March 31, 2005

To:
The European Commission
Working Party on the Protection of Individuals
with Regard the Processing of Personal Data
e-mail: markt-privacy-consultations@cec.eu.int

Comments of the Electronic Privacy Information Center (EPIC) and the Information Society Project (ISP) at the Yale Law School on the Public Consultation of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data on Data Protection Issues related to Intellectual Property Rights

---

TABLE OF CONTENTS

I.
INTERESTS OF COMMENTATORS

The Electronic Privacy Information Center (EPIC) and the Information Society Project (ISP) at the Yale Law School submit these comments to the public consultation on Data Protection Issues related to Intellectual Property Rights with the purpose of applying the provisions of Directive 95/46/EC to Digital Rights Management (DRM) systems.

The Electronic Privacy Information Center (EPIC) is a non-partisan public interest research organization established in 1994 to focus public attention on emerging civil liberties issues. EPIC publishes *Privacy and Human Rights: An International Survey of Privacy Laws and Developments,* a comprehensive annual report that examines privacy developments around the world and emerging privacy issues. EPIC also maintains an extensive resource on DRM and privacy online at http://epic.org/privacy/drm/. The Information Society Project (ISP) at the Yale Law School was created in 1997 to study the implications of the Internet, telecommunications, and new information technologies on law and society.

Dr. Kristina Irion
Visiting Fellow

Electronic Privacy Information Center
1718 Connecticut Ave NW
Suite 200
Washington DC 20009
USA

+1 202 483 1140 [tel]
+1 202 483 1248 [fax]
http://www.epic.org
irion@epic.org

Chris Riley
Student Fellow

Eddan Katz
Executive Director

Yale Law School
Information Society Project (ISP)
P.O. Box 208215
New Haven, CT 06520-8215
USA

+1 (203) 432-4830 [tel]
+1 (203) 436-0851 [fax]
http://islandia.law.yale.edu/isp/index.html

Commentators[*]

[*] The commentators would like to thank Marc Rotenberg , President of EPIC, Chris J. Hoofnagle , Director of EPIC West, and Cedric Laurant, EPIC Policy Council, for their valuable comments and contributions.

II.
INTRODUCTION

The basic right to privacy is an element of Europe's constitutional legacy.[1] The European Union is committed to the protection of personal data in Art. 8 of the Charter of Fundamental Rights of the European Union, according to which it is imperative that personal data be processed fairly for specified purposes and with the consent of the person concerned or on some other legitimate basis laid down by law.[2] The same basic principles are included in EC harmonization legislation that Member States have transposed in their national data protection laws. The regulations on the processing of individual data provide a neutral framework that is increasingly challenged by the "technologisation of copyright"[3] embodied in Digital Rights Management (DRM) systems.

In the past, readers of books and magazines, viewers of broadcast television, and listeners of radio programming or music were able to receive content without the risk that their personal information could be obtained by others.[4] Copyright holders were compensated for their works and the right of privacy was respected. With the advent of DRM systems users are taken from a culture where there is freedom to enjoy media anonymously to one where access will be conditioned upon revealing one's identity.[5] And once the individual has given up their freedom to be anonymous, media companies will claim that they have the freedom to exploit information about the individual's media consumption by selling it to others - perhaps even the government.

Copyright comprises the sum of privileges that are granted by international agreements and national statutory laws to the creator of literary or artistic works. Directive 2001/29/EC on the harmonization of certain aspects of copyright and related rights in the information society provides for reproduction, communications and distribution rights for the copyright owner.[6] The Directive also introduces provisions protecting technological measures against circumvention and protecting rights management information against alteration.[7] Thus, extending legal protection to tools for assisting copyright enforcement has been deemed necessary to respond to the "digital challenge" in order to legally back

---

[1] Compare Art. 8 of the European Convention of Human Rights and Fundamental Freedoms of 1950, *available at* <http://www.echr.coe.int/Convention/webConvenENG.pdf>, and national constitutions of EU Member States.

[2] *Available at* <http://www.europarl.eu.int/charter/pdf/text_en.pdf>.

[3] Bygrave, Lee A., "The Technologisation of Copyright: Implications for Privacy and Related Interests", *24 European Intellectual Property Review 51*, 2002, pp. 51-57.

[4] See International Working Group on Data Protection in Telecommunications, Common Position on Privacy and Copyright Management, adopted on 4-5 May 2000 in Rethymnon/ Crete, *available at* <http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_en.htm>.

[5] *See* Julie Cohen, "A Right to Read Anonymously: A Closer Look at "Copyright Management in Cyberspace", 28 Conn. L. Rev. 981 (1996).

[6] Arts. 2-4 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspect of copyright and related right in the information society, OJ L 167/10.

[7] Arts. 6-7, *id*.

up copyright holders' efforts to prevent piracy, plagiarism, and unauthorized exploitation of their works.

DRM systems are the copyright holders' attempt to translate the terms and conditions of the licensed use of digital content into a technological structure of restrictions and permissions that cannot be altered.[8] Copyright-protected works are fortified with DRM systems that are designed to support the following functionalities: access control, restriction of unauthorized reproduction, authentication of the work and the right holders, and protection of the authenticity of this data.[9] These technologies may be contained within the operating system, program software, in the actual hardware of a device, or a combination of all three. Together with the terms and conditions of the license to use the copyright-protected work, DRM systems are most often imposed unilaterally and implemented *ex ante* by the copyright holder.[10] Control over the terms of access to and use of digital works and the technological means to enforce this control have resulted in ever increasing collection and processing of personal data of users. Moreover, DRM techniques create methods of control for the copyright holder that may exceed the legal rights. In effect, where the law grants a limited right, the DRM may create an absolute rights.

The development of DRM systems must be examined carefully, in particular because concern for the individual's right to privacy is relegated behind the interests of copyright owners. In an attempt to secure content, many DRM systems require the user to identify and authenticate a right of access to the protected media. Not only the amassing of personal data is routine DRM operation before any activity endangers the copyright. Moreover, during the entire life cycle of the copyright-protected work, the use of the work in compliance with the license can be monitored, which implies the possibility of monitoring the behavior and habits of individual users for decades.[11] Eventually, this creates a strong incentive for the data controller to engage in profiling using the personal data obtained. The controller can examine individual consumption, combine personal accounts with other information, target users with direct marketing, and even resell user profiles to third parties. In a different context, applications with similar features would be referred to as spyware for their severe invasions into individual privacy, and would be treated with cautious suspicion or outright prohibition.

In the following sections, we argue that DRM systems that refrain from the processing of personal information are preferable from the consumer's perspective and also help ensure legal predictability; in the next section, we discuss the extent to which currently operating DRM systems interfere with individuals privacy; and in the third section we apply EC

[8] Also referred to as Rights Expression Language (REL).

[9] Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management - Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 418–446, p. 420.

[10] Bygrave (2002), *supra* n. 3, p. 54.

[11] Compare recital (57) of the Copyright Directive 2001/29/EC, which recognizes that DRM depending of their design "process personal data about the consumption patterns […] by individuals and allow for tracing of online-behavior".

data protection regulation specifically for DRM systems, demonstrating the effect of legal restrictions on implementation and call for strict enforcement of data protection laws.

III.
ARGUMENT

1. DRM Abstinence from Data Processing

Art. 9 of the Copyright Directive states explicitly that its provisions apply without prejudice to legal provisions in *inter alia* data protection and privacy.[12] Only DRM systems that do not perform any processing of users' individual data fall outside the scope of the relevant EC Data Protection Directive 95/46/EC.[13] DRMs are not captured by the privacy regulatory regime if they do not collect personal information but merely rely on "the use of effective technological measures" designed to prevent or restrict access and unauthorized reproduction through methods "such as encryption, scrambling or other transformation of the work […] or copy control *mechanism*".[14] Along with such a restriction come a number of advantages for the distribution of copyright-protected works, elaborated below.

First, there is a strong preference in the EC privacy regime and on the part of consumers for transactional anonymity, an option which prevails outside electronic commerce. This can be deduced from recital (26) of Directive 95/46/EC which exempts "data rendered anonymous in such a way that the data subject is no longer identifiable" from the principles of data protection. Self-restriction is demanded by the principle of minimality derived from Art. 6 (1) (c) and (e) of Directive 95/46/EC, which should be read in conjunction with the burden of proof, that "it shall be for the [data] controller to ensure that paragraph 1 is complied with." There is ample documentation of consumers' preference for remaining anonymous in online transactions that forms part of the demand side parameters.[15] DRMs that monitor individual use and consumption undermine consumers' expectations of privacy.[16]

---

[12] Directive 2001/29/EC, *supra* n. 6.

[13] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

[14] Art. 6 (3) of Directive 2001/29/EC, *supra* n. 6.

[15] Bygrave (2003), *supra* n. 9, p. 424; Mulligan, Deirdre K ./ Burstein, Aaron: "Implementing Copyright Limitations in Rights Expression Languages", paper presented at 2002 ACM Workshop on Digital Rights Management, p. 2.

[16] Rotenberg, Marc: "Testimony on the WIPO Copyright Treaties Implementation Act and Privacy Issues" before the Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives, June 5, 1998, *available at* <http://www.epic.org/privacy/copyright/epic-wipo-testimony-698.html>.

Second, the set-up, maintenance, and communication of a distribution scheme for copyright-protected works are greatly simplified if the DRM system does not process personal data. The initial collection of personal data requires adherence to elaborate information duties towards the data subject and a readiness to specify the legitimate purpose and substantiate on the compliance with the principles relating to data quality.[17] The handler of personal data is also required to implement appropriate technical and organizational measures to guarantee confidentiality, security, and integrity of the personal data held.[18] Moreover, by opting for DRM that does not rely on the processing of personal data, controllers minimize the significant risks of non-compliance with the regulatory regime on data protection. The data controller is liable for remedies and damages, and can be sanctioned to refrain from a certain practice that are in conflict with data protection law.[19] Data Protection Authorities (DPAs) are equipped with effective powers of investigation and intervention which enable them to enforce these regulations.[20] The copyright holder who has a vital interest in the sustainability of its distribution scheme and DRM might consider it worthwhile to resist processing of personal data *a priori*.

A third caveat against the mandatory processing of personal data for rights management before any copyright infringement has occurred is disproportionality against privacy. The principle of proportionality is spelled out in Art. 7 (f) of Directive 95/46/EC as one reason that legitimizes data processing, and is a principle relating to data quality in Art. 6 (c) of Directive 95/46/EC. In copyright protection, the circumvention of DRM systems that qualify as effective technical measure is actionable,[21] the authenticity of rights-management information does enjoy legal protection,[22] and Directive 2004/48/EC on the enforcement of intellectual property rights is due for transposition in the Member States on April 29, 2006.[23] At the intersection of copyright and privacy a fair balancing of interests is indispensable in order to fine-tune a technological progress with the inherent tendency to perform surveillance. Even the Copyright Directive advises controllers to "incorporate privacy safeguards" in accordance with the Data Protection Directive.[24] Borrowing from competition law analysis, a comparison of DRM solutions looking at their privacy invasiveness may prove to be a useful test for proportionality. It will help to introduce some intra-modal competition for privacy that cannot be left at discretion of each copyright owner.

Finally, under EC data protection regulation, DRM systems are required to refrain from recording and reporting ongoing access and use of licensed e-content that does not amount to a breach of copyright if the data subject has not unanimously consented to it.[25]

---

[17] See Arts. 10, 6 and 7 of Directive 95/46/EC, *supra* n. 13.
[18] See Arts. 16-17 of Directive 95/46/EC, *id*.
[19] See Arts. 22-23 of Directive 95/46/EC, *id*
[20] See Art. 28 of Directive 95/46/EC, *id*.
[21] Art. 6 (1) of Directive 95/46/EC, *supra* n. 6; note the request for proportionality in recital (48), *Id*.
[22] Art. 7 (1) of Directive 95/46/EC, *id*.
[23] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Corrigendum, OJ L 195/16.
[24] See recital (57) of Directive 2001/29/EC, *supra* n. 6, for rights-management information systems.
[25] That is expression of self-determination, see Art. 7 (a) of Directive 95/46/EC, *supra* n. 13

The same applies to the processing of personal information for profiling, direct marketing, and (commercial) transfer to third parties that are beyond the primary purpose of copyright protection. Privacy protection is even stricter where the use of e-content would reveal the special categories of data enumerated in Art. 8 (1) of Directive 95/46/EC.[26] There is a strong case that the consumption of intellectual goods may sometimes reveal sensitive data about a person's individual dispositions and preferences.[27] This general prohibition on the processing of special categories of data can only be overridden by the exemptions of Art. 8 (2) of Directive 95/46/EC, again with the explicit consent of the data subject.[28] Before collecting the data subject's consent there must be detailed information about the intended data processing. This will be explored in further detail in the third argument below.

2. Privacy Invasiveness of Current DRM Systems

Current generation DRM systems are capable of greatly infringing on users' legal rights to privacy, far beyond the level and nature of infringement necessary to protect the legal rights of content producers. DRM systems "engage in detailed surveillance of content consumption by consumers within private spaces," including "the content used, the time of use, the frequency of use, and the location of use."[29] Furthermore, information is also collected by "multiple third parties" whose identities are "not well disclosed".[30] Beyond what is necessary for the enforcement of intellectual property rights, personal information is being collected and used for targeted marketing and other purposes.

It is difficult in general to determine what information is actually collected by DRM systems. Furthermore, this information is subject to change in later versions of the software. Therefore we will examine more generally the architectures of DRM systems, and consider the privacy risks which are possible. We offer two principles to characterize the possible privacy risks presented by the systems: *individual identification*, the association of content or activity with personally identifiable information such as a name or address, and *unnecessary collection* of information, the collection of information concerning the use of copyrighted content which is not necessary for the enforcement of

[26] Such sensitive personal data includes racial or ethnic origin, political opinions, religious and philosophical beliefs, trade-union membership, health and sex life, see Art. 8 (1) of Directive 95/46/EC, *id.*

[27] Compare Article 29 Data Protection Working Party, Working Document on data protection issues related to intellectual property rights, January 18, 2005, WP 104, p. 6; Bygrave (2002), *supra* n. 10, *at* Privacy Implication; Bygrave (2003), *supra* n. 9, p. 434; Cohen, Julie E., "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", 28 Conn. Law Review 981, pp. 1006-14, and "DRM and Privacy", *18 Berkeley Technology Law Journal,* 2003, pp. 575-617, pp. 576-579.

[28] Insofar as Member States have transposed into their national laws the exception for consent to the processing of personal data, Art. 8 (2) (a) of Directive 95/46/EC, *supra* n. 13.

[29] Mulligan, Deirdre K ./ Han, John/ Burstein, Aaron: "How DRM-Based Content Delivery Systems Disrupt Expectations of 'Personal Use'"; paper presented at 2003 ACM Workshop on Digital Rights Management, see also Cohen (2003), *supra* n. 27, p. 577f.

[30] Mulligan/ Han/ Burstein (2003), *id.*

copyright restrictions on the content. [31] Such unnecessary information is usually reported back to a server operated by the copyright owner and used for marketing purposes.

Let us examine some modern DRM systems with a focus on privacy risks inherent to the systems. Consider the VCast network, a service for digital media broadcasting to multiple devices.[32] The VCast business model depends on its ability to control retransmission of its broadcasts. The VCast network website describes its DRM using the following statement: "The content owners can distribute their digital media or even let users to download or copy without worries as it will prompt the users to acquire the license from internet when they try to open the media from any source."[33] In other words, the VCast DRM requires *online authentication* before a local copy of content can be used. Because online authentication is likely to include the content being accessed, the time and date of access, and account information of the party seeking to use the content, information is being provided to the copyright owner or an intermediary, which may far exceed the limits of information necessary to enforce copyright. Furthermore, the account information is likely capable of being associated with a name and address, which allows the collected information to be associated with an identified individual.

Regulation in a system requiring online authentication for use should seek to protect the user from these privacy risks. It should ensure that any information collected for copyright protection purposes is not linked with personally identifiable information which may be needed for billing purposes, and that no information is requested as part of the online authentication process if it is not strictly necessary to determine whether or not the desired access is permitted by the copyright restrictions on the content.

Next, consider the online music service Napster-to-Go.[34] Napster-to-Go is based on a subscription model in which users pay a flat monthly fee to gain unlimited access to a library of music files, which can be downloaded and played on a computer or transferred to a supported device. Other music stores, such as Apple's iTunes,[35] do not use a subscription model, but sell tracks individually (and collected in albums) to users. All of these services require that the music be played only through approved players, which makes it possible for the service provider to design the music player to keep a record of consumer activity, such as frequency and common orderings of song usage, information which can be valuable for marketing purposes. This record may then be reported back to a service provider.

Similar behavior is possible as well in eBooks[36] and other forms of digital content. In the case of Microsoft's eBook Reader, this means that the media software and users' choices

---

[31] These principles are discussed by Mulligan and Burstein in the context of DRM as part of paper entitled "Implementing Copyright Limitations in Rights Expression Languages". The paper focuses primarily on RELs in general, but section 4.1 focuses on issues of privacy.

[32] See <http://www.vcast.net>.

[33] See <http://www.vcast.net/eng/network.htm>.

[34] See <http://www.napster.com/ntg.html>.

[35] See <http://www.apple.com/itunes/>.

[36] An eBook is a digital encoding of a book. Two popular eBook formats are produced by Adobe and Microsoft. See <http://www.adobe.com/epaper/ebooks/> and <http://www.microsoft.com/reader/>.

in electronic books are digitally linked not only to the user's computer, but also to the company's identity management system, Microsoft Passport.[37] This arrangement allows tracking of both the individual and the individuals' computer. Some systems, such as Microsoft's Windows Media Player, assign a Globally Unique Identifier (GUID) to the media device that facilitates tracking.[38] These systems create records that enable profiling and target marketing of individuals' tastes by the private sector.

These are clear examples of unnecessary collection of information. Additionally, most of these services require the creation and use of a personalized account for transactions, which likely involves the collection of personally identifiable information for billing purposes. This makes it possible to associate personally identifiable information with a record of activity. Though it is possible to perform individual electronic commerce transactions with some degree of anonymity,[39] which would prevent both unnecessary collection and individual identification, these services do not permit such an option, and do not adequately inform the casual user that such an option exists.

Regulations for DRM should include preventing programs used for digital content consumption from collecting and reporting back information concerning use of the content which is not strictly necessary to enforce copyrights on the content. Furthermore, regulation in systems that require personalized accounts should force the systems to establish a barrier between account information used for billing purposes and any records of account activity in order to prevent individual identification.

3. Enforcement of the Data Protection Directive

Whenever DRM includes the processing of personal data, the national transpositions of the relevant Directive 95/46/EC apply. Within this category, DRM technology is either designed to invariably link an individual to the reference material (*e.g.*, watermarks)[40] or collects information that can "reasonably"[41] be expected to identify an individual. The latter is particularly relevant in the context of DRM systems that install cookies, collect (mobile) phone numbers, e-mail addresses and (permanent) IP addresses, or incorporate device authentication that can be linked back to a specific individual. The application of

---

[37] This service is now called ".Net Passport." Russel Kay, *Copy Protection: Just Say No* , Computerworld, (Sept. 4, 2000); Megan E. Gray & Will Thomas DeVries, *The Legal Fallout From Digital Rights Management Technology*, 20 Comp. & Internet Lawyer 20 (April 2003).

[38] Richard Smith, *Serious Privacy Problems in Windows Media Player for Windows XP* , Computerbytesman, Feb. 20, 2002, *available at* <http://www.computerbytesman.com/privacy/wmp8dvd.htm>.

[39] Services such as Paypal (see <http://www.paypal.com/>) allow money to be exchanged between a buyer and a seller of a good without any semblance of a trust relationship; they could likely be used in this context to support anonymous e-commerce for music files or electronic books.

[40] Or personalized hardware key "dongles". Compare Article 29 Data Protection Working Party, Working Document on data protection issues related to intellectual property rights, January 18, 2005, WP 104, p. 5.

[41] Compare recital (26) of Directive 95/46/EC, *supra* n. 13.

privacy regulations to these information is backed by Recital (24) of Directive 2002/58/EC, according to which "terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms."[42]

Information processing for transaction management and copyright enforcement are distinct purposes for which the processing of personal data is deemed necessary for the performance of a contract to which the data subject is party (Art. 7 (b) of Directive 95/46/EC). These purposes must not be confused, and scrutiny for compliance with the principles relating to data quality has to be undertaken on a separate basis. In connection with the limitation principle endorsed in Art. 6 (1) (e) of Directive 95/46/EC any further processing of personal data collected for processing the transaction, such as payment details and the destination for (electronic) delivery, cannot be considered necessary after the transaction has concluded. Copyright enforcement itself has to justify the items of personal data that are processed within the architecture of a given DRM system. Injecting all available transactional data into the DRM is destined to be inadequate, irrelevant and excessive in relation to the purpose for which personal data is further processed. Within the purpose limitation principle, any retention of data which permits identification longer than necessary violates Art. 6 (1) (e) of Directive 95/46/EC. It is upon the data controller to ensure conformity with the principles relating to data quality laid down in Art. 6 (1) of Directive 95/46/EC.[43] Besides, harvesting personal information from third sources destined for different purposes is unsolicited processing of personal data that runs contrary to data protection regulation in place.[44]

Provided that the design of DRM will have to reconcile the interest in copyright control with data protection regulation in place the enforcement of specific license terms with DRM might turn out to be disproportionately privacy invasive. For instance the duration of monitoring individual's use of e-content can amount to decades without any sound concern that a breach copyright will occur. Under the law of contract, it is feasible to derogate from the provisions in copyright legislation that allow for exemptions and limitations for due process and lawful use. The more narrow the license terms are stricken the more rigid the complementary DRM system has to construed in order to monitor compliance of the users at the expense of users' privacy.[45] The monolithic imposition of terms and conditions in a license agreement is also captured by the regulation on unfair terms in consumer contracts.[46] Data controllers are best advised to give consumer information in plain and understandable language on the data processing of their DRM that is distinct from the remaining license terms and conditions.

---

[42] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37.

[43] Art. 6 (2) of Directive 95/46/EC, *supra* n. 13.

[44] Compare Article 29 Data Protection Working Party, Opinion 2/2003 on the application of data protection principles to Whois-Directories.

[45] Bygrave (2002), *supra* n. 10, *at* Copyright and Privacy in the Good Old Days.

[46] Directive 93/13/EEC of the Council of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29.

Any further processing of personal data with the means of DRM systems for purposes that exceed the protection of copyright requires the unambiguous consent of the data subject (Art. 7 (a) of Directive 95/46/EC). In Art. 2 (h) of this Directive "the data subject's consent" is defined as "any freely given specific and *informed* indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed". A number of existing practices fail to require an adequate informed consent and do not satisfy the information duties imposed on the data controller in Art. 10 of Directive 95/46/EC. It is established practice that the licensing of copyright-protected works takes the form of a contractual agreement based on pre-formulated terms and conditions written by the copyright owner.[47] The inclusion of information concerning the intended processing of personal data for secondary purposes into such a license agreement, acceptance of which is considered consent, does not amount to an informed consent as it is demanded in Directive 95/46/EC.[48]

Moreover, the consumer should be given a choice on whether personal data is processed for secondary purposes without having to forego the use of copyright-protected work. A recent US lawsuit illustrates how DRM implementations can be privacy invasive. In February 2002, Sunncomm, Inc., a DRM systems developer, and Music City Records settled a lawsuit by a California woman who objected to their practice of tracking and disclosing personal information - including music consumption patterns - to third-parties with no opt-out scheme. In the case, the plaintiff's attorney argued that SunnComm: "never disclose[d] on the shrink-wrap of the CD(s) that consumers cannot listen to music on their computers anonymously. If left unchecked, this will be the start of an era where consumers will be coerced to give up their privacy to listen to music on their computers."[49] The settlement agreement required the companies to provide notice to consumers of their information collection practices and to refrain from requiring consumers to disclose their personal information as a condition of downloading, playing, or listening to a CD.[50]

The Article 29 Working Party recognized that standards are shaping DRM technological development on a massive scale, and that privacy considerations have to be included at the stage of development of DRM standards and systems.[51] Copyright Directive 2001/29/EC, in recital (57), encourages copyright holders that any rights-management

---

[47] Compare Bygrave (2002), *supra* n. 10, *at* Other Problematic Consequences.

[48] Or deemed unfair and one-sided, compare decision of Federal Supreme Court (Germany) of March 16, 1999, reference XI ZR 76/9, *available at* <http://www.datenschutz-berlin.de/recht/de/rs/bgh/telewerb.htm>; *UFC Que Choisir v. AOL France*, decision of Court of First Instance of Nanterre, June 2, 2004 (appealed), *available at* <http://www.foruminternet.org/telechargement/documents/tgi-nan20040602.pdf> (in French).

[49] *DeLise v. Fahrenheit* , No. CV-014297 (Cal. Sup. Ct. Sept. 6, 2001)(Pl. Comp. at ¶ 1), *available at* <http://www.techfirm.com/mccomp.pdf>.

[50] Press Release, SunnComm, Inc., *Sunncomm and Music City Records Agree to Resolve Consumer Music Cloqueing Law Suit by Providing Better Notice and Enhancing Consumer Privacy* (Feb. 22, 2002), *available at* <http://www.xenoclast.org/free-sklyarov-uk/2002-February/001580.html>.

[51] Compare Article 29 Data Protection Working Party, Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group), January 23, 2004, WP 86.

system "should" incorporate privacy safeguards in accordance with the Data Protection Directive. There are a number of proposals that promote the use of DRM technology to engineer privacy enhancing technologies (PET).[52] It is important that EC Data Protection Authorities (DPA) are provided with information on the data collection and the efforts on developing privacy enhancing technologies that allow them to follow up these developments closely. For example the ambivalence of trusted computing platforms to privacy could be dealt with during development.[53] Trusted computing enables many new security enhancements that may greatly enhance users' privacy. At the same time, these features also enable applications that may enforce policies detrimental to individual privacy and anonymity.

Trusted computing can lessen an individual's ability to act or communicate anonymously whenever applications log their usage on particular computer systems and tie their data to these systems. Functionality provided by trusted computing may also encourage requiring strong identification of individuals, even where such identification is unnecessary or where authentication would suffice. Robust DRM has been cited as one primary application of trusted computing, and such DRM would likely associate individual usage licenses with strong identifiers. Media consumption could be authorized, even tracked, in ways that generate data associated with individuals. While strong identification is desirable in some contexts, such as providing adequate financial or medical privacy, the ease of demanding such identification may prove too great a temptation for other, less sensitive applications.

IV.
CONCLUSION

Digital Rights Management systems are being developed to further the control of copyright owners over their works without adequate regard for the privacy interests of the user of the work. Consumers concerned about the overzealous collection of their personal data and the monitoring of their consumption patterns or online-behavior have in most instances not even a chance to access copyright-protected work and have their privacy respected. Unless companies are required to respect the legal responsibilities for the personal data they collect through DRM, there is no economic incentive to create anonymous or privacy-friendly implementations of DRM. Albeit any copyright control via DRM technology is required to adhere to the EC privacy regime, concern for the privacy of personal information is fully absent from the design process.[54] This omission is unnecessary, as there are a number of advantages in favor of DRM systems, which do not

[52] Korba, Larry/ Kenny, Steve, "Towards Meeting the Privacy Challenge: Adopting DRM", 2002 ACM Workshop on Digital Right Management; Cameron, Alex, "Infusing Privacy Norms in DRM: Incentives and Perspectives from Law", in Deswarte *et al* (Eds.), Information Security Management, Education and Privacy, pp. 8f.

[53] Compare Article 29 Data Protection Working Party, Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group), January 23, 2004, WP 86.

[54] High Level Group on Digital Rights Management, Final Report, p. 5.

process personal data. In a maturing market, privacy respecting DRM systems are able to become distinguished and competitive options for the distribution and enforcement of copyright-protected work.

It is our belief that current technology carries with it by design severe risks to privacy in the form of unnecessary information collection, retention of information beyond the purpose of collection, and association of collected information with individual identifiers. In order to leverage a shift to privacy-supporting design, existing DRM technology must be scrutinized according to national data protection regulation by data protection authorities (DPA) within their *ex officio* powers. Together with necessary guidance on the intended application of data protection laws only hands-on regulatory enforcement will reverse the tendency that DRM routinely process personal data. The initiative of the Article 29 Data Protection Working Party should make clear to copyright holders and developers of DRM that the fusion of DRM and Privacy Enhancing Technologies (PET) is for the mutual benefit of privacy and copyright protection.

V.
AUTHORITIES

Legislation

Directive 93/13/EEC
of the Council of 5 April 1993 on unfair terms in consumer contracts, OJ L 95/29.

Directive 95/46/EC
of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281/31.

Directive 2001/29/EC
of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspect of copyright and related right in the information society, OJ L 167/10.

Directive 2002/58/EC
of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, OJ L 201/37.

Directive 2004/48/EC
of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights, Corrigendum, OJ L 195/16.

Official Documents

Article 29 Data Protection Working Party, Opinion 2/2003 on the application of data protection principles to Whois-Directories, WP 76, *available at* <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp76_en>.

Article 29 Data Protection Working Party, Working Document on Trusted Computing Platforms and in particular on the work done by the Trusted Computing Group (TCG group), January 23, 2004, WP 86, *available at* <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2004/wp86_en.pdf>.

Article 29 Data Protection Working Party, Working Document on data protection issues related to intellectual property rights, January 18, 2005, WP 104, *available at* <http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp104_en.pdf>.

High Level Group on Digital Rights Management, Final Report, *available at* <http://europa.eu.int/information_society/eeurope/2005/all_about/digital_rights_man/doc/040709_hlg_drm_final_report.doc>.

International Working Group on Data Protection in Telecommunications, Common Position on Privacy and Copyright Management, adopted on 4-5 May 2000 in Rethymnon/ Crete, *available at* <http://www.datenschutz-berlin.de/doc/int/iwgdpt/co_en.htm>.

Bibliography

Bechthold (2003)

Bechthold, Stephan, "The Present and Future of Digital Rights Management", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management – Technological, Economic, Legal and Political Aspects, Springer, Berlin 2003, pp. 597-654, *available at* < http://www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf >.

Bygrave (2002)

Bygrave, Lee A., "The Technologisation of Copyright: Implications for Privacy and Related Interests", *24 European Intellectual Property Review 51*, 2002, pp. 51–57, *available at* <http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf>.

Bygrave (2003)

Bygrave, Lee A.: "Digital Rights Management and Privacy - Legal Aspects in the European Union", in: Becker/ Buhse/ Günnewig/ Rump (eds.), Digital Rights Management – Technological, Economic, Legal and Political Aspects, Springer,

Berlin 2003, pp. 418–446, available at <http://folk.uio.no/lee/publications/DRM_privacy.pdf>.

Cameron (2004)

Cameron, Alex, "Infusing Privacy Norms in DRM: Incentives and Perspectives from Law", in Deswarte *et al* (Eds.), Information Security Management, Education and Privacy, IFIP 18th World Computer Congress, TC11 19th International Information Security Workshops, 22-27 August 2004, Toulouse, France (Kluwer 2004), *available at* <http://www.fasken.com/WEB/fmdwebsite.nsf/.pgRedirNewWin?OpenPage&url=www.fasken.com/WEB/fmdwebsite.nsf/AllDoc/5234D874DDEF7FE888256ECC00523EE4/$File/ADC_INFUSING_PRIVACY_NORMS_IN_DRM.PDF&ht=600&wt=600&opts=YES>.

Chaum (1992)

Chaum, David, "Achieving Electronic Privacy," Scientific American (August 1992).

Cohen (1996)

Cohen, Julie E., "A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace", 28 Conn. Law Review 981, pp. 1006-14.

Cohen (2003)

Cohen, Julie E., "DRM and Privacy", *18 Berkeley Technology Law Journal,* 2003, pp. 575-617, *available at* <http://www.law.georgetown.edu/faculty/jec/drmandprivacy.pdf>.

Einhorn/ Rosenblatt (2005)

Einhorn, Michael A./ Rosenblatt, Bill, "Peer-to-Peer Networking and Digital Rights Management: How Market Tools Can Solve Copyright Problems", February 17, 2005, Policy Analysis, Series No. 534, CATO Institute, *available at* <http://www.cato.org/pub_display.php?pub_id=3670>.

Korba/ Kenny (2002)

Korba, Larry/ Kenny, Steve, "Towards Meeting the Privacy Challenge: Adopting DRM", 2002 ACM Workshop on Digital Right Management, *available at* <http://crypto.stanford.edu/DRM2002/KorbaKennyDRM20021.pdf>.

Mulligan/ Burstein (2002):

Mulligan, Deirdre K./ Burstein, Aaron: "Implementing Copyright Limitations in Rights Expression Languages"; paper presented at 2002 ACM Workshop on Digital Rights Management, *available at* <http://crypto.stanford.edu/DRM2002/mulligan_burstein_acm_drm_2002.doc>.

Mulligan/ Burstein/ Han (2003):

Mulligan, Deirdre K./ Han, John/ Burstein, Aaron: “How DRM-Based Content Delivery Systems Disrupt Expectations of ‘Personal Use’”; paper presented at 2003 ACM Workshop on Digital Rights Management, *available at* <http://www.sims.berkeley.edu/~john_han/docs/p029-mulligan.pdf>.

Rotenberg (1998)

Rotenberg, Marc: “Testimony on the WIPO Copyright Treaties Implementation Act and Privacy Issues” before the Subcommittee on Telecommunications, Trade, and Consumer Protection, Committee on Commerce, U.S. House of Representatives, June 5, 1998, *available at* <http://www.epic.org/privacy/copyright/epic-wipo-testimony-698.html>.

Sobel (2003)

Sobel, Lionel S., "DRM as an Enabler of Business Models: ISPs as Digital Retailers", *18 Berkeley Technology Law Journal*, p. 667-695, available at <https://www.law.berkeley.edu/institutes/bclt/drm/papers/sobel-drm-btlj2003.pdf>.
