

# The Technologisation of Copyright: Implications for Privacy and Related Interests

[Published in *European Intellectual Property Review*, 2002, vol. 24, no. 2, pp. 51–57]

*Lee A. Bygrave*

## Introduction

A profound change is occurring in the way that intellectual property is protected. The change may be summed up as the technologisation of copyright. This somewhat inelegant phrase denotes the increasing use of technological mechanisms – including information systems architectures – to ensure that copyright is respected, particularly in the online environment. The basic purpose of this opinion is to discuss the possible impact of this development on the privacy and related interests of users of information products. Only the basic contours of the issue are sketched here but it is hoped, nevertheless, to show that the issue warrants detailed discussion. For the issue is fundamental to determining the quality of life in the digital age.

The opinion begins with an outline of the traditional interrelationship of copyright and privacy law. It then provides a brief description of the catalysts for the technologisation of copyright. Thereafter, an examination is made of how this technologisation might affect the privacy and related interests of information consumers. As part of the analysis, account is taken of certain legal instruments pertaining directly to the issue. The focus here is on the European Community (E.C.) Directive on copyright of 2001,<sup>1</sup> the United States (U.S.) Digital Millennium Copyright Act of 1998,<sup>2</sup> and the E.C. Directive on data protection of 1995.<sup>3</sup>

## Copyright and privacy in the “good old days”

Copyright and privacy rights – broadly conceived – share a great deal in terms of their respective origins. Both have emerged to a considerable extent from doctrines on personality rights. This process has involved some cross-fertilisation of the two sets of interests: notions of copyright have helped to ground privacy rights, and notions of privacy have helped to ground copyright.<sup>4</sup> This mutual aid has existed not just at the level of legal theory but also in practice. For instance, copyright law has furthered privacy interests by restricting publication of certain film material in which persons are portrayed,<sup>5</sup> and by restricting the ability of third parties to duplicate and further

---

<sup>1</sup> Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (O.J. L 167, 22.6.2001, 10 *et seq.*).

<sup>2</sup> Public Law No. 105-304 (1998), codified at 17 U.S.C. §§ 1201–1205 (1999).

<sup>3</sup> 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 (O.J. L 281, 23.11.1995, 31 *et seq.*).

<sup>4</sup> See, e.g., S. Warren and L. Brandeis, “The Right to Privacy” (1890) 4 *Harvard Law Review* 193 *et seq.*, especially 198 (arguing, *inter alia*, that common law protection of intellectual, artistic and literary property is based upon a broader principle of protection of privacy and personality).

<sup>5</sup> See, e.g., U.K. Copyright, Designs and Patents Act 1988 (as amended), s. 85(1); Australia’s federal Copyright Act 1968 (as amended), s. 35(5); Norway’s Intellectual Property Act 1961 (*lov om opphavsrett til åndsverk m.v. 12. mai 1961 nr. 2*; as

exploit lists of personal data compiled in certain registers.<sup>6</sup> Further, the exemptions to copyright in relation to the “private” or “fair” use of copyrighted material help to prevent copyright impinging unduly upon the private sphere of information consumers.<sup>7</sup> At the same time, privacy rights in the form of data protection law help copyright by placing limits on the processing of personal information that might subsequently be exploited in breach of copyright. Moreover, the respective agenda of copyright and privacy protection are similar, at least in their basic mechanics. Both attempt essentially to control the flow of information so as to safeguard certain values and interests.

Nevertheless, we should not overplay the similarities between their respective agenda. Nor should we overplay the extent to which the copyright community has taken privacy concerns actively into consideration and *vice-versa*. Any such consideration has been incidental and *ad hoc*. It is also apparent, for example, that the “private use” and “fair use” exemptions in copyright law are grounded not so much upon privacy considerations but on the interest of the wider community in gaining access to the fruits of creative endeavour.<sup>8</sup> Further, the privacy of consumers of copyrighted material has clearly been due to a range of factors that have little to do with copyright law.<sup>9</sup> Probably the most important of these factors has been that sales of copyrighted material have usually been able to be carried out as anonymous cash transactions and, concomitantly, that the material itself has lacked mechanisms to monitor and report on its usage.

Equally clear is that the concerns of copyright differ in fundamental respects from the concerns of privacy and data protection. Put somewhat simplistically, the steering axiom for data protection advocates is “knowledge is power”. For copyright-holders, a steering axiom of greater importance is “knowledge is wealth”. More particularly, copyright is an attempt to protect the incentive to produce original works and contribute to public well-being by assuring the creators an economic benefit of their creative activity.<sup>10</sup> By contrast, data protection attempts to maintain the incentive to participate in a democratic, pluralist society by securing the privacy, autonomy and integrity of individuals.<sup>11</sup>

---

amended), s. 45c. For further discussion, see S. Theedar, “Privacy in photographic images” (1999) 6 *Privacy Law & Policy Reporter* 75–78.

<sup>6</sup> See, e.g., the decision of the Federal Court of Australia in *Telstra Corporation Limited v. Desktop Marketing Systems Pty Ltd* [2001] FCA 612, 25 May 2001 in which Telstra Corporation Limited was found to hold copyright in the white and yellow page databases which it publishes. The case caused the shutdown of a reverse phone directory service (“blackpages”) operated by a third party. The service covered major cities in Australia. Given a phone number, it was able to find the name and address of the owner.

<sup>7</sup> See further L.A. Bygrave and K.J. Koelman, “Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems”, in *Copyright and Electronic Commerce* (P.B. Hugenholtz ed., 2000), pp. 59, 99 *et seq.*

<sup>8</sup> Note, though, that privacy considerations have figured in certain decisions of the German Federal Supreme Court (*Bundesgerichtshof*) limiting the ability of copyright-holders to monitor and prohibit private/domestic audio-recording practices. In this regard, see *Personalausweise* decision of 25 May 1964 [1965] GRUR 104; *Kopierläden* decision of 9 June 1983 [1984] GRUR 54. For other examples where privacy considerations appear to have played some role in setting boundaries for copyright, see Bygrave and Koelman, *ibid.*, pp. 102–103 and references cited therein.

<sup>9</sup> For an overview of these factors, see G. Greenleaf, “‘IP, Phone Home’: ECMS, ©-Tech, and Protecting Privacy against Surveillance by Digital Works”, in *Proceedings of the 21<sup>st</sup> International Conference on Privacy and Data Protection* (1999), pp. 281, 282–283.

<sup>10</sup> See generally J.A.L. Sterling, *World Copyright Law* (1998), pp. 57–61.

<sup>11</sup> See generally L.A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (2002), Chapter 7 and references cited therein.

## The digital dilemma – and responses

Any tensions that have existed between copyright and privacy rights as a result of the differences in their respective agenda, have been kept largely in abeyance up until recently. Now, however, a significant tension between the two sets of rights is emerging in the context of cyberspace. This tension arises not so much from the core natures of either set of rights. Rather, it arises from a particular response of copyright-holders to what is often termed the “digital dilemma”.<sup>12</sup> The “digital dilemma” with respect to copyright springs from the fact that the digital environment (including the technology that creates that environment) brings a greatly increased ability to copy information in breach of copyright.

The response by the copyright community to this threat has been, firstly, to conclude (indeed, to a great extent, *assume*) that the pre-existing balance of power struck between the interests of copyright-holders and the interests of information users, has shifted radically in favour of the latter. From this conclusion (or assumption) has flowed a second conclusion, which is that traditional user rights under copyright law need to be rolled back significantly. The result has been a vigorous campaign for reform of copyright law to strengthen the rights of copyright-holders at the expense of user rights, at least in relation to digital artefacts.

## Technologisation

The push for legal reform has been accompanied by increasing recognition that “the answer to the machine is in the machine” – to quote the now rather worn phrase of Clark.<sup>13</sup> Expressed alternatively using Lessig’s terminology,<sup>14</sup> the copyright community has become evermore aware of the important ways in which “code” or information systems architecture regulates how information can be used, and it has become determined to exploit these regulatory abilities for the protection of intellectual property. Thus, we see the development of a range of technological (and, to some extent, organisational) mechanisms to help secure copyright in digital artefacts. Taken together, these mechanisms have tended to go under the name of Electronic Copyright Management Systems; more recent terminology refers increasingly to Digital Rights Management Systems (DRMS).

In a nutshell, such systems provide an infrastructure allowing the creator of an information product to enforce copyright in the product when it is accessed online by other parties. This facility breaks down into several overlapping functions, the most central of which are, in summary:

- controlling access to information products;
- preventing the unauthorised copying of the products;

<sup>12</sup> See, e.g., Committee on Intellectual Property Rights and the Emerging Information Infrastructure; Computer Science and Telecommunications Board; Commission on Physical Sciences, Mathematics, and Applications; National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age* (2000).

<sup>13</sup> C. Clark, “The Answer to the Machine is in the Machine”, in *The Future of Copyright in a Digital Environment* (P.B. Hugenholtz ed., 1996), pp. 139–148.

<sup>14</sup> See generally L. Lessig, *Code, and Other Laws of Cyberspace* (1999).

- identifying the products and those who own copyright in them; and
- ensuring that the latter identification data are authentic.

Realisation of these functions is envisaged as being built around a variety of copyright-protective technologies involving, *inter alia*, steganography (e.g. digital watermarking for authentication of identification data), encryption (e.g. for controlling access to information products) and various electronic agents (e.g. web spiders for monitoring information usage).<sup>15</sup>

Currently, though, there is a paucity of fully operational DRMS involving all of the above functionalities.<sup>16</sup> Hence, much uncertainty still surrounds the exact ways in which they will operate.

The technologisation of copyright has a parallel in the field of privacy and data protection, where there is also increasing recognition of the need to create technological mechanisms that ensure respect for privacy interests particularly in the online world. These mechanisms go often under the name of Privacy-Enhancing Technology (PETs).<sup>17</sup> However, PETs have yet to receive the same sort of statutory backing as copyright-protective technologies are receiving – a point returned to below.

## Privacy implications

While uncertainty still surrounds the exact means and parameters of DRMS operations, little doubt exists that they will have the potential of amassing a great deal of data about the persons who purchase usage rights to information products. They will also have the potential of registering data about persons who merely *browse* – i.e. who inspect or sample information products without purchasing a particular right with respect to them. In both cases, data could be registered which are normally not registered in conjunction with ordinary shopping transactions effectuated in “meatspace”. Hence, a DRMS could facilitate the monitoring of what people privately read, listen to, view or sample, in a manner that is more comprehensive than what hitherto has been usual.<sup>18</sup> This surveillance potential would be augmented, of course, if a DRMS were integrated with other information systems so that the monitoring data could readily be combined with data about persons’ activities in other contexts, thus enabling the composition of fine-grained personal profiles.

This potential could not only weaken the privacy interests of information consumers to an unprecedented degree but also inhibit the expression of non-conformist opinions and

---

<sup>15</sup> For a relatively detailed overview of these mechanisms, see Greenleaf, *supra* n. 9, pp. 284–288. See also, e.g., D.S. Marks and B.H. Turnbull, “Technical Protection Measures: The Intersection of Technology, Law and Commercial Licences” [2000] E.I.P.R. 198, especially 212–213; K.J. Koelman and N. Helberger, “Protection of Technological Measures”, in *Copyright and Electronic Commerce* (P. B. Hugenholtz ed., 2000), pp. 165, 166–169; Koelman and Bygrave, *supra* n. 7, pp. 60 – 61, 108–110.

<sup>16</sup> For examples of existing systems, see D.J. Gervais, “Electronic Rights Management and Digital Identifier Systems” (1998) 4 *Journal of Electronic Publishing*, Issue 2, at <<http://www.press.umich.edu/jep/04-03/gervais.html>> (last visited 6.11.2001).

<sup>17</sup> For an overview, see, e.g., H. Burkert, “Privacy-Enhancing Technologies: Typology, Critique, Vision”, in *Technology and Privacy: The New Landscape* (P.E. Agre and M. Rotenberg eds., 1997), pp. 125–142.

<sup>18</sup> See further J.E. Cohen, “A Right to Read Anonymously: A Closer Look at ‘Copyright Management’ in Cyberspace” (1996) 28 *Connecticut Law Review* 981; Bygrave and Koelman, *supra* n. 7; Greenleaf, *supra* n. 9.

preferences.<sup>19</sup> Thus, a DRMS could function as a kind of digital Panopticon. This eventuality has unsettling implications for the long-term health of pluralist, democratic society. It remains to be seen just how effectively data protection laws will be able to reign in such an eventuality – a point dealt with in more detail below.

## Other problematic consequences – w(h)ither the soul of copyright?

A DRMS will also have the potential to reduce the autonomy of information consumers in another, less subtle way by enabling the ready imposition of predetermined licensing conditions on information usage. There is a danger that such conditions will undercut the exemptions from copyright which traditionally are provided under copyright law (e.g. for private use of information products). As Koelman notes, this danger is also attributable to the current limitations in the ability of technology itself to take due account of the numerous lawful copyright exemptions – “[t]echnology – at this stage – is simply too crude to accommodate all the subtleties of the law”.<sup>20</sup> The danger could be augmented by the enactment of legal rules restricting the circumvention of copyright-protective technologies even in cases when these technologies render nugatory the lawful copyright exemptions.<sup>21</sup>

The technologisation of copyright has troubling implications not just for the autonomy and privacy of information users but also for broader social discourse. Knowledge is increasingly structured and distributed by digital information systems. Thus, the technologisation of copyright will increasingly impinge on knowledge flows. Concomitantly, how technologisation occurs is vitally important for the quality of social discourse, particularly the extent to which we are able to maintain ‘digital diversity’ and a broad public domain.<sup>22</sup> An aggressive technologisation of copyright could seriously impair the flow of knowledge throughout society, with the impoverishment of social discourse as a further result.

Additionally, technologisation will have consequences for the long-term status of copyright law. It is likely to facilitate the use of contract as the primary means of regulating usage of copyrighted material,<sup>23</sup> thus helping to marginalise traditional copyright law in favour of contract law – at least in the digital context. In broader terms, this is a development in which enforcement of intellectual property rights increasingly relies on private fiat, decreasingly on public law with its finely tuned balance of interests.<sup>24</sup>

---

<sup>19</sup> *Ibid.*

<sup>20</sup> K.J. Koelman, “The protection of technological measures vs. the copyright limitations”, Paper presented at the ALAI Congress, “Adjuncts and Alternatives for Copyright”, New York, 15. June 2001, at <<http://www.ivir.nl/publications/koelman/alaiNY.htm>>.

<sup>21</sup> See further, e.g., T.C. Vinje, “Copyright Imperilled?” [1999] E.I.P.R. 192, 197 *et seq.*; J.E. Cohen, “Some Reflections on Copyright Management Systems and Laws Designed to Protect Them” (1997) 12 *Berkeley Technology Law Journal* 161, especially 179 *et seq.* Note too criticism of the efficacy of the E.C. copyright Directive of 2001 (particularly Art. 6(4)) in countering this danger: see, e.g., T.C. Vinje, “Should We Begin Digging Copyright’s Grave?” [2000] E.I.P.R. 551, 556–558; P.B. Hugenoltz, “Why the Copyright Directive is Unimportant, and Possibly Invalid” [2000] E.I.P.R. 499, 500.

<sup>22</sup> See further B. Fitzgerald, “Intellectual Property Rights in Digital Architecture (including Software): The Question of Digital Diversity” [2001] 23 E.I.P.R. 121–127. See also, e.g., P.B. Hugenoltz, “Code as code, or the end of intellectual property as we know it” (1999) *Maastricht Journal of European and Comparative Law* 308, 316 *et seq.* and references cited therein.

<sup>23</sup> As Hugenoltz aptly notes, “technological measures will be applied mostly in combination with contract”: *ibid.*, 312.

<sup>24</sup> See further, e.g., C.E.A. Karnow, *Future Codes: Essays in Advanced Computer Technology and the Law* (1997), chapter 3; T.C. Vinje, “A Brave New World of Technical Protection Systems: Will There Still be Room for Copyright?” [1996] E.I.P.R. 431, especially 437.

Finally, the technologisation of copyright will have profound consequences for the way in which copyright is perceived by the community at large – a point that has not been sufficiently emphasised in policy discussions to date. The push by copyright-holders to pre-emptively secure copyright in ways that greatly impinge on the privacy and autonomy of information consumers, is leading to accusations of regulatory overreaching.<sup>25</sup> Lending strength to such accusations is the trend by legislators to give strong statutory backing to copyright-protective technologies – a development returned to further below. Also lending strength to such accusations is the failure by copyright-holders to adequately supply empirical justification for their claim that they shall be ripped off to an unprecedented degree if they do not apply copyright-protective technologies and obtain extensive statutory support for these. There already exists considerable antipathy or indifference to copyright amongst many information consumers. The perception of regulatory overreaching which comes in the wake of technologisation exacerbates these attitudes and fosters a crisis of legitimacy for the copyright industry.

To sum up so far, the technologisation of copyright could well have troubling consequences for the privacy and autonomy of information users. It could also have troubling consequences for the long-term status of, and respect for, copyright law. Indeed, one is tempted to say that, with extensive technologisation, copyright could well end up losing its soul.

## The copyright Directive

The use of copyright-protective technologies is being afforded strong statutory support. In Europe, this support is provided primarily by Articles 6 and 7 of the copyright Directive passed in 2001, and more indirectly by Articles 11 and 12 of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996.<sup>26</sup> Article 6 of the Directive stipulates, in summary, that adequate legal protection shall be provided against the intentional circumvention of any effective “technological measures” (i.e. copyright-protective technologies). Article 7 of the Directive stipulates, in summary, that adequate legal protection shall be provided against: (a) the intentional and unauthorised alteration or removal of “electronic rights management information”; and (b) the distribution of copyrighted works from which such information has been removed or altered, in the knowledge that such distribution breaches copyright. Articles 11 and 12 of the WIPO Copyright Treaty (WCT) are broadly similar to these provisions. In the following, focus is put on the Directive rather than the WCT.

The above provisions are complex and raise numerous issues of interpretation.<sup>27</sup> Two such issues are broached in this opinion. Both concern directly the privacy-invasive potential of copyright-protective technologies.

<sup>25</sup> See, e.g., Hugenholtz, *supra* n. 22, 314–315; P. Samuelson, “Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised” (1999) 14 *Berkeley Technology Law Journal* 519.

<sup>26</sup> See too the mirroring provisions in Articles 18 and 19 of the WIPO Performances and Phonograms Treaty of 1996.

<sup>27</sup> For analysis of some of these issues, see, e.g., K.J. Koelman, “A Hard Nut to Crack: The Protection of Technological Measures” [2000] 22 E.I.P.R. 272–280; Koelman and Helberger, *supra* n. 15, pp. 169 *et seq.*; A.M.E. de Kroon, “Protection of Copyright Management Information”, in *Copyright and Electronic Commerce* (P.B. Hugenholtz ed., 2000), pp. 229, 250 *et seq.*

The first issue is whether the concept of “technological measures” in Article 6 of the Directive (and Article 11 of the WCT) extends to devices that monitor usage of copyrighted information. If such devices are not covered, then their disablement will not constitute a breach of Article 6(1). This, of course, would be the most privacy-friendly result. If such devices are covered, their disablement will, *prima facie*, violate Article 6(1), though the violation could perhaps be legitimised pursuant to data protection law. Note that Article 9 of the Directive states that its provisions shall be without prejudice to legal provisions in other areas, including data protection and privacy. As indicated further below, however, the efficacy of data protection law in this context is unclear.

The Directive itself provides no obvious answer to the issue. This is also the case with the WCT. However, there can be little doubt that some monitoring devices are covered, given the broad way in which “technological measures” is defined in the Directive – i.e. as “any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts [in breach of copyright] ...” (Article 6(3)). At the same time, the requirement that the device be concerned with copyright protection in the *normal* course of its operation, could be taken to mean that monitoring devices which are only *incidentally* concerned with such protection fail to qualify as technological measures. This would be the case, for example, with ordinary devices for the setting of so-called “cookies” and/or “web bugs” (also termed “1-pixel gifs”). One might also query whether devices that *merely* carry out monitoring tasks (albeit with copyright protection as the primary purpose) can properly be viewed as “designed to prevent or restrict” breaches of copyright. However, it is easier to argue that monitoring *per se* can have the requisite preventative/restrictive function – indeed, to argue otherwise would ignore the increasingly self-evident control dynamics that are central to the notion of panopticism.

It is instructive to compare Article 6 of the Directive with section 1201(i) of the U.S. Digital Millennium Copyright Act (DMCA). The latter provision permits the disabling of *access controls* upon certain conditions:

- 1) the access controls collect or disseminate information about the online activities of a person;
- 2) conspicuous notice about this information processing is not given;
- 3) the data subject is not provided the ability to prevent the information being gathered and disseminated; and
- 4) the disabling of the controls has the sole effect, and is solely for the purpose, of preventing the collection and dissemination.

This provision seems clearly aimed at allowing for the disabling of ordinary “cookies”-mechanisms and “web bugs” (if all of the above conditions apply). However, doubts have been raised about its application to other monitoring devices that are more integral to copyright-protective technologies.<sup>28</sup> Its practical utility is also questionable given that the DMCA restricts the supply of tools that could disable the access controls in question.<sup>29</sup>

The second issue concerns the scope of what the copyright Directive terms “rights management information” (RMI). More specifically, the issue is whether personal data relating to a consumer

---

<sup>28</sup> See Samuelsen, *supra* n. 25, 553 *et seq.*

<sup>29</sup> DMCA, s. 1201(a)(2) and (b)(1).

of copyrighted information are to be treated as a necessary component of RMI. The issue is important because if such data are *not* to be treated as a necessary component, alteration or erasure of such data by an information consumer cannot fall foul of Article 7(1).

The term RMI is defined in Article 7(2) as including “information about the terms and conditions of use of the [copyrighted] work or other subject matter”. The same pertains to the definition of RMI in Article 12(2) of the WCT. Does information about “terms and conditions of use” necessarily include personal data about the users of copyrighted works? Does it necessarily include personal data relating to how the works are used? The expression “terms and conditions of use” does not, *prima facie*, comfortably embrace such data.<sup>30</sup> However, given that some information usage licences may be quite user-specific, it is arguable that such data may be covered.<sup>31</sup> Support for this argument can also be derived from recital 57 in the preamble to the Directive which recognises that RMI-systems may “process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour”.

By contrast, section 1202 of the U.S. DMCA specifically defines “copyright management information” (the equivalent to RMI) as excluding digital information used for monitoring usage of copyrighted works. Again, the U.S. legislation appears at first blush to be more privacy-friendly than the Directive.<sup>32</sup>

If personal data about information users are to be treated as a component of RMI, the removal or alteration of such data will only breach Article 7(1) if the act concerned is unauthorised. The requisite authority may probably be derived from legislation, particularly legislation on privacy/data protection.<sup>33</sup> The question then becomes whether and to what extent alteration or erasure of the data is actually permitted or required pursuant to data protection laws. This is a difficult question: the answers to it will tend to vary from jurisdiction to jurisdiction and depend on the outcome of complex, relatively open-ended interest-balancing processes that hinge considerably on an assessment of what information processing is “necessary” in the particular circumstances of the case.<sup>34</sup>

In Europe, the most important privacy safeguards in this respect will have to be derived primarily from the E.C. Directive on data protection, together with national laws implementing it. The Directive will permit the non-consensual registration and further processing of data on consumers of copyright-protected works if, in summary, the processing is necessary for the performance of a contract or for the establishment, exercise or defence of legal claims or for realising legitimate

---

<sup>30</sup> Bygrave and Koelman (*supra* n. 7, p. 115) claim accordingly that such data appear not to be covered by the definition of RMI in the WCT.

<sup>31</sup> This is also the line taken by Greenleaf, *supra* n. 9. Bygrave and Koelman (*ibid*) recognise this possibility too.

<sup>32</sup> This is not to say, though, that information consumers in the U.S.A. therefore enjoy generally more legal protection for their privacy than information consumers in Europe do. It is probably more accurate to say that, on the whole, legal protection for information consumers’ privacy is more extensively and systematically built up in European jurisdictions than it is in the U.S. See generally P.M. Schwartz and J.R. Reidenberg, *Data Privacy Law: A Study of United States Data Protection* (1996). The apparent disparity is partly evidenced by the “safe harbor” agreement which was concluded in July 2000 between the U.S. and E.U. and which stipulates conditions for permitting the flow of personal data from the E.U. to the U.S. See E.C. Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce (O.J. L 215, 25.8.2000, 7 *et seq.*).

<sup>33</sup> See also de Kroon, *supra* n. 27, p. 254. Note too Article 9 referred to in the main text above.

<sup>34</sup> See further the extensive analysis of European data protection rules in Bygrave and Koelman, *supra* n. 7, especially pp. 75–97.

interests that outweigh the privacy interests at stake.<sup>35</sup> If these conditions are construed liberally, information consumers will find it difficult to legitimately remove or alter data about them registered by DRMS operators.

Recital 57 in the copyright Directive stipulates that “technical” privacy safeguards for such data “should” be incorporated in accordance with the data protection Directive. Thus, the recital goes some way to encouraging the use of PETs. However, from a privacy perspective, recital 57 is disappointing. It is disappointing for three reasons.

First, it seems to link the use of PETs only to the design and operation of RMI-systems, not also to the design and operation of the technological measures referred to in Article 6. This is rather incongruous as the ongoing monitoring of information usage is most likely to occur through the application of these technological measures.<sup>36</sup> Certainly, data protection rules and measures may still apply in the context of Article 6 – particularly given Article 9 – but it would have been preferable for the Directive to encourage more directly the use of PETs in that context too.

Secondly, recital 57 appears not to *mandate* the use of PETs. It states only that privacy safeguards “should”, not “shall”, be incorporated.

Thirdly, the reference in the recital to the data protection Directive is problematic because that Directive fails to specifically address the use of PETs.<sup>37</sup> Moreover, the data protection Directive has very little to say about the desirability of transactional anonymity or even pseudonymity. Certainly, parts of the Directive – particularly Articles 6 to 8 stipulating the basic conditions for when personal data may be processed – can be read as encouraging transactional anonymity,<sup>38</sup> but this encouragement is far from direct. By contrast, German federal legislation on data protection contains relatively far-reaching provisions specifically mandating transactional anonymity and, to some extent, pseudonymity.<sup>39</sup> It is to be hoped that the German approach inspires greater legislative support for transactional anonymity and pseudonymity in other jurisdictions too.

More generally, several question marks hang over the extent to which data protection laws will apply to DRMS operations. These question marks arise not just because of continuing uncertainty about how DRMS will function in practice but also because of uncertainty about the ambit of data protection laws in a digital context. Perhaps the most significant issue here relates to the fact that data protection laws tend to apply only when data are personal; i.e. can be linked to identifiable natural/physical persons. It is to be expected, though, that DRMS operations will involve to a considerable degree the processing of so-called “clickstream” data that are primarily

---

<sup>35</sup> *Ibid*, pp. 75–78. More stringent conditions apply for the processing of certain categories of especially sensitive personal data, though exactly which types of data would fall within these categories in a DRMS context is somewhat unclear: *ibid*, pp. 78–81.

<sup>36</sup> Further, as Dusollier points out, the definition of RMI in Art. 7 as information “provided by rightholders”, does not accurately apply to the situation in which information usage is actively monitored; such monitoring will rather occur as an automatic function of a technological measure referred to in Art. 6. See S. Dusollier, “Electrifying the Fence: The Legal Protection of Technological Measures for Protecting Copyright” [1999] E.I.P.R. 285, 296.

<sup>37</sup> Perhaps this is why recital 57 does not mandate PET application.

<sup>38</sup> See further Bygrave, *supra* n. 11, chapter 18.

<sup>39</sup> See particularly §§ 3(4), 4(1), 4(4) and 6(3) of the Teleservices Data Protection Act (*Teledienstedatenschutzgesetz*) of 1997. Also noteworthy are the recently enacted provisions on “Datenvermeidung” and “Datensparsamkeit” in § 3a of the 1990 Federal Data Protection Act (*Bundesdatenschutzgesetz*) as amended in May 2001.

linked to the Internet protocol (IP) addresses of computers. The extent to which such data may qualify as personal data for the purposes of data protection law is still being worked out.<sup>40</sup> Moreover, it is to be expected that DRMS will involve, to a large extent, the use of various types of electronic agents – i.e. software applications which, with some degree of autonomy, mobility and learning capacity, execute specific tasks for a computer user or computer system. Again, the way in which the operations of these agents may fall within the ambit of data protection legislation is only just beginning to be systematically considered.<sup>41</sup>

## Considerations for the future

A problem with much of the debate about the implications of new forms of copyright protection is that it is accompanied by a large degree of uncertainty. As this opinion highlights, uncertainty reigns on many fronts. There is uncertainty about the parameters and *modus operandi* of DRMS; uncertainty about the ambit and application of legal rules with respect to both copyright and data protection; and uncertainty about the impact of market mechanisms. Hence, the debate is largely based on assumptions about potentialities. This is an important point to bear in mind.

Indeed, current concerns about the technologisation of copyright might end up being largely unsubstantiated. We might be conjuring up a threatening mountain out of what proves to remain a molehill. Several factors could serve to hinder the large-scale implementation of privacy-invasive DRMS. Such systems might be marginalised by market mechanisms – for example, strong consumer preferences for privacy, combined with competition between copyright-holders to satisfy these preferences.<sup>42</sup> The take-up of privacy-invasive DRMS might also be hindered by difficulties in achieving standardisation and compatibility of technological measures.<sup>43</sup>

These uncertainties notwithstanding, future policy must aim to prevent copyright-protective mechanisms from knocking down privacy and related interests through technological fiat or one-eyed lobbying on the part of copyright-holders. Such interests should not be sacrificed given their importance for the vitality of democratic, pluralist society.

Moreover, if copyright-protective mechanisms trample over privacy, it is highly likely that copyright-holders will lose financially if not in other ways. Copyright is easier to swallow if it is seen as respecting users' privacy and autonomy. Further, copyright-holders should benefit if electronic commerce takes off, and electronic commerce is likely to take off only if consumer privacy is seen to be protected. Considerable evidence exists to indicate that numerous consumers are reluctant to enter into online commercial transactions because they fear for their privacy.<sup>44</sup>

---

<sup>40</sup> For preliminary discussion of the issue, see G. Greenleaf, 'Privacy principles – irrelevant to cyberspace?' (1996) 3 *Privacy Law & Policy Reporter* 114–115; Bygrave and Koelman, *supra* n. 7, pp. 72–73; Bygrave, *supra* n. 11, chapter 18.

<sup>41</sup> For a preliminary analysis, see L.A. Bygrave, "Electronic Agents and Privacy: A Cyberspace Odyssey 2001" (2001) 9 *International Journal of Law and Information Technology* 275.

<sup>42</sup> See also Samuelsen, *supra* n. 25, 565–566. Cf. Hugenholtz, *supra* n. 22, p. 312 (noting previous instances of the market marginalisation of certain anti-copying devices because of their irritation to consumers).

<sup>43</sup> There exists a myriad of competing standards with respect to the structuring and provision of RMI. See further Gervais, *supra* n. 16.

<sup>44</sup> See, e.g., A. Bhatnagar, S. Misra and H. Raghav Rao, "On Risk, Convenience, and Internet Shopping Behavior" (2000) 43 *Communications of the ACM* 98.

A second objective should be to work towards a better integration of technological measures for protecting copyright with PETs. As noted above, the technologisation of copyright has a parallel in the technologisation of privacy and data protection. This parallel should be exploited for the benefit of privacy and data protection. A large range of technological and organisational mechanisms exist to enforce copyright in a digital environment. Some are more privacy-invasive than others. We need to encourage the development and application of the least privacy-invasive devices. Such encouragement is actually required already by some laws, particularly in Germany, and it arguably follows, though more indirectly, from the data protection Directive.