combat illegal activities on the Internet fall well short of what is needed to ensure that the rule of law applies online and to stimulate the trust necessary to make e-commerce flourish. This is we believe an essential issue for the coming months and years.

In a recent House of Lords debate in the UK (25 November 2009), *Baroness McIntosh of Hudnall* referred to the "*complex business of tackling the growing problem of online copyright infringement"* and stressed *"I have a residual worry about how the issues of privacy and data protection will be addressed and what the mechanisms will be for ensuring that the new legislation is fairly and proportionately applied. I hope the Minister can make some observations on that when he replies."* This statement reflects our views.

There are already important provisions in the 1995 Directive (Recital 30 - Articles 7c) and f) – Article 13.1 g)), but solutions must be envisaged/encouraged by the European Commission to ensure that privacy can be combined with the protection of other rights, and that it does not ultimately help those who don't respect the rules. The Commission should ensure appropriate implementation of the existing provisions of this Directive (and other instruments) that are meant to help legitimate parties to protect their rights. An Interpretative Communication on this issue - and clarifying how certain provisions of the Directive can be used to ensure that privacy is protected while other rights are also safeguarded - could also be helpful to ensure more uniform application of the rules in the short term. If not progress is made, we would strongly encourage the Commission to propose a legislative amendment specifying the right of legitimate parties/relevant intermediaries to process/disclose data - under very specific circumstances and conditions – to allow the effective protection of legitimate rights. We are certain that solutions are available, even in the very short term.

We would very much appreciate an in-depth discussion with the Commission on the issues mentioned above and on the solutions that could be developed at a pan-European level.

International Federation of Film Distributors Associations (FIAD): 74 avenue Kléber, 75116 PARIS - http://www.fiad.eu
International Federation of Film Producers Associations (FIAPF): 9 rue de l'Echelle, 75001 Paris - http://www.fiapf.org
International Video Federation (IVF): 83 rue Ducale, 1000 Bruxelles - http://www.ivf-video.org – ID number: 70 13 47 78 46 - 25
Motion Picture Association (MPA) – 46 avenue des Arts, 1000 Bruxelles - http://www.mpaa.org – ID number: 95 20 14 01 713 -39