

4.2.2 Digital Rights Management and Privacy — Legal Aspects in the European Union¹⁰²⁴

Lee A. Bygrave¹⁰²⁵

I Introduction

As legal phenomena, intellectual property rights and privacy rights have tended to live separate lives. At the same time, regimes for protecting intellectual property have had, up until lately, only a marginal practical impact on the privacy of information users. However, recent developments in Digital Rights Management Systems (DRMS) are bringing to the fore considerable tension between the enforcement of intellectual property rights and the maintenance of consumer privacy. This tension arises not so much out of differences between the basic nature of intellectual property and that of privacy. Rather, it arises from a push by the holders of intellectual property rights (and their intermediaries) to secure their interests by utilising DRMS with the potential to facilitate an unprecedented degree of surveillance of consumers' reading, listening, viewing and browsing habits. The basic purpose of this chapter is to explore this tension and discuss how it is likely to be resolved in terms of European Community (EC) law.

II The Traditional Relationship between Intellectual Property Rights and Privacy Rights

Intellectual property rights and privacy rights share a great deal in their respective origins and agenda. Both have grown to a considerable extent from the same soil provided by doctrines on personality rights. This growth process has involved some cross-fertilisation of the two sets of interests: notions of intellectual property have helped to develop privacy rights, and notions of privacy have helped to develop intellectual property rights.¹⁰²⁶

This cross-fertilisation has existed not just at a theoretical level but also in practice. For example, copyright law has furthered privacy interests by restricting publication of certain film material in which persons are portrayed,¹⁰²⁷ and by restricting the ability of third parties to duplicate and further exploit

¹⁰²⁴ Much of this chapter is based on work published in Bygrave (2002a) and Bygrave, Koelman (2000). Thanks to Kamiel Koelman and Graham Greenleaf for helpful commentary along the way. All following references to Internet addresses were current as of 1st March 2003.

¹⁰²⁵ Norwegian Research Centre for Computers and Law, University of Oslo.

¹⁰²⁶ See, e.g.: Warren, Brandeis (1890): 198 (arguing, *inter alia*, that common law protection of intellectual property is based upon a broader principle of protection of privacy and personality).

¹⁰²⁷ See, e.g., the United Kingdom's Copyright, Designs and Patents Act 1988 (as amended), s. 85(1); Norway's Intellectual Property Act 1961 (*lov om opphavsrett til åndsverk m.v. 12. mai 1961 nr. 2*; as amended), § 45c. For further discussion, see: Theedar (1999).

personal data compiled in certain registers.¹⁰²⁸ Moreover, the exemptions to copyright provided in relation to the “private” or “fair” use of copyright works help to prevent copyright impinging unduly upon the private sphere of information consumers.¹⁰²⁹ At the same time, privacy rights in the form of data protection law aid copyright by limiting the registration and dissemination of personal data that might subsequently be used in breach of copyright.

Nevertheless, there exist fundamental differences between the respective concerns of these two sets of rights. Put somewhat simplistically, the steering axiom for privacy advocates is “knowledge is power”. For holders of intellectual property rights (and their intermediaries), a steering axiom of greater importance is “knowledge is wealth”. More specifically, copyright — broadly conceived — 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.¹⁰³⁰ By contrast, privacy rights in the form of data protection law attempt to maintain the incentive to participate in a democratic, pluralist society by securing the privacy, autonomy and integrity of individuals.¹⁰³¹

It is also apparent that active consideration by privacy advocates for intellectual property rights has tended to be incidental and *ad hoc*. The concern of copyright-holders for privacy rights can be characterised the same way. Concomitantly, the “private use” and “fair use” exemptions in copyright law are arguably grounded not so much upon privacy considerations but on the interest of the wider community in gaining access to the fruits of creative endeavour.¹⁰³² Indeed, the fact that intellectual property regimes have tended, up until lately, to have had only a marginal practical impact on the privacy of information users is due mainly to two interlinked factors that have little to do with intellectual property law *per se*. First, the sale of copyright material from copyright-holders or their intermediaries to end-users of the material has traditionally been able to be carried out

¹⁰²⁸ See, e.g., the decision of the Federal Court of Australia in *Telstra Corporation Limited v. Desktop Marketing Systems Pty Ltd* [2001] FCA 612, 25th 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.

¹⁰²⁹ See: Bygrave, Koelman (2000): 99ff.

¹⁰³⁰ See: Sterling (1998): 57–61.

¹⁰³¹ See: Bygrave (2002b): Chapter VII and references cited therein.

¹⁰³² 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 25th May 1964 [1965] GRUR 104; *Kopierläden* decision of 9th June 1983 [1984] GRUR 54. Similarly, privacy considerations have played a significant role in Norwegian policy here: see, e.g.: *Norges Offentlige Utredninger*, 1983, no. 35, p. 36. For other examples where such considerations appear to have played some role in setting boundaries for copyright, see: Bygrave, Koelman (2000): 102–103 and references cited therein.

as an anonymous cash transaction. Secondly, the material itself has been unable to monitor and report on its usage.¹⁰³³

III Defining Privacy and Related Interests

What is exactly meant by the concept of “privacy”? The concept is notoriously difficult to define precisely, and the considerable literature on the subject proffers a large number of partly conflicting definitions.¹⁰³⁴ For present purposes, “privacy” denotes a state of limited accessibility. More specifically, it denotes a state in which a person (or organisation) is more or less inaccessible to others, either on the spatial, psychological or informational plane.¹⁰³⁵

Privacy as thus defined is closely related to, though not fully commensurate with, autonomy (i.e., self-determination). The latter is an example of an interest which can promote privacy at the same time as privacy can promote it. Such interests are hereinafter termed “privacy-related interests”.¹⁰³⁶ Other important interests in this category are, at the level of the individual, integrity (i.e., a person’s state of intact, harmonious functionality based on other persons’ respect for him/her) and dignity (i.e., a person’s intrinsic worth). At a societal level, important privacy-related interests are democracy (i.e., active participation of citizens in public government of societal processes) and pluralism (i.e., diversity of opinions and lifestyles, plus diffusion of power such that one single group or organisation does not dominate other groups/organisations).

IV The Operational Parameters of DRMS in a Privacy Perspective

The basic functions of DRMS are envisaged as follows:

- (i) controlling access to copyright works (and possibly other information products);
- (ii) restricting unauthorised reproduction (and possibly other usage) of such works;
- (iii) identifying the works, the relevant right-holders (and possibly the conditions for authorised usage of the works); and
- (iv) protecting the authenticity of the latter identification data.¹⁰³⁷

Facilitating each of these functions are a variety of technologies.¹⁰³⁸ These technologies can involve, *inter alia*, steganography (e.g., “digital watermarks”¹⁰³⁹ for

¹⁰³³ For more detail on these and other relevant factors, see: Greenleaf (2002): 37–38.

¹⁰³⁴ For an overview, see: Inness (1992).

¹⁰³⁵ See also, *inter alia*: Gavison (1980): 428–436; Bok (1982): 10.

¹⁰³⁶ For further analysis of such interests, see, e.g.: Bygrave (2002b): Chapter 7.

¹⁰³⁷ See generally Part 2 of this volume.

¹⁰³⁸ Again, see generally Part 2 of this volume. See also: Greenleaf (2002): 43–46; Marks, Turnbull (2000): 212–213; Koelman, Helberger (2000): 166–169; Bygrave, Koelman (2000): 60–61, 108–110.

dissemination and authentication of identification data), encryption (e.g., for controlling access to information products) and various electronic agents (e.g., “web spiders”¹⁰⁴⁰ for monitoring information usage).

It should be stressed, though, that many DRMS are still at the design stage. Accordingly, some uncertainty exists about their exact *modus operandi* once they are implemented on a wide scale.¹⁰⁴¹ For many systems, the exact functions and inter-relationships of some of the system actors — publishers, media distributors, certification authorities, etc. — have not yet been delineated. Uncertainty also surrounds the amount and content of data that these actors will register, the precise nature of the payment mechanisms to be employed, and the degree to which various DRMS will be kept separate from other information systems. From a privacy perspective, important questions include the extent to which DRMS will collect and further process *personal* data (i.e., data which relate to, and enable identification of, an individual person — see further *Scope of data protection law* in section V below), the purposes for which these data will be used and the conditions under which they will be disseminated to external actors.

In light of the above-listed functions and technological mechanisms, it is highly likely that many, if not most, DRMS will register at least some personal data relating to purchasers of copyright works (and possibly other information products).¹⁰⁴² This registration will tend to occur pursuant to contract. The registered data could be stored centrally within the system and/or embedded as (part of) digital watermarks in the works themselves. The works might also be configured to enable ongoing (or periodical) registration of the way in which they are used by the purchaser, transmission of these usage data back to a central monitoring service provider, and/or automatic renewal/modification of usage rights on the basis of online interaction with the provider — i.e., what Greenleaf aptly terms “IP, phone home”.¹⁰⁴³

Systems might also register data relating to persons who merely engage in online browsing (i.e., inspecting or sampling an information product without purchasing a particular right with respect to it). Such registration could automatically occur through the use, for example, of “cookies” mechanisms¹⁰⁴⁴ or “web bugs”¹⁰⁴⁵.

¹⁰³⁹ In brief, a “digital watermark” is digital code which is embedded into text, video or audio files and which typically contains data about the usage rights attached to the files: see further Petitcolas in this volume (page 81).

¹⁰⁴⁰ “Web spider” is the name commonly used for Internet search engines — i.e., software robots that trawl, retrieve and index data stored on the Internet, see further: <http://www.monash.com/spidap4.html>.

¹⁰⁴¹ For examples of existing systems, see generally Part 2 of this volume. See also: European Commission (2002); Gervais (1998).

¹⁰⁴² More accurately, what is being purchased is an on-line disseminated copy (or copies) of, and/or certain usage rights with respect to, such materials.

¹⁰⁴³ See: Greenleaf (2002).

¹⁰⁴⁴ By “cookies” is meant transactional data, in the form of a simple text file, about a browser’s Internet activity which are automatically stored by an Internet server on the browser’s computer, often without the browser’s

Alternatively, it could occur more explicitly through making access to material (that has been otherwise “fenced off” using encryption methods) conditional upon disclosure and registration of browser identity.

An additional category of personal data, which will flow through most points of a DRMS, are the unique numbers (International Standard Work Codes or the like) that identify the creators, authors, editors, etc., of copyright works. In the following, however, attention is directed to purchaser- and browser-related data since the processing of these raises the most significant privacy-related issues.

The privacy of purchasers and browsers will be potentially affected at all stages of the data-processing cycle inherent in a DRMS — from the initial registration of data to their subsequent re-usage — at least insofar as the data are personal (i.e., can be linked to an identifiable purchaser or browser). The collection or further processing of the data will tend to render the data subjects (i.e., the person(s) to whom the data relate) more transparent *vis-à-vis* the system operator(s) and possibly external actors.

The data processing could concurrently impinge on a multiplicity of privacy-related interests. The autonomy of a purchaser or browser will be diminished, for example, if a DRMS facilitates the processing of data about them without their consent or knowledge, or if the processing causes them to behave along lines determined primarily by the system operator(s). Further, their integrity could be detrimentally affected and their dignity affronted if the processing does not conform with their expectations of what is reasonable — which will often be the case with non-consensual or covert data processing.

Tensions between DRMS and privacy-related interests are likely to be particularly sharp in connection with the (re-)use of personal data for secondary purposes (i.e., purposes that differ from the purposes for which the data were first collected). A typical example here is when personal data originally collected in order to ensure enforcement of a particular transaction are subsequently employed for the purposes of cross-selling or other marketing of products *vis-à-vis* the data subjects. Such “re-purposing” of data will be especially unsettling if it occurs without the data subjects’ prior consent or if it falls outside their reasonable expectations. It will also be problematic, not just for the data subjects but also the data user(s), if it involves applying the data for purposes for which the data are not suited.

Privacy and related interests could additionally come under fire when copyright-holders (or their representatives) seek information from third parties about the

knowledge. Cookies mechanisms are primarily aimed at customising an Internet service for the browser’s subsequent use of the service or linked services. For further description of such mechanisms and the issues they pose for privacy, see: Mayer-Schönberger (1998).

¹⁰⁴⁵ By “web bugs” is meant miniscule images, commonly in the form of opaque, 1-by-1 pixel GIFs (graphic files), which are embedded in website pages or electronic mail with the aim of transmitting information to a remote computer when the pages or mail are viewed. Their presence and function are usually invisible to browsers. See further: <http://www.privacyfoundation.org/resources/webbug.asp>.

identity of persons who are purportedly infringing copyright. Disclosure of such information could well involve the “re-purposing” of personal data. The current litigation between the Recording Industry Association of America (RIAA) and Verizon Internet Services provides a case in point. Here Verizon — an Internet Service Provider (ISP) — has been served with a subpoena to disclose the identity of one of its customers who is alleged to have unlawfully downloaded music files in which copyright subsists. The RIAA has knowledge of only the Internet Protocol (IP) address of the customer. Verizon is resisting enforcement of the subpoena partly on privacy grounds, but lost in the first round of litigation.¹⁰⁴⁶

The problems described above are not unique to DRMS; they can arise in the context of many other data-processing systems, both commercial and non-commercial. Nevertheless, by their very nature, DRMS will play a pivotal role in determining the character of surveillance of persons’ reading, listening and viewing habits, particularly in what hitherto has been commonly regarded as the private sphere. Monitoring of these habits could well end up being considerably more extensive than previously. Indeed, it is not difficult to envisage a situation in which DRMS come to form a kind of digital Panopticon that not only diminishes consumers’ privacy but inhibits their expression of non-conformist opinions and preferences.¹⁰⁴⁷ These control dynamics would have disturbing implications for the well-being of pluralist, democratic society.¹⁰⁴⁸ Their effect would be exacerbated in tact with the extent to which each DRMS is linked with other information systems containing personal data about consumers.

The amount and content of consumer data which are registered in a DRMS, along with the ways in which these data are further processed, will be determined by a large range of factors. The focus of this chapter is on legal factors, particularly the limitations set by data protection laws. Yet we must not forget that other types of factors — commercial, technological, organisational — play important roles too. For instance, the business backgrounds of the actors running DRMS will have significant consequences for how much purchaser- or browser-related data are registered and the uses to which the data are subsequently put.

As Greenleaf notes, many DRMS

*“will be run directly by publishing houses with lots of different products to shift and a strong interest in secondary use of identified consumption data, or by booksellers with a similar combination of interests. We will not always be ‘lucky’ enough either to have some central industry-based monitoring body standing between consumers and publishers trying to act as an ‘honest broker’, or to be dealing direct with the author who has only her own product to sell. Which business models succeed will have a significant effect on privacy”.*¹⁰⁴⁹

¹⁰⁴⁶ See: *Recording Industry Association of America v. Verizon Internet Services*, decision of 21st January 2003 by Judge Bates of the US District Court for Columbia.

¹⁰⁴⁷ See: Cohen (1996); Bygrave, Koelman (2000); Greenleaf (2002).

¹⁰⁴⁸ On panopticism and its effects, see: Lyon (1994); Gandy (1993).

¹⁰⁴⁹ See: Greenleaf (2002): 51.

At the same time, though, some DRMS operators could conceivably be willing to minimise registration and usage of purchaser- and browser-related data in order to attract the custom of persons who fear for their privacy in the online world. It is well-established that privacy fears pose a major hindrance to broad consumer take-up of electronic commerce.¹⁰⁵⁰ Hence, there exists a marketplace incentive for DRMS operators to attempt to assuage such fears. While consumer concern for privacy is often fickle and myopic,¹⁰⁵¹ the point remains that promotion of consumer privacy can translate into promotion of commercial interests. And the readiness of people to enter into electronic commerce as consumers (or, perhaps more accurately, as “prosumers”) is likely to depend at least in part upon the extent to which they feel assured that their privacy and related interests will be respected by other marketplace actors.

V The Impact of Data Protection Law on DRMS

V.1 Point of Departure for Analysis

The following analysis canvasses the impact of data protection law on DRMS using the EC Directive on data protection of 1995 (hereinafter also “DPD”)¹⁰⁵² as the principal regulatory point of departure. The aim of the analysis is to give a broad-brush treatment of the main issues at hand.¹⁰⁵³

While not the only international regulatory instrument on data protection, the DPD is, in practical terms, the most influential such instrument for the European Union (EU) as a whole.¹⁰⁵⁴ It goes the furthest in terms of providing prescriptive guidance on data protection across a range of sectors. At the time of writing this Chapter, the DPD has been transposed into national legislation by the vast majority of EU Member States, along with most of the East European countries that are poised to gain membership of the Union. Pursuant to its incorporation into the 1992 Agreement on the European Economic Area (EEA), the DPD has also been implemented by those countries that are not members of the EU but

¹⁰⁵⁰ See, e.g.: Bhatnagar, Misra, Raghav Rao (2000); Samarijiva (1997): 282ff.

¹⁰⁵¹ See, e.g.: Froomkin (2000): 1501ff.

¹⁰⁵² See: Directive 95/46/EC of the European Parliament and of the Council of 24th 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, 23rd November 1995, 31 et seq.)

¹⁰⁵³ A more detailed analysis is found in Bygrave, Koelman (2000).

¹⁰⁵⁴ For an overview of the other main international instruments, see: Bygrave (2002b): 30ff. Special mention should be made of the provisions on the right to privacy set down in Art. 8 of the 1950 European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR) and in Art. 17 of the 1966 International Covenant on Civil and Political Rights. These provisions provide much of the formal normative basis for data protection instruments like the DPD at the same time as they function as data protection instruments in their own right. However, case law developed pursuant to them so far adds little if anything to the principles found in the DPD and, in some respects, falls short. See: Bygrave (1998).

party to the EEA Agreement (i.e., Norway, Iceland and Liechtenstein). Moreover, the Directive exercises considerable influence over other countries outside the E.U., not least because it prohibits, with some exceptions, the transfer of personal data to these countries if they do not provide “adequate” levels of data protection (DPD, Art. 25(1)).

In practice, though, what will directly impact on DRMS is not the DPD as such but national legislation transposing the Directive. On certain points, some of this legislation varies from the Directive and from the equivalent legislation of other EU Member States. This is because the Directive accords Member States a significant margin for manoeuvre when transposing its requirements. Nevertheless, the Directive does not envisage that such variation will incur conflict with its own rules or the respective legislation of other Member States.¹⁰⁵⁵

It is also important to note that the DPD is not the only EC data protection instrument with the potential to affect DRMS operations. The DPD is supplemented by the 2002 Directive on privacy and electronic communications (hereinafter also “DPEC”).¹⁰⁵⁶ The latter Directive replaces the 1997 Directive on privacy and telecommunications.¹⁰⁵⁷ The DPEC is aimed at extending and “fine-tuning” the principles of the DPD so that they may sensibly apply to the provision of “publicly available electronic communications services” that fall within the scope of Community law (DPEC, Arts. 1–3; see also preamble, recital 4). It is part of a regulatory package aimed primarily at regulating transmission networks and services as opposed to the *content* of communications.¹⁰⁵⁸ Although many DRMS are primarily concerned with managing exploitation of content rather than merely facilitating its transmission, parts of their operations could come within the ambit of the DPEC. This is significant because, as

¹⁰⁵⁵ See: Bygrave (2002b): 34–35 and references cited therein.

¹⁰⁵⁶ See: Directive 2002/58/EC of the European Parliament and of the Council of 12th July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (OJ L 201, 31st July 2002, 37 et seq.). The deadline for national implementation of this Directive is 31st October 2003 (Art. 17(1)).

¹⁰⁵⁷ See: Directive 97/66/EC of the European Parliament and of the Council of 15th December 1997 concerning the processing of personal data and the protection of privacy in the telecommunications sector (OJ L 24, 30th January 1998, 1 et seq.) — repealed as of 31st October 2003.

¹⁰⁵⁸ See: Directive 2002/21/EC of the European Parliament and of the Council of 7th March 2002 on a common regulatory framework for electronic communications networks and services (OJ L 108, 24th April 2002, 33 et seq.), particularly preamble, recital 5. Article 2(c) of this Directive defines “*electronic communications service*” as “*a service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on electronic communications networks, including telecommunications services and transmission services in networks used for broadcasting, but excludes services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services, as defined in Article 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks*”. The DPEC (Art. 2) applies this definition as well.

pointed out below, the DPEC tightens some of the apparent laxity of the DPD in important respects.

V.2 Scope of Data Protection Paw

Data protection laws focus specifically on regulating various stages in the processing of personal data in order to safeguard the privacy and related interests of the data subjects. A threshold question when seeking to apply such laws is whether the object of purported regulation concerns *personal* data; generally, the laws do not apply unless the data concerned can be properly classified as personal. In other words, a DRMS may be affected by the laws only insofar as it processes such data.¹⁰⁵⁹

The concept of personal data is usually given a broad and flexible legal definition. The following definition in the DPD is fairly representative:

“any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity” (Art. 2(a)).¹⁰⁶⁰

The focus of the definition on the potential of data to enable identification of a person means that “personal data” may encompass, in theory, a great deal of data with *prima facie* little direct relationship to a particular person. Concomitantly, data may be “personal” even if they allow a person to be identified only in combination with other (auxiliary) data.¹⁰⁶¹

However, certain limitations are to be read into the identifiability criterion. Most importantly, the criterion will not be met under the Directive simply by the existence of a remote and purely theoretical possibility of identification; identification must be possible by the use of methods that are “reasonably likely to be used” in the circumstances (recital 26 in the DPD preamble).¹⁰⁶² Further, data will usually not be personal if they can only be linked to a group of persons as opposed to a single (natural/physical) person.¹⁰⁶³

¹⁰⁵⁹ The ambit of data protection laws tends to be delimited according to several other criteria as well (see: Bygrave (2002b): 31, 50–56) but, with respect to DRMS, these criteria are not nearly as significant as the requirement that data be personal.

¹⁰⁶⁰ Recital 14 in the preamble to the Directive makes clear that this definition encompasses sound and image data on natural persons.

¹⁰⁶¹ See: European Commission (1992): 9.

¹⁰⁶² For detailed discussion of this and other factors relating to identifiability, see: Bygrave (2002b): 41ff.

¹⁰⁶³ The data protection laws of some jurisdictions (e.g., Italy and Switzerland) expressly cover data on organised collective entities such as corporations, partnerships and citizen initiative groups: see: Bygrave (2002b): Chapters 9–10. This notwithstanding, such data are only covered if they can be linked back to one particular entity as opposed to a group of entities. The DPEC also expressly provides some protection for the data protection interests of corporations and other legal persons in their role as “subscribers” to electronic communications services (Art. 1(2)): see: *ibid*: 208.

Nevertheless, the legal threshold for what amounts to personal data is low. Thus, many, if not most, DRMS are likely to involve the processing of such data, particularly on purchasers and browsers. It is not possible, though, to determine in the abstract precisely every type of data in a DRMS which will be regarded as personal. This is particularly the case with e-mail addresses, machine addresses (i.e., IP numbers and domain names) and “clickstream” data linked to these.¹⁰⁶⁴ However, the definition of personal data in the DPD is certainly broad enough to embrace such data. Moreover, the DPEC seems to be built on an assumption that at least some such data may be personal (see especially preamble, recitals 24–25).¹⁰⁶⁵ If there exists, for example, a readily accessible directory listing one particular person against one particular address, the latter — along with clickstream data linked to it — are likely to be personal data.¹⁰⁶⁶ The opposite result will pertain if numerous persons are registered against that address. However, the mere possibility of multiple persons sharing a machine with an address registered in the name of only one person is unlikely to disqualify that machine address from being treated as personal data.¹⁰⁶⁷

The extent to which the DPD and similar legislation may cover processing of e-mail addresses, machine addresses and attached clickstream data is not the only point of uncertainty regarding the ambit of data protection laws in a digital context. A closely related point of uncertainty concerns the extent to which these laws may sensibly apply to the operations 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. This issue will be of increasing significance as DRMS are likely to involve more and more use of various types of such agents. The issue is only just beginning to be systematically considered.¹⁰⁶⁸

V.3 Regulation of Data Processing

Responsibility for Compliance

Primary responsibility for observing the rules laid down in data protection laws is placed on those actors that control the means and purposes of the processing of data on other persons. These actors are commonly termed “controllers” or “data controllers”. The DPD defines a “controller” as the “natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data” (Art. 2(d)).

¹⁰⁶⁴ By “clickstream” data is meant information on, *inter alia*, which type of computer, operative system and browser program are used, along with lists of visited websites and keywords typed into search-programs. See: Greenleaf (1996a): 91–92; Kang (1998): 1225ff.

¹⁰⁶⁵ Note that the DPEC adopts the same definition of “personal data” as the DPD (DPEC Art. 2).

¹⁰⁶⁶ See: Greenleaf (1996b): 114–115.

¹⁰⁶⁷ See: Bygrave (2002b): 316–318.

¹⁰⁶⁸ For a preliminary analysis, see: Bygrave (2001).

It is important to note that this definition envisages the possibility of there being more than one controller per data-processing operation (i.e., control can be shared). Secondly, a controller need not be in possession of the personal data concerned.¹⁰⁶⁹ Thirdly, who is controller can change from one data-processing operation to another, even within one information system.¹⁰⁷⁰ Fourthly, what is decisive for determining who is controller is not the formal allocation of control responsibilities as set down in, say, contractual provisions, but the *factual* exercise of control.

A controller is to be distinguished from what the DPD terms a “processor” — i.e., a person or organisation engaged in processing personal data “on behalf of” a data controller (Art. 2(e)). Controllers must ensure, through appropriate contractual or other arrangements, that processors carry out their tasks in accordance with the laws that are enacted pursuant to the DPD (Art. 17(2)–(3); see also Art. 16). Liability for a processor’s non-compliance with these laws is put on the shoulders of the controllers (Art. 23(1)).

Accordingly, for the purposes of DRMS operations, it is most crucial to work out which system operators are controllers as opposed to processors. The result of such classification will obviously vary from one system to another, depending on the internal allocation of responsibilities in each. In the following, it is assumed that each system will be run by at least one operator that functions as a controller with respect to the processing of personal data on purchasers and/or browsers.

Core Data Protection Principles¹⁰⁷¹

The application of data protection law to a DRMS means that the system operator(s) — whether controller(s) or processor(s) — must process personal data according to rules that, in sum, manifest an overarching principle that personal data should be processed both *fairly* and *lawfully* (see especially DPD, Art. 6(1)(a)). This principle is manifest, in turn, in rules giving effect to a multiplicity of other principles. In terms of the DPD, the most important of these principles are the following:

¹⁰⁶⁹ See also: Terwangne, Louveaux (1997): 236.

¹⁰⁷⁰ In the context of an electronic communications network, recital 47 in the preamble to the DPD indicates that the person or organisation providing the transmission services (e.g., an ISP) is normally not to be regarded as the controller of personal data contained in a transmitted message; the controller will instead be the person or organisation “*from whom the message originates*”. However, transmission service providers “*will normally be considered controllers in respect of the processing of the additional personal data necessary for the service*”. Such service providers will have to comply with the rules in the DPEC as well as those of the DPD.

¹⁰⁷¹ By “principle” is primarily meant a normative proposition denoting the pith and basic thrust of a set of legal rules. At the same time, these principles have a regulatory force of their own: many of them are incorporated in the DPD and other regulatory instruments as legally binding rules in their own right or as guiding standards that may be applied (by, e.g., data protection authorities) in case-specific interest-balancing processes.

- (i) fair collection principle — personal data should be collected by fair and lawful means (see especially Art. 6(1)(a));
- (ii) minimality principle — the amount of personal data collected should be limited to what is necessary to achieve the purpose(s) for which the data are collected and further processed (see especially Arts. 6(1)(c), 6(1)(e), 7–8);
- (iii) purpose specification principle — personal data should be gathered for specified and legitimate purposes and not processed in ways that are incompatible with those purposes (Art. 6(1)(b));
- (iv) disclosure limitation principle — disclosure of personal data to third parties should occur only with the consent of the data subject or with legal authority (see, e.g., Art. 7(a));
- (v) data quality principle — personal data should be accurate, complete and relevant in relation to the purposes for which they are processed (see especially Art. 6(1)(d));
- (vi) security principle — security measures should be implemented to protect personal data from unintended or unauthorised disclosure, destruction or modification (Art. 17);
- (vii) principle of data subject participation and control — data subjects should be able to participate in, and exercise a measure of control over, the processing of data on them by others (see, e.g., Arts. 7(a), 8(2)(a), 10–12, 14(b));
- (viii) accountability principle — parties responsible for processing data on other persons should be accountable for complying with the above principles (see especially Art. 23).

Three other principles are worth noting too. Each of them can be seen as an elaboration of the above-listed principles. The first is that persons should be given the opportunity to remain anonymous when entering into transactions with others (see especially DPD, Art. 6(1)(e) and (c), together with Arts. 7–8). The second is that persons should be informed of, and given access to, data on them held by others, and be able to rectify these data if inaccurate or misleading (DPD, Arts. 10–12). The third is that fully automated evaluations of a person's character should not be used to reach decisions that significantly impinge upon the person's interests (DPD, Art. 15). The first of these three principles is implicit in the minimality principle, while the latter two are implicit in the principle of data subject participation and control. And, of course, all three are implicit in the overarching principle of fair and lawful processing.

The scope of the latter principle — particularly the fairness criterion in DPD Art. 6(1)(a) — probably extends beyond what is stipulated in the other provisions of the Directive; were this not the case, the Directive's reference to the criterion would be redundant. At the same time, the full scope of the criterion cannot be defined in the abstract. Yet there can be little doubt that a central element of it is a requirement that data controllers respect and therefore take into account the reasonable expectations of the data subjects. This requirement generates in

turn other requirements not all of which are obviously present in the DPD or other data protection laws.¹⁰⁷²

Basic Conditions for Data Processing

The DPD prohibits the collection and further processing of personal data unless the processing satisfies one or more specified conditions. Article 7 lays down the alternative conditions for the processing of personal data generally. These conditions are, in summary:

- (a) the data subject “unambiguously” consents to the processing;
- (b) the processing is “necessary” for the “performance” or conclusion of a contract with the data subject;
- (c) the processing is “necessary” for compliance with a “legal obligation” on the data controller;
- (d) the processing is “necessary” for protecting the “vital interests” of the data subject;
- (e) the processing is “necessary” for performing a task executed in the “public interest” or in exercise of official authority; or
- (f) the processing is “necessary” for the pursuance of “legitimate interests” that override the conflicting interests of the data subject.

Of these conditions, paras. (a), (b), (c) and (f) are most pertinent to the operation of a DRMS. Regarding para. (a), this must be read in light of Art. 2(h), which defines “the data subject’s consent” 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”. From this definition, it appears that consent need not be in writing. However, the express registration of consent on paper or electronic medium will aid in fulfilling the requirement in Art. 7(a) that consent be “unambiguous”.¹⁰⁷³ Arguably, the latter requirement will be met even if consent is not explicit (see below), but the data subject’s actions must leave no doubt that he/she has given consent.

In the context of a DRMS, the simple fact that a purchaser takes the initiative to enter into a transaction with a system operator could be seen as a manifestation of consent to the operator’s registration of at least some data on the purchaser. However, this consent will only extend to the registration practices which the purchaser could reasonably expect or about which the purchaser is notified by the operator. Given the concern of the DPD to ensure that data processing is carried out in a manner that is *fair* to the interests of data subjects, notification of the purchaser will have to be done in such a way as to help ensure such fairness. Thus, notification will arguably need to occur *prior* to the purchase transaction taking place (i.e., during the browsing phase), and it will need to involve *active* steps on the part of the operator (i.e., through the latter creating

¹⁰⁷² For elaboration of some such requirements, see Bygrave (2002b): 58–59, 335–336.

¹⁰⁷³ Cf. recital 17 in the preamble to the DPEC (“Consent may be given by any appropriate method enabling a freely given specific and informed indication of the user’s wishes, including by ticking a box when visiting an Internet website”).

screen-icons that can reasonably be said to catch the attention of potential purchasers).¹⁰⁷⁴ The same considerations apply with respect to browsers.

However, the registration of the fact that a person accesses the server of a DRMS — without the person necessarily going on to browse through the server's various pages — is not justifiable under para. (a) if the person is not given an opportunity to consent to that registration. Hence, if a server operates with a mechanism for automatically creating and setting cookies at the time the server is first accessed, and assuming the cookies constitute personal data (see *Scope of data protection law* in this section above), the mechanism will fall outside the bounds of para. (a). Indeed, in the context of DRMS operations, it is hard to see that such a cookies mechanism will meet any of the other conditions in Art. 7, except possibly those laid down in paras. (b) and (f).

The condition set out in Art. 7(b) will often be met with respect to the processing of purchaser-related data in the context of a DRMS given that there will exist a contract between the purchaser and a system operator. The condition may also be satisfied with respect to the processing of browser-related data insofar as the processing is “in order to take steps at the request of the data subject prior to entering into a contract” (Art. 7(b)). The main point of concern is to determine which data processing is “necessary” in both cases.

The necessity criterion should be read as embracing two overlapping requirements: (1) that the processing corresponds to a pressing social or commercial need; and (2) that the processing is proportionate to the aim of the contract.¹⁰⁷⁵ The stringency of these requirements will vary from case to case in accordance with the kind of data processing involved. In other words, exactly which types of data processing will meet the requirements is a question of fact that cannot be answered conclusively in the abstract. The requirements will be clearly met, though, if the relevant system operator registers only those data as are necessary for enforcing the terms of a contract entered into with a purchaser. Such data would probably include the purchaser's name and address, the name and price of the purchased product, together with the date of purchase. It is also clear that the condition in para. (b) will not be met with respect to a data subject who is purely browsing. The condition will only be relevant once the data subject actively requests the system operator to prepare for an imminent purchase transaction.

Less clear is the extent to which para. (b) can properly be used to justify the monitoring of purchasers' private activities *after* a contract is entered into, with the aim of checking compliance with the contract.¹⁰⁷⁶ There can be little doubt that monitoring in pursuit of such an aim may be linked to the notion of contrac-

¹⁰⁷⁴ See also: Terwangne, Louveaux (1997): 239, 241.

¹⁰⁷⁵ Cf. Art. 6(1)(c) of the Directive (personal data must be “not excessive” in relation to the purposes for which they are processed). The term “necessary” in Art. 8(2) of the ECHR is interpreted along similar lines: see, e.g., *Leander v. Sweden* (1987) *Series A of the Publications of the European Court of Human Rights*, No. 116, para. 58.

¹⁰⁷⁶ Cf. the “IP, phone home” function of DRMS described in section IV above.

tual “performance”, but this does not mean that all such monitoring will fulfil the test of proportionality inherent in the necessity criterion. The monitoring could capture in its net a range of personal data that are not strictly required for compliance purposes.

The condition set down in Art. 7(c) could be relevant insofar as the controller has legal obligations towards other DRMS actors. However, solid grounds exist for narrowly construing the term “legal obligation” such that it does not cover purely contractual obligations. Were the term not construed in this way, para. (c) could be used by data controllers to create at will a legal competence to process personal data simply by writing up a contract (to which the data subject is not party). A narrow reading is also supported by the existence and wording of para. (b).¹⁰⁷⁷

If an appropriate legal obligation is found to exist between DRMS actors, a question of fact will again arise as to what data are necessary to process in order to comply with the obligation. The necessity criterion here will be the same as in relation to para. (b) — along with paras. (d), (e) and (f). It is doubtful that the criterion will be met in the case of registration and further processing of data relating to persons who only browse. Hence, the use of cookies mechanisms to register such data will fall outside the scope of para (c).

The condition laid out in para. (f) is perhaps the most flexible and open-ended of the conditions in Art. 7. The Directive provides little useful guidance on how the various interests in para. (f) are to be balanced. Who, for example, is intended to undertake the interest balancing? Recital 30 in the preamble states that, in balancing the various interests, Member States are to guarantee “effective competition”; Member States may also determine conditions for use of personal data “in the context of the legitimate ordinary business activities of companies and other bodies”, and for disclosure of data to third parties for marketing purposes. Otherwise, the Directive leaves it up to the Member States to determine how the interests are to be balanced.

An interesting issue in relation to para. (f) is the extent to which it may justify the use of cookies mechanisms involving non-consensual registration of the fact that a person has accessed the server of a DRMS. The issue is, of course, only pertinent insofar as the data registered (e.g., the address of the visitor’s machine) can properly be viewed as “personal” pursuant to DPD Art. 2(a). As noted above in *Scope of data protection law*, the Directive on privacy and electronic communications seems to be built on the assumption that cookies may contain personal data (see especially recital 25 in the DPEC preamble). Cookies mechanisms may serve the legitimate interests of DRMS operators (see again recital 25 in the DPEC preamble which notes that cookies can be a “legitimate and useful tool” for facilitating, *inter alia*, the “provision of information society services”). However, it is difficult to see how cookies can be deemed “necessary”

¹⁰⁷⁷ Note that Art. 7(c) in an earlier proposal for the Directive referred to an “obligation imposed by national law or by Community law”. See: European Commission (1992): 17, 72.

for satisfying such interests, though admittedly the propriety of such an assessment all depends on how the interests are defined and on exactly what data are registered. If the interests are defined in terms of achieving “best possible conditions for product marketing”, the use of cookies mechanisms might be seen as necessary, even if those mechanisms only generate relatively coarse-grained data about consumer preferences. Yet even if such mechanisms are found necessary, they may well be “trumped” by the data subjects’ interests in privacy, integrity and autonomy. The strength of these interests will increase in tact with the increase in detail and sensitivity of the data generated by the cookies mechanisms.

It is additionally noteworthy that the DPEC permits the employment of cookies mechanisms only for “legitimate” purposes and on the basis that data subjects be notified of, and given the opportunity to refuse, their usage (Art. 5(3); see also preamble, recital 25). However, actual consent of data subjects is not a necessary condition for applying cookies: “access to specific website content may still be made conditional on the well-informed acceptance of a cookie or similar device, if it is used for a legitimate purpose” (preamble, recital 25). At the same time, the DPEC fails to clearly specify *when* data subjects are to be notified of cookie usage.¹⁰⁷⁸ In the interests of privacy, the point of departure should normally be that notification shall occur *before* a cookie is stored on the data subject’s computer. Yet, if what the Directive is most concerned about here is to give data subjects an opportunity to refuse cookie storage — notification being merely a means to that end — it could be strongly argued that notification may occur *after* cookie storage since data subjects themselves can easily remove the cookies pursuant to notification.¹⁰⁷⁹

To sum up so far, the four main processing conditions discussed above should, in combination, enable the registration and further processing of certain types of purchaser-related data by DRMS operators. They may also allow for the registration and further processing of certain types of browser-related data, though to a much lesser extent than in the case of data on purchasers.

Sensitive Data

The stringency of the conditions for data processing is increased in some respects for certain classes of data which are deemed to be especially sensitive (see Art. 8). Such data embrace information on a person’s “*racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and [...] health or sex life*” (Art. 8(1)).¹⁰⁸⁰ Determining which data come within these categories will not always be easy, partly because of the vague way in which the

¹⁰⁷⁸ The same omission occurs with respect to DPD Art. 10 (cf. Art. 11) which requires data controllers to inform data subjects about basic details of their processing operations when the data are collected from the data subjects directly. It has been argued that the information must be provided before or at the time of the data collection, see: Bygrave (2002b): 352.

¹⁰⁷⁹ On deletion of cookies, see, e.g., D. Whalen’s “Unofficial Cookie FAQ”, version 2.6, at: <http://www.cookiecentral.com/faq/#2.2>.

categories are formulated and partly because the determination of sensitivity tends to be coloured by context.

A DRMS might involve the processing of some of the above types of data inasmuch as certain personal preferences of purchasers and/or browsers are registered by a system operator. If, for instance, a purchaser enters into a contractual transaction for the use of an information product concerning a particular religious or sexual theme, and the product is registered against the purchaser's name (or pseudonym or other unique identifier), it could be argued that sensitive data about the purchaser have thereby been processed. Yet it could also be contended that the connection between the product's theme and the purchaser's personality in such a case is too remote: i.e., just because a person buys usage rights with respect to a particular product does not necessarily mean that the product reflects the person's own taste; he/she may simply be sampling or analysing a range of different products. The strength of this contention will depend on several factors, including the nature of the product (e.g., an academic treatise on sadomasochism will tend to say less about the purchaser's personal sexual inclinations than, say, a video-clip depicting sadomasochistic rituals for the purpose of viewer enthrallment) and the nature of the transaction (e.g., a one-off transaction will also tend to say less about the purchaser's personal preferences than a series of transactions involving information products that focus on a similar theme). The same sort of analysis will apply with respect to registration of products in which a particular browser shows interest.

Article 8 of the Directive opens with a prohibition on the processing of the above categories of data, but follows up with a list (in Art. 8(2)) of alternative exemptions to this prohibition. In the context of DRMS operations, the relevant exemptions are found in Art. 8(2)(a) — i.e., processing may occur if the data subject explicitly consents to it (except where national laws override this condition) — and Art. 8(2)(e) — i.e., processing may occur if the data in question “are manifestly made public” by the data subject, or their processing is “necessary for the establishment, exercise or defence of legal claims.”

Regarding the first-mentioned exemption, consent must be “explicit”.¹⁰⁸¹ Hence, the process of requesting and providing consent must occur as a formally separate process to the actual purchase transaction. There must be a specific request by the system operator for permission from the purchaser/browser to process the data in question, followed by a specific reply in the affirmative. Arguably too, there must be some sort of record made of the request and reply, with measures in place to keep the record secure from unauthorised access and modification.

¹⁰⁸⁰ Data on “offences, criminal convictions or security measures” are also afforded extra protection under Art. 8(5), though these are less relevant in the context of DRMS. There is some debate about whether the list of data categories in Art. 8(1) is exhaustive or not. The preferred view is that the list is exhaustive, though the loose way in which the categories are formulated makes it possible to interpret them broadly. See: Bygrave (2002b): 344.

¹⁰⁸¹ Cf. the more lenient criterion of non-ambiguity in Art. 7(a).

As for the second-mentioned exemption in Art. 8(2)(e), one issue concerns the meaning of “manifestly made public”. Given the nature of the data involved, the phrase should arguably be interpreted fairly narrowly as indicating an *obvious and conscious readiness* by the data subject to make the data available to *any* member of the general public. The extent to which this condition will be satisfied in the context of a DRMS will depend on the data subject’s understanding of the operational parameters of the particular system. If the data subject believes that the system operates as a closed system *vis-à-vis* other systems (i.e., that the system operators observe strict rules of confidentiality when handling purchaser-/browser-related data), it is difficult to see the condition being satisfied.¹⁰⁸²

Another issue in relation to Art. 8(2)(e) concerns the meaning of “legal claims”. Again, it is strongly arguable that the phrase is not intended to cover claims arising from purely contractual obligations, for the same reasons as are given above with respect to Art. 7(c). Indeed, the sensitive nature of the data involved is an extra ground for reading the phrase in this way. Nevertheless, it is quite possible that national legislation implementing the Directive will allow for data processing in order for a data controller to defend a legal claim in the form of copyright, as the latter is statutorily anchored. Another issue, though, will be the extent to which such processing is “necessary” (as defined above) for the defence of such a legal claim. Here, the necessity criterion should be interpreted strictly since the data in question are regarded as especially sensitive. Thus, “necessary” should be held as denoting a stringent standard of *indispensability*. For instance, while initial registration of such data might be found indispensable for ensuring that copyright is not breached, it will be incumbent on the data controller concerned to delete or anonymise the data once the relevant interests of the copyright holder can be safeguarded in some other way.

Anonymity and PETs

As a general rule, personal data shall be anonymised once the need for person-identification lapses — i.e., 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” (DPD, Art. 6(1)(e)). This rule should be read in conjunction with the necessity criterion in Arts. 7–8 and the stipulation in Art. 6(1)(c) that personal data be “not excessive” in relation to the purposes for which they are processed. Read together, these rules arguably embody a general principle requiring, as a point of departure, that data-processing systems allow persons to enter into transactions anonymously unless there are overriding legitimate interests to the contrary. It could also be argued, albeit more tenuously, that the rules require active consid-

¹⁰⁸² It is even difficult to see the condition being satisfied in relation to non-virtual shopping: while the purchase of, say, a book in a non-virtual shop will typically be a public act in the sense that any member of the public can incidentally witness the transaction, the purchaser will rarely intend a record of that transaction to be made available (in non-anonymous format) to any member of the public.

eration to be given to developing *technological* tools for ensuring transactional anonymity or, where anonymity is not legally permitted, for ensuring that persons are able to enter into transactions using pseudonyms.¹⁰⁸³

Such tools typically go under the name of “privacy-enhancing technologies” (or “PET’s”). They consist of technical (and, to some extent, organisational) mechanisms that are developed with the aim of reducing or eliminating the collection and further processing of personal data.¹⁰⁸⁴ The DPD provides little *direct* encouragement of PET usage. The closest it comes to expressly mandating such usage is in Art. 17, along with recital 46 of the preamble, yet these provisions are concerned *prima facie* with security measures (i.e., protecting personal data against accidental or unlawful destruction, loss, modification and disclosure) rather than privacy protection more generally.

By contrast, the DPEC is more direct and active in its encouragement of transactional anonymity and thereby of PET usage to facilitate such anonymity.¹⁰⁸⁵ In particular, it states that “[s]ystems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum [...]” (preamble, recital 30; see also more generally Art. 6). As indicated above, a similar stipulation can probably be read into the DPD.

Purpose Specification

Another set of rules with the potential to significantly affect DRMS are those expressing the principle of purpose specification (sometimes also termed the finality principle). The principle is expressed most directly in DPD Art. 6(1)(b) which requires personal data to be “collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes”. In a DRMS context, this requirement has obvious repercussions for the secondary uses to which system operators will be able to put purchaser-/browser-related data.

The principle in Art. 6(1)(b) is grounded partly in concern for ensuring that data are processed in ways that conform with data subjects’ reasonable expectations. It is additionally grounded in concern for ensuring that data are used for purposes to which they are suited (i.e., a concern for adequate information quality).

From the wording of Art. 6(1)(b), it is apparent that the purposes for which the operator of a DRMS registers data on a purchaser or browser must be defined, documented and announced in advance of registration.¹⁰⁸⁶ The purposes must

¹⁰⁸³ Further on the interrelationship of anonymity and pseudonymity, along with their respective significance for privacy/data protection, see: Rossnagel, Scholz (2000); Clarke (1996).

¹⁰⁸⁴ See, e.g.: Burkert (1997).

¹⁰⁸⁵ German legislation is also explicit on this point: see particularly § 3a of the 1990 Federal Data Protection Act (*Bundesdatenschutzgesetz*), as amended in May 2001. See also §§ 4(4), 4(6) and 6(3) of the 1997 Federal Teleservices Data Protection Act (*Teledienstschutzgesetz*), as amended in December 2001.

¹⁰⁸⁶ See: European Commission (1992): 15.

also be notified to the data subject (see also DPD Arts. 10 and 11). Further, they must be “legitimate”. Arguably, the term “legitimate” denotes a criterion of social acceptability which is broader than that of lawfulness, though it is difficult to determine how much broader.¹⁰⁸⁷ The conditions laid down in Arts. 7–8 (see subsections *Basic conditions for data processing* and *Sensitive data* in section V above) provide some, but not exhaustive, guidance on the ambit of the legitimacy criterion. At the same time, a DRMS operator cannot define the purposes of data processing in the same broad and diffuse terms as are found in Arts. 7–8: use of the adjective “specified” in Art. 6(1)(b) indicates that the purposes need to be delineated more concretely and narrowly.¹⁰⁸⁸ Moreover, the legitimacy criterion arguably requires that the specified purposes have (objectively) more than a marginal connection with the operator’s ordinary field of activity.¹⁰⁸⁹ This notwithstanding, the vast majority of DRMS will probably be able to meet the legitimacy criterion fairly easily. Other criteria, particularly those of necessity (dealt with in the preceding sections) and compatibility (see immediately below) will probably tend to pose greater difficulties for system operators.

In terms of the compatibility criterion, if we accept that one of the underlying concerns of Art. 6(1)(b) is to ensure that data are processed in conformity with data subjects’ reasonable expectations, any secondary purpose should not pass the test of compatibility/non-incompatibility unless the data subject is (objectively) able to read that purpose into the purpose(s) first specified, or the secondary purpose is otherwise within the ambit of the data subject’s reasonable expectations.¹⁰⁹⁰ It is doubtful, for example, that a DRMS operator who/which has specified billing as the primary purpose for collecting purchaser data, would satisfy this test if the data were subsequently used for marketing (either by the operator or by others to which the operator has passed the data). In such a case, the “re-purposing” of the data would most probably require prior consent from the data subject.¹⁰⁹¹

The DPEC appears to embrace a fairly stringent version of the purpose specification principle in the relations between communications service providers and service users/subscribers. Traffic data on users/subscribers may only be used for the purpose of marketing the provider’s own services if the subscriber has consented (Art. 6(3)). Otherwise, such data must be erased or made anonymous when no longer needed for purposes of communication transmission, billing or interconnection payments (Arts. 6(1) and 6(2)).

¹⁰⁸⁷ See: Bygrave (2002b): 338–339.

¹⁰⁸⁸ See: European Commission (1992): 15.

¹⁰⁸⁹ Norway’s Personal Data Act 2000 (*lov om behandling av personopplysninger av 14. april 2000 nr. 31*) seems to adopt a similar line when it stipulates that personal data shall be “*used only for explicitly stated purposes that are objectively justified with respect to the activities of the controller*” (“*bare nyttes til uttrykkelig angitte formål som er saklig begrunnet i den behandlingsansvarliges virksomhet*”: § 11(1)(b)).

¹⁰⁹⁰ See: Bygrave (2002b): 340.

¹⁰⁹¹ See: Bygrave (2002b): 335–341 and case references cited therein.

Other Provisions

The rules canvassed in the above sections are likely to have the greatest impact on the running of DRMS. However, numerous other rules in data protection legislation are also likely to have some effect in shaping DRMS operations. These rules deal specifically with, *inter alia*, fully automated profiling practices (DPD, Art. 15),¹⁰⁹² information access rights (DPD, Arts. 10–12),¹⁰⁹³ and the flow of personal data from EU Member States to countries outside the EU (DPD, Arts. 25–26).¹⁰⁹⁴

Moreover, these and many of the rules canvassed in the above sections may be subjected to derogations. For instance, the DPD gives EU Member States the opportunity of adopting legislative measures that derogate from the provisions in, e.g., Arts. 6(1) and 10–12 if it is necessary to safeguard, *inter alia*, “the prevention, investigation, detection and prosecution of criminal offences [...]” (Art. 13(1)(d)), or “the protection of the [...] rights and freedom of others” (Art. 13(1)(f)). Both exemptions are relevant to DRMS and could be used by copyright holders or their representative organisations as leverage points for pressuring Member States into drafting data protection laws that are more “DRMS-friendly” than, say, Arts. 6(1) and 10–12 would *prima facie* allow.

Another such leverage point could be Art. 9 which requires Member States to derogate from the bulk of the Directive’s provisions, with regard to “processing of personal data carried out solely for . . . the purpose of artistic or literary expression” though only if the derogations are “necessary to reconcile the right to privacy with the rules governing freedom of expression”. Of course, Art. 9 is only relevant for DRMS insofar as the basic rationale of such systems can properly be characterised as the promotion of freedom of artistic or literary expression — a debatable point!

VI The Copyright Directive

As intimated in section II above, the impact of DRMS on privacy and related interests is legally regulated not simply by data protection instruments; intellectual property rules play a considerable role too. The most significant of the latter rules in terms of EC law are those contained in Arts. 6–7 of the Directive on copyright of 2001 (hereinafter also “CD”).¹⁰⁹⁵ These provisions afford support for many of the technologies upon which DRMS are based. Article 6

¹⁰⁹² See: Bygrave (2002b): 319–328.

¹⁰⁹³ See: Bygrave (2002b): 352–354; Bygrave, Koelman (2000): 87–88.

¹⁰⁹⁴ See: Bygrave, Koelman (2000): 89–93.

¹⁰⁹⁵ See: Directive 2001/29/EC of the European Parliament and of the Council of 22nd May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (OJ L 167, 22nd June 2001, 10 et seq.). Articles 6–7 build upon and are intended to implement Arts. 11–12 of the World Intellectual Property Organization (WIPO) Copyright Treaty of 1996 (hereinafter “WCT”). See too the mirroring provisions in Arts. 18–19 of the WIPO Performances and Phonograms Treaty of 1996.

stipulates, in summary, that adequate legal protection shall be provided against the intentional circumvention of any effective “technological measures” for protecting intellectual property.¹⁰⁹⁶ Article 7 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 copyright works from which such information has been removed or altered, in the knowledge that such distribution breaches copyright or related rights.

Both of these provisions are complex and raise numerous issues of interpretation.¹⁰⁹⁷ The following analysis is concerned only with their potential impact on privacy and related interests. More particularly, it focuses on the extent to which these provisions (and the Directive more generally) permit the circumvention of devices (including “technological measures” as defined in Art. 6) which monitor end-users’ reading, listening, viewing or browsing habits. Expressed alternatively, when (if at all) may an end-user take steps to prevent the operation of such devices? Arriving at an answer here involves addressing two questions:

- (i) does prevention breach Art. 6 or 7?
- (ii) if a breach occurs, is it nevertheless permitted under the DPD (or DPEC)?

The relationship between the CD on the one hand and the DPD and DPEC on the other, is complex and difficult to fully delineate in the abstract. How these instruments shall intersect in practice depends largely on how they are transposed in national laws, and in each case EU Member States are given a fairly broad margin of appreciation when carrying out transposition. Importantly, the CD states that its provisions shall be “without prejudice” to legal provisions in other areas, including “data protection and privacy” (Art. 9). Hence, the provisions of the CD do not necessarily trump those of the DPD or DPEC. Yet, as indicated in section V, the latter instruments will not necessarily permit privacy and related interests to prevail over conflicting interests of DRMS operators.

The Meaning of “Technological Measures”

In terms of the potential impact of CD Art. 6 on privacy and related interests, an important issue is whether the concept of “technological measures” extends to devices that *monitor* usage of copyright works. If such devices are not covered, their disablement will not constitute a breach of Art. 6(1). If such devices are covered, their disablement will, *prima facie*, violate Art. 6(1), though the violation could perhaps be justified pursuant to data protection law.

¹⁰⁹⁶ Note that Art. 6 does not apply to computer software, protection for which is to be derived primarily from Directive 91/250/EEC of 14th May 1991 on the legal protection of computer programs (see CD, preamble, recital 50; cf. recital 60 and Art. 9).

¹⁰⁹⁷ For analysis of some of these issues, see: Koelman (2000); Koelman, Helberger (2000): 169 et seq; Kroon (2000): 250 et seq; Hart (2002): 61–63; Retzer (2002); Huppertz (2002); Fallenböck (2002/2003). For analysis of the equivalent issues under Australian and Hong Kong copyright law, see: Greenleaf (2002): 52 et seq.

The CD itself provides no obvious answer to the issue.¹⁰⁹⁸ However, there can be little doubt that some monitoring devices may be covered in light of the broad definition of “technological measures” — i.e., “*any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject matter, which are not authorised by the rightholder of any copyright [or related rights] [...]*” (Art. 6(3)). Potentially augmenting the breadth of this definition is the apparent lack of a requirement that the measure concerned be inextricably linked with protection of copyright (or a related right).¹⁰⁹⁹ On its face, the definition focuses on the prevention or restriction of acts that a rightholder (as opposed to copyright law) has not authorised.¹¹⁰⁰ The extent of authorisation could vary with the whim of each rightholder. Authorisation could cover more than reproduction and dissemination of copyright works; mere access (on an individualised basis) to such works (or possibly other information products) might also be subject to authorisation. This possibility is clearly brought out in subsequent provisions of Art. 6(3) which, in the course of defining when technological measures are deemed “effective”,¹¹⁰¹ refer to “*application of an access control [...] process*” as one way of achieving control of protected subject-matter.

At the same time, the requirement that a technological measure be concerned with prevention/restriction of unauthorised acts in the *normal* course of its operation, most probably means that monitoring devices which are only incidentally concerned with such protection fail to qualify as technological measures.

¹⁰⁹⁸ The same can be said with respect to WCT Art. 11 upon which CD Art. 6 is based. Cf. § 1201 of the US Copyright Act introduced by the Digital Millennium Copyright Act 1998 (Public Law No. 105–304 (1998), codified at US Code, Title 17, §§ 1201–1205). This permits the disablement of monitoring mechanisms tied to access controls, if several cumulative conditions are met (see § 1201(i)). These conditions are, in summary, that: (1) the access controls, in the normal course of operation, collect or disseminate “*personally identifying information*” about the online activities of a person who seeks access to the protected work; (2) conspicuous notice about this information processing is not given; (3) the data subject is not provided the capability to prevent the information being gathered or disseminated; (4) circumvention of the controls has the sole effect, and is solely for the purpose, of preventing the collection or dissemination; and (5) circumvention does not breach another law. These provisions seem 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 their application to other monitoring devices that are more integral to copyright-protective technologies; see: Samuelsen (1999): 553 et seq. The practical utility of the provisions is also questionable given that § 1201(a)(2) and (b)(1) restricts the supply of tools that could disable such access controls.

¹⁰⁹⁹ For further discussion of the extent to which technological measures must be connected with copyright protection, see: Fallenböck (2002/2003): section VII(D); Koelman (2000). For parallel discussion with respect to Australian and Hong Kong law, see Greenleaf (2002): 58 et seq.

¹¹⁰⁰ Cf. WCT Art. 11 which refers to acts “which are not authorized by the authors concerned *or permitted by law*” (emphasis added).

¹¹⁰¹ Article 6 applies only to “effective” technological measures.

One might also query whether devices that *merely* carry out monitoring tasks (albeit with protection of intellectual property as the primary purpose) can properly be viewed as “designed to prevent or restrict” unauthorised acts. Pertinent examples here would be devices for the generation and placement of cookies, web bugs and/or web spiders. On the one hand, it could be argued that monitoring *per se* can have the requisite preventative or restrictive function, particularly in light of the increasingly self-evident control dynamics that are central to panopticism.¹¹⁰² Since monitoring facilitates detection of unauthorised actions, it acts as a deterrent for such behaviour, thereby restricting (inhibiting) the behaviour if not, at least in some instances, preventing (stopping) it outright. Part of the argument is that “restrict” is intended to denote a less stringent form of control than “prevent”; if the former term were not so intended, it would risk being made logically redundant by the latter term. The argument as a whole has much to commend it.

On the other hand, the argument is possibly undermined by the requirement that a technological measure be “effective” — i.e., that the measure “achieves the protection objective” (Art. 6(3)). This objective is formulated as a form of “control”. Hence, the issue here turns partly on how “control” is supposed to be understood. That term is not directly defined in the Directive. On its own, “control” is sufficiently flexible to cover the process of behavioural modification described in the preceding paragraph (i.e., detection → deterrence → inhibition). However, the effectiveness requirement could be read as indicating that the control is intended to be relatively concrete, tangible and certain; concomitantly, that the control has an obvious mechanical immediacy in the sense that it must be circumvented before unauthorised use of the protected subject matter is possible. On this view, the control dynamics of monitoring may be deemed as too nebulous and inconsequential to meet the effectiveness requirement. By way of analogy, a contrast can be drawn between the control effect of mounting a video surveillance camera over the unlocked entrance to a house, and the equivalent effect of placing a padlock on the door (and other possible entry points). In the situation where only a camera is used, a would-be intruder could physically enter the house despite the camera (even though the latter may deter such intrusion); in this sense, the camera is not “effective”. In the other situation, a would-be intruder could not physically enter the house unless he/she picked, cut or otherwise disabled the locking device; in this sense, the device is “effective” and thereby analogous to a technological measure as envisaged under Art. 6.¹¹⁰³ The plausibility of this view is strengthened by the fact that it does not render superfluous use of the term “restrict” alongside the term “prevent”. The former term may denote some sort of impediment to accessing or copying which falls short of completely stopping (i.e., preventing) these processes yet which goes beyond merely discouraging them. An example here would be a device that permits access to some but not all of a particular digital product.

¹¹⁰² See: Lyon (1994); Gandy (1993).

¹¹⁰³ Obviously, the fact that the device could be disabled, would not mean that it fails the effectiveness requirement; Art. 6 is predicated on the very possibility of such devices being disabled or otherwise circumvented.

Much the same line of interpretation has been taken in a recent decision by a single judge of the Federal Court of Australia in a case dealing with the meaning of “technological protection measure” under Australia’s federal Copyright Act 1968 (as amended).¹¹⁰⁴ According to Justice Sackville,

“[t]he definition [of “technological protection measure”] [...] contemplates that but for the operation of the device or product, there would be no technological or perhaps mechanical barrier to a person gaining access to the copyright work, or making copies of the work after access has been gained [...] I do not think the definition is concerned with devices or products that do not, by their operations, prevent or curtail specific acts infringing or facilitating the infringement of copyright [...], but merely have a general deterrent or discouraging effect on those who might be contemplating infringing copyright [...]”.¹¹⁰⁵

The judge went on to consider whether this interpretation renders superfluous the term “inhibit” in the definition of “technological protection measure”. He found that the term should be given a narrow construction such that it does not cover mere deterrence or discouragement but a situation in which the extent of unlawful copying is limited as opposed to prevented completely: “A copy control mechanism, for example, might not prevent all copying that infringes copyright, but might limit the extent of unlawful copying [...] for example by reducing the quality of copies that can be made [...]”.¹¹⁰⁶ The judge noted further that while the relevant legislative history — including work on drafting the CD — is not conclusive of the issues here, it is consistent with his interpretation.¹¹⁰⁷

The decision in the case has been appealed and carries little formal weight for interpretation of Art. 6. Yet it is noteworthy given the paucity of other case law on point and given the fact that it indirectly provides considerable benefits for privacy interests.

¹¹⁰⁴ See: *Kabushiki Kaisha Sony Computer Entertainment et al. v. Eddy Stevens* [2002] FCA 906, decision of 26th July 2002 by Justice Sackville (appealed). Under the Australian legislation, a “technological protection measure” means “a device or product, or a component incorporated into a process, that is designed, in the ordinary course of its operation, to prevent or inhibit the infringement of copyright in a work or other subject matter by either or both of the following means: (a) by ensuring that access to the work or other subject-matter is available solely by use of an access code or process (including decryption, unscrambling or other transformation of the work or other subject-matter) with the authority of the owner or licensee of the copyright; (b) through a copy control mechanism” (s. 10). This definition seems to be basically the same as the equivalent definition in CD Art. 6(3). While it does not operate prima facie with an effectiveness criterion as found in Art. 6, the criterion can probably be read into it: see the judgment of Justice Sackville referred to below; see: Greenleaf (2002): 58. Moreover, there is probably little if any substantial difference between the meaning of “inhibit” (s. 10) and “restrict” (Art. 6(3)).

¹¹⁰⁵ See: paragraph 115 of judgment; see too paragraph 117.

¹¹⁰⁶ See: paragraph 116 of judgment.

¹¹⁰⁷ See: paragraph 117 of judgment.

The Scope of “Rights Management Information”

Turning to CD Art. 7, an important privacy-related issue concerns the scope of “rights management information” (RMI). More specifically, the issue is whether personal data relating to a consumer of copyright work 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, e.g., an information consumer cannot fall foul of Art. 7(1). RMI is defined in Art. 7(2) as “information provided by rightholders” including “*information about the terms and conditions of use of the [copyright] work or other subject matter*”.¹¹⁰⁸ Does information about “terms and conditions of use” necessarily include data about the identity of users of copyrighted works? Does it necessarily include personal data relating to how the works are used? On its face, the expression “terms and conditions of use” does not comfortably embrace such data.¹¹⁰⁹ This applies *a fortiori* with respect to data on actual usage. However, given that some information usage licences may be quite user-specific, it is arguable that at least data on user identity may be covered.¹¹¹⁰ A fairly clear indication that also information on actual usage of a work may be covered, is found in recital 57 in the preamble to the Directive. According to recital 57, RMI-systems could “*process personal data about the consumption patterns of protected subject-matter by individuals and allow for tracing of on-line behaviour*”.¹¹¹¹ The logic of recital 57, though, is at odds with the fact that RMI is defined as information “provided by rightholders” as opposed to end-users (Art. 7(2)) — ordinarily, data about “consumption patterns” would be provided by end-users, not rightholders. However, the logical tension between recital 57 and Art. 7(2) dissipates if the expression “provided by” is construed somewhat loosely to denote a process whereby rightholders *facilitate* the collection and further processing of the data concerned, thus providing (albeit indirectly) the data.

It could be queried whether Art. 7(1) captures the alteration or removal of RMI when these are not embedded in the copyright work or other protected subject-matter. With respect to the equivalent provisions in Australian and Hong Kong copyright legislation, Greenleaf argues that RMI will only be protected when it is stored in or with the work concerned; concomitantly, elements of RMI will not be protected once they are separated from a work in order to be transmitted

¹¹⁰⁸ The definition of RMI in WCT Art. 12(2) is similar. Note, though, the point of difference described *infra*, n. 1113.

¹¹⁰⁹ Accordingly, it has been claimed that such data appear not to be covered by the definition of RMI in the WCT; see: Bygrave, Koelman (2000): 115.

¹¹¹⁰ See also: Greenleaf (2002): 67 (in relation to definitions of RMI under Australian and Hong Kong law). Bygrave, Koelman (2000): 115 recognise this possibility too. Cf. § 1202(c) of the US Copyright Act (US Code, Title 17) which defines “*copyright management information*” (the equivalent to RMI) as excluding “*any personally identifying information about a user of a work [...]*”.

¹¹¹¹ Cf. Greenleaf (2002): 67: claiming that the definitions of RMI in both the WCT, Australian and Hong Kong legislation do not encompass information about actual usage as they refer only to “conditions” of use.

back to, say, a DRMS server as part of an ongoing monitoring process (“IP, phone home”).¹¹¹² This argument is based on the fact that the Australian and Hong Kong legislation define RMI in terms of information that is “attached” to a copy of a work.¹¹¹³ However, CD Art. 7(2) does not *prima facie* limit the scope of RMI in this way. Hence, RMI or elements thereof will probably still be protected under Art. 7 even if not embedded in or stored with a work or other protected subject-matter.

If personal data about information users are to be treated as a component of RMI — which seems most likely to be the case — the removal or alteration of such data will breach Art. 7(1) only if performed “without authority”. The requisite authority may probably be derived from legislation, particularly legislation on privacy/data protection.¹¹¹⁴ 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: as shown in section V, the answers to it will 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. It will be recalled that the DPD permits the non-consensual registration and further processing of data on consumers of copyright works if the processing is necessary for the performance of a contract or for the establishment, exercise or defence of legal claims or for realising legitimate interests that outweigh the privacy interests at stake.¹¹¹⁵ 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 preamble to the CD stipulates that “technical” privacy safeguards for such data should be incorporated in accordance with the DPD. Thus, the recital goes some way to encouraging the use of PETs. However, from a privacy perspective, recital 57 is disappointing. 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 Art. 6. This is rather incongruous as the ongoing monitoring of information usage is most likely to occur

¹¹¹² See: Greenleaf (2002): 67.

¹¹¹³ For Australia, see Copyright Act 1968, s. 10; for Hong Kong, see Copyright Ordinance 1997, s. 274(3). The latter legislation stipulates as an alternative to the criterion “attached” that the information “appears in connection with the making available of a work or fixed performance to the public”. The definition of RMI in WCT Art. 12(2) also refers only to information which is “attached to a copy of a work or appears in connection with the communication of a work to the public”.

¹¹¹⁴ See: Kroon (2000): 254. Note too CD Art. 9.

¹¹¹⁵ Recall too that more stringent conditions apply for the processing of certain categories of especially sensitive personal data (DPD Art. 8), though exactly which types of data would fall within these categories in a DRMS context is somewhat unclear: see subsection *Sensitive data* in section V.

through the application of these technological measures.¹¹¹⁶ Certainly, data protection rules and measures may still apply in the context of Art. 6 — particularly given Art. 9 — but it would have been preferable for the Directive to encourage more directly the use of PETs in that context too. Further, the recital’s reference to the DPD is problematic because, as noted in subsection *Anonymity and PETs* in section V above, that Directive fails to specifically address, let alone encourage, the use of PETs. The DPD also has very little to say specifically about the desirability of transactional anonymity or even pseudonymity (again, see subsection *Anonymity and PETs* in section V above).

VII Considerations for the Future

A considerable degree of uncertainty afflicts the debate about the implications of DRMS. 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 necessarily based to a large degree on assumptions about potentialities.

Indeed, current concerns about DRMS 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 and their business partners to satisfy these preferences.¹¹¹⁷ The take-up of privacy-invasive DRMS might also be hindered by difficulties in achieving standardisation and compatibility of technological measures.¹¹¹⁸

These uncertainties notwithstanding, future policy must aim to prevent development of DRMS from riding roughshod over privacy. The health of the “digital age” would be dealt a significant blow were the privacy and related interests of information consumers to be sacrificed through technological fiat or one-eyed lobbying on the part of copyright-holders and their business allies. It is very likely that business interests would suffer too: the recording industry (and, to a lesser extent, software industry) already faces a “crisis of legitimacy” particularly with respect to Internet-savvy youth culture. Respect for intellectual property

¹¹¹⁶ Further, as Dusollier points out, the definition of RMI in Art. 7(2) 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: Dusollier (1999): 296.

¹¹¹⁷ See: Samuelson (1999): 565–566; Hugenholtz (1999): 312 (noting previous instances of the market marginalisation of certain anti-copying devices because of their irritation to consumers).

¹¹¹⁸ There has existed a myriad of competing standards with respect to the structuring and provision of RMI. See: Gervais (1998).

rights will be easier to attain if the holders of those rights are seen to respect the privacy and autonomy of information consumers. Further, as noted in section IV, mass take-up of electronic commerce — which should clearly benefit copyright-holders and their business partners — will probably occur only if potential consumers feel that their privacy is not going to be severely compromised.

We are beginning to see some recognition of these points on the part of copyright-holders. In the USA, for example, the Business Software Alliance, Computer Systems Policy Project and RIAA have recently adopted “Technology and Record Company Policy Principles” which mention the need to develop DRMS that “*do not violate individuals’ legal rights to privacy or similar legally protected interests of individuals*” (principle 5).¹¹¹⁹

How industry embracement of such a principle will be translated into practical measures remains to be seen. It is clear, though, that if the principle is to be given proper effect, there will need to be extensive integration of technological measures for protecting intellectual property rights with PETs. Such integration will have numerous facets. One important facet will involve building mechanisms into DRMS architecture which enhance the transparency of the systems for information consumers. Another important facet will involve building mechanisms into the systems’ architecture which preserve, where possible, consumer anonymity, and which allow for pseudonymity as a fall-back option where anonymity is not feasible for legal or technical reasons.¹¹²⁰ At the same time, it may be useful to draw on the technological-organizational structures of DRMS to develop equivalent systems for privacy management.¹¹²¹

In theory, the chances of achieving integration should be increased by the fact that both DRMS and PETs are based on a similar “logical imperative”, this being control of information. Nevertheless, we should not overlook the fact that the economic interests steering many DRMS will not necessarily coincide with the privacy interests of information consumers. Neither should we forget that a large range of technological-organisational devices exist to enforce intellectual property rights in a digital environment and that some of these 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 the DPEC along with German data protection legislation, and it arguably follows, albeit more indirectly, from the DPD and Art. 8 of the ECHR.

¹¹¹⁹ The principles, adopted 14th January 2003, are set out at: http://www.bsa.org/usa/policyres/7_principles.pdf.

¹¹²⁰ See: Feigenbaum (2002). See also the recommendations in: International Working Group on Data Protection and Telecommunications (2000); Greenleaf (2002): 79–81; Information and Privacy Commissioner of Ontario (2002).

¹¹²¹ For preliminary work along these lines, see: Korba, Kenny (2002). More generally, see: Zittrain (2000).