ARTICLE 29 Data Protection Working Party

xxxx/05/EN
WP 104

Working document on data protection issues related to intellectual property rights

January 18, 2005

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 E (Services, Copyright, Industrial Property and Data Protection) of the European Commission, Internal Market Directorate-General, B-1049 Brussels, Belgium, Office No C100-6/136.

Website: www.europa.eu.int/comm/privacy

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

set up under Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995[1],

having regard to Article 29, Article 30(1)(c) and Article 30(3) of the above Directive,

having regard to its rules of procedure, and in particular Articles 12 and 14 thereof,

HAS ADOPTED THE PRESENT Working document on:

Data protection issues related to intellectual property rights

1. Introduction

The Working Party notes that the increasing exchange of information linked to the development of the Internet touches more and more the delicate question of control over copyright protected information. Issues at stake relate in particular to the rights and obligations of actors having interests in copyright protected information, and who are involved in the management of digital rights.

The Working Party acknowledges the necessity of implementing measures to safeguard the rightful interests of holders of intellectual property rights against alleged fraud. At the same time, the Working Party ("WP") has observed that some of these measures aimed at ensuring the effective protection of some copyright material against alleged unlawful exchange, taken at various levels by copyright holders, involve the processing of personal data of individuals. The first aspect the Working Party intends to address relates to the digital management of rights ("DRMs") which is currently developing, insofar as DRMs provide for the identification and tracing of individuals accessing legally protected information (e.g., songs, software) on the Internet. The second aspect relates to the possibilities available to copyright holders to enforce their rights against individuals suspected of copyright violation.

Considering the different levels where data protection issues arise, this document intends to recall not only the main legal principles to be complied with by copyright holders in the exercise of the rights, but also by other actors involved more specifically in the digital management sphere, such as the industry and service providers offering digital rights management technology.

a. Digital Rights Management

As regards the development of digital rights management, the WP notes that new technologies to identify and/or trace users are being established at the level of exchange of information as well as at platform level (i.e., verification of hardware/software).

As regards the exchange/downloading of information on the Internet, in case of transactions on copyright protected information, the access to such information is submitted more and more to

[1] Official Journal L 281, 23.11.1995, p. 31, available at:
http://europa.eu.int/comm/internal_market/privacy/law_fr.htm

preliminary control of the user's identity, which is completed by further tracing of the use of the information, through tags or digital watermarks. Users will for example, often have to identify themselves before being able to download a song from an official provider, and their profile will be completed with information collected through the unique identifier included in each piece of music downloaded by the user. In addition to the claimed purpose of control of the use of the information by the individual in compliance with DRM, the tagging is often used to profile and target advertisements to the users. As already stated by the International Working Group on Telecommunications, "Electronic Copyright Management Systems (ECMS) are being devised and offered which could lead to ubiquitous surveillance of users by digital works. Some ECMS are monitoring every single act of reading, listening and viewing on the Internet by individual users thereby collecting highly sensitive information about the data subject concerned"[2].

At the level of platforms, the Working Party has been following closely the developments of some industry projects, such as TCG, destined to ensure the trusted character of information included in and accessed from a computer platform. If such systems, as acknowledged by the WP, can have a very positive impact on the level of security of information, their potential applications are wide and could very well permit the distance verification of copyright compliance of the constituents of computer platforms. In its working document of 23 January 2004, the WP mentioned that "TPM-based applications could be used […] for instance by the content industry in order to regain the control of the distribution and use of digital content (including software) that they have lost with the advent of Internet and peer-to-peer applications". Such controls could happen on a routine basis, in the framework of any kind of contact between platforms, as "the use of TPM, promoted by such a strong representation from industry, is likely to become a de facto standard, a necessary feature to participate in the information society".

b. Enforcement of copyright

While control and tracing is developing at the source with the intention of checking "a priori" every user downloading legally information on the Internet, the protection of copyright information also leads most of copyright actors to take actions "a posteriori" and to conduct investigations towards users suspected of infringements.

Among the means used by right holders, the Working Party notes in particular the following:

Peer-to-peer tools available on the Internet have been identified as a major mean to find information on individuals making available on-line, or downloading, protected information. The research conducted by right holders is usually based on the collection of the IP address of the users[3]. This information is then combined with users' data as detained by ISPs. In some cases the right holders directly request the identity of the user to the ISP in order to send cease and desist letters to the users. In other cases copyright holders request the collaboration of ISPs so that they themselves send letters to the users concerned asking them to take down the alleged infringing material, or that they disconnect users from the network.

[2] International Working Group on Data Protection in Telecommunications, "Common Position on Privacy and Copyright Management" adopted at the 27th Meeting of the Working Group on 4-5 May 2000.

[3] While a few years ago many users were still assigned dynamic address, which changed at each connection to the Internet. The development of connections through cable or ADSL goes together with the assignation of permanent IP address to users. In case of a permanent IP address, which might become the rule with the development of the new IPv6 protocol, the tracing of Internet users will be even more easy (see in this regard the Opinion 2/2002 of the Working party of 30 May 2002 on the use of unique identifiers in telecommunication terminal equipments: the example of IPv6, WP 58, 10750/02/EN).

The extent to which right holders obtain access to detailed users information varies depending on countries. In Belgium, right holders have been requesting the collaboration of ISPs to send warnings to users. In the United-States, ISPs were requested to communicate the ID of their clients *directly* to the music industry representatives, without Court order[4]. This led to several court decisions (i.e., the Verizon case – December 2003), where finally such direct communication of information to right holders was considered illegal by the Court. As another example, the Australian legislation (through the "Anton Pilar order") permits the search of inquiries, including domiciliary visits, by private actors such as holders of IP rights.

In order to connect alleged infringements with users responsible and to complete the profile of the user, attempt is made by right holders to use existing public registers, such as "Whois" databases, which keep personal details about those who have registered a domain name. It contains in particular information as to the name of the contact-point for the domain name, including phone number, e-mail address and other personal data. Some information is accessed directly on-line, while other details are kept off-line and must thus be requested to the controller of the database.

Finally, the Working Party notes that, considering the fact that the collection of personal information by right holders is regulated by data protection principles, discussions are taking place in several countries with stake holders in order to give them more flexibility as to the processing of personal data. In this context, the French data protection legislation, for example, now includes an exemption aiming specifically at allowing the processing of judicial data by specific right holders defined by the law[5], in certain circumstances and subject to prior authorisation by the French DPA[6].

The Working Party deems it necessary, in this changing context, to recall the main data protection principles and the extent to which they apply in the framework of digital right management and enforcement of copyright.

II. The management of intellectual property rights

The legitimate purpose followed by right holders to prevent misuse of protected information often results in the tracing of users and the monitoring of their preferences. In particular, the use of unique identifiers linked with the personal information collected leads to the processing of detailed personal data. Directive 95/46 on the protection of personal data provides for several principles that shall be complied with by any right holder in such case where personal data are being processed. Article 2(3) (a) of Directive 2004/48/EC, on the enforcement of intellectual property rights confirmed the principle that the Directive 2004/48/EC does not affect Directive 95/46 and therefore the application of the data protection principles.

[4] Copyright holders based their request on Section 512 of the Digital Millennium Copyright Act, on Limitations on liability relating to material online. According to these provisions any copyright holder or his/her representative can ask a justice auxiliary of a federal court to deliver an injunction to an ISP to provide the identity of a user suspected of activities infringing copyright. This procedure is quite flexible as it allows obtaining personal data related to the user without starting a whole judicial process.

[5] The exemption applies to legal persons as exhaustively enumerated by articles L. 321-1 and L. 331-1 of the Intellectual Property Code, and having as object the defense of interests of right holders.

[6] The CNIL shall have to precise the quality of judicial information included in the files, as well as the duration of its storage. It will also have the duty to ensure that such processing is adequate with regard to what is strictly needed to fight counterfeiting (Decision of the "Conseil Constitutionnel" n°*2004-499 DC, 29 July 2004)*. It should be noted that, according to the Constitutional Court, identification by users through their IP address can only be allowed in the framework of a judicial procedure**.**

Focus will be put in this document on the necessity principle and the need for anonymous access to network services, on the transparency principle, the compatibility of purpose and the limitation regarding storage of data.

- Principles of necessity / anonymity

The Working Party reaffirms the necessity to allow for anonymous or pseudonymous transactions on the Internet. This principle was developed by the Working party on several occasions[7], since its Recommendation related to "Anonymity on the internet" adopted on 3 December 1997, where the WP already stated that the processing of personal data on the Internet has to respect data protection principles just as in the off-line world. "Users should have the option to access the Internet without having to reveal their identity where personal data are not needed to provide a certain service"[8]. This principle is justified by the necessity principle stated in article 6 c) of the data protection Directive, according to which personal data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.

In this perspective, the Working Party emphasises that, where DRM technologies are used in order to protect specific information, tools should be used that preserve the anonymity of the user. Greater attention should therefore be paid to privacy enhancing technologies while developing these new tools.

- Use of unique identifiers

The use of unique identifiers enables the interconnection of data related to a single individual, and facilitates their profiling. In the framework of digital rights management, they permit the profiling of the user based on the quality and quantity of documents he/she consults. For example, a company offering legal content online will be able to trace the circulation of such watermarked documents (which use unique identifiers) on peer-to-peer networks and identify the user at the origin of the legal downloading as well as further alleged unlawful uses of the document. Also in the workplace, the music or the film industry would have the capability to trace the use by their employees of protected information put at their disposal. 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. The tagging of a document should not be linked to an individual except if this link is necessary for the performance of the service or if the individual has been informed and has consented to it.

- Information of the data subject

As stated by the International Working Group on Telecommunications, it should be provided for the greatest possible transparency in the operation of the copyright management system. Pursuant to article 10 of Directive 95/46, no information can be collected regarding data subjects without them being informed about several elements, and in particular, the identity of the controller, the purpose(s) of the processing, the recipients or categories of recipients of the data and the existence of a right of access and rectification of the data.

---

[7] Recommendation 3/97 "Anonymity on the internet", adopted 3.12.1997;
Working document: Processing of Personal Data on the Internet, adopted by the Working Party on 23 February 1999, WP 16, 5013/99/EN/final.
Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware, adopted by the Working Party on 23 February 1999, 5093/98/EN/final, WP 17;

[8] International Working Group on Data Protection in Telecommunications, opt. cit., p. 2.

This information should be displayed in a visible manner before the user actually provides personal data or before he/she starts downloading tagged information[9].

- Compliance with the purpose limitation principle (compatibility)

Any personal data collected from the user on a voluntary basis or because they are necessary for the performance of the service should only be used in compliance with the stated purpose, as provided for by article 6 b) of the Directive. Indeed, it is not allowed, for example, to collect the name and address of the user at the occasion of a credit card payment, and to use them for marketing purposes, after having linked them with the preferences of the user collected through downloaded tagged information. Also pursuant to article 13 of the Directive on privacy and electronic communications, the user should be clearly informed and be given the choice to accept such profiling and marketing of his data. The same principle applies for any envisaged transfer of the users' data to third parties. Moreover, the Working party stresses that the collection of information related to consumption habits can lead to the processing of sensitive data, if data subjects are being profiled on the basis of the nature of the information consulted (e.g. the downloading of a book over religious or political issues…). Such processing could only take place in strict compliance with the provisions of article 8 of Directive 95/46.

- Limited storage of personal data

As stated in article 6 e) of Directive 95/46, personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Any personal data collected at the occasion of the provision of a protected product or service shall therefore be deleted as soon as it is no longer necessary for billing purpose or for any other purpose acknowledged by the user, such as maintaining a commercial relationship. It would not be compliant with this legal principle to keep all users data on a general basis just in the possible eventuality of alleged misuse of copyright information by a specific user.

III. The extent of investigation powers

In addition to the development of technical protection through tagging and tracing of copyright documents, for a few years copyright holders have been initiating actions intended to prosecute more specifically those suspected of copyright infringements. Such actions imply the collection of information about users suspected, by different means and using various information publicly or non-publicly available, as described in section I b.

While such processing of information is indisputably legitimate in the framework of one's own litigation, the methods of collection and the nature of the data collected are nevertheless regulated according to data protection principles, such as the following:

- Principle of compatibility

Right holders base their research primarily on the establishment of facts available on-line, such as the displaying of copyright protected documents in peer-to-peer networks. Data such as date and time of possible infringement, nature of the protected document, as well as indirect identifiers such

[9] See Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union, 5020/01/EN/Final, WP 43, adopted on May 17th.

as pseudonyms of the author of the possible infringement, are available. The temptation is then great to complete this collection of personal information with additional details that could be found with the help of Internet service providers or in other databases, such as the Whois data base, which compiles information about domain name holders.

The Working Party insists on the legal restrictions applying to the re-use of personal information. The content of databases, be they public or not, can only be processed and further used for a purpose compatible with the one for which they were first collected. As regards the Whois database, the Working party has already emphasised in its opinion of 13 June 2003[10] that "from the data protection viewpoint it is essential to determine in very clear terms what is the purpose of the Whois and which purpose(s) can be considered as legitimate and compatible to the original purpose. […] This is an extremely delicate matter as the purpose of the Whois directories can not be extended to other purposes just because they are considered desirable by some potential users of the directories. Some purposes that could raise data protection (compatibility) issues are for example the use of the data by private sector actors in the framework of self-police activities related to alleged breaches of their rights e.g. in the digital right management field."

On the basis of the compatibility principle as well as in compliance with the confidentiality principle included in Directives 2002/58 and 95/46, data detained by ISPs processed for specific purposes including mainly the performance of a telecommunication service cannot be transferred to third parties such as right holders, except, in defined circumstances provided by law, to public law enforcement authorities.

- Role of Internet Service providers

The Working Party recalls that no systematic obligation of surveillance and collaboration can be imposed on ISPs, pursuant to article 15 of Directive 2000/31 on electronic commerce.
ISPs can neither be obliged, except in specific cases where there is an injunction of enforcement authorities, to provide for a general "a priori" storage of all traffic data related to copyright. The Working Party has stated at several occasions[11] that "where traffic data are to be retained in specific cases, there must therefore be a demonstrable need, the period of retention must be as short as possible and the practice must be clearly regulated by law, in a way that provides sufficient safeguards against unlawful access and any other abuse."

- Processing of judicial data

As stated in article 8 of the Data protection Directive, processing of data related to offences, criminal convictions or security measures can be processed only under strict conditions as implemented by Member States. While any individual obviously has the right to process judicial data in the process of his/her own litigation, the principle does not go as far as permitting in depth investigation, collection and centralisation of personal data by third parties, including in particular, systematic research on a general scale such as the scanning of the Internet or the request of communication of personal data detained by other actors such as ISPs or controllers of Whois registries. Such investigation falls within the competence of judicial authorities.

In this regard, the Working Party notes that the recent Directive 2004/48 of 28 April 2004 on the enforcement of intellectual property rights provides for conditions in which personal data shall be

[10] Opinion 2/2003 on the application of data protection principles to the Whois directories, 10972/03/EN final, WP 76.
[11] See for example Opinion 5/2002 adopted on 11 October 2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-11 September 2002) on mandatory systematic retention of telecommunication traffic data, 11818/02/EN/Final, WP 64.

requested by judicial authorities. These authorities may order, on justified and proportionate request, communication of information on the origin and distribution networks of the goods or services which infringe an intellectual property right, when the infringement presents a commercial scale, and without prejudice of principles related to confidentiality of information sources or the processing of personal data. A fair balance shall have to be found between the legitimate interests of copyright holders and individuals concerned. The criteria of the commercial advantage linked with the infringement may be decisive in this respect.

4. Conclusion

The Working Party is concerned about the fact that the legitimate use of technologies to protect works could be detrimental to the protection of personal data of individuals. As for the application of data protection principles to the digital management of rights, it has observed, an increasing gap between the protection of individuals in the off-line and on-line worlds, especially considering the generalised tracing and profiling of individuals. The Working Party calls for a development of technical tools offering privacy compliant properties, and more generally for a transparent and limited use of unique identifiers, with a choice option for the user.

As far as the investigation powers is concerned, the Working Party deems it necessary to recall that investigations performed by private actors such as copyright holders must be performed in a clear legal framework along the lines developed above, especially as to the information that can legally be collected, and to the enforcement powers that can be attributed to these actors.