Access to the Individual: Digital Rights Management Systems and the Intersection of Informational and Decisional Privacy Interests

PAUL GANLEY[1]

Abstract

This article examines emerging systems for protecting content under the rubric of Digital Rights Management. The potential for fine grained management of information works carries with it an unparalleled opportunity for distributors to closely monitor the reading (construed broadly) habits of individuals. The chief aim of this article is to expose how the extensive collection of personal information ('regulated' by the notion of informational privacy) combined with the possibility of personalised marketing strategies threatens individual choice and intellectual freedom (discussed by reference to conceptions of decisional privacy). Having addressed the problem, this article goes on to examine some of the legal and technological mechanisms currently available to deal with the issue, before concluding that, whilst at present they are inadequate, they contain within them the seeds of a more robust and mutually beneficial solution. It is hoped that by confining this discussion to a specific context, some lessons may emerge that can contribute to the wider debate on Internet privacy.

1. Introduction

Technical mechanisms for protecting copyrighted materials from unlawful reproduction have been around since the 1970s, when newsletters were first printed using non reproducing blue ink and signals from videotapes were distorted in a manner that would inhibit re-recording without affecting playback.[2] Despite this, until relatively recently, the most important means of preventing unlawful copying has been the *inherent nature* of the medium itself. Thus copying a book, even by way of a photocopier, is a relatively cumbersome task and the resulting copy is invariably less pleasant to read. Similarly, copying an audio-visual work generally requires the time that it takes to play the

---

[1] This paper is derived from the authors LLM dissertation submission. Thanks must go to Andrew Murray for his encouragement and supervision throughout; and also to Arvin Lee and Bankim Kapur for their helpful input. All errors, oversights and opinions remain those of the author who can be contacted at paul.ganley@bakernet.com

[2] Garfinkel, *Database Nation* (O'Reilly: Sebastopol 2001) p. 198

work itself, and often results in a noticeable loss of quality. It is this inherent nature that has defined and organised much of what we call the publishing industry today.

The emergence of digital networks, in particular the Internet, has radically altered this paradigm. Digitisation has enabled quick and perfect replication, whilst the Internet represents an infrastructure for cheap, global communications. Interpreting this change as empowerment or anarchy is of less concern here than an appreciation of its organisational nature[3] and the significance of its effects.[4] This, in turn, equates to a guarantee that stakeholders under the pre-existing system will attempt to redress the balance.[5]

Common sense dictates that the easiest way to keep control over something is to watch it, closely. Thus, as control slips, stakeholders are increasingly turning to surveillance as a means of real-time rights enforcement. Digital Rights Management (DRM) is an emerging industry which demonstrates most vividly this principle of monitored dissemination. It is individual privacy interests implicated in this practice that form the basis for discussion here.

---

[3] *See, e.g.*, Castells, *The Internet Galaxy: Reflections on the Internet, Business, and Society* (OUP: Oxford 2001) pp. 52-55 ('self-publishing, self-organisation, and self-networking constitute a pattern of behaviour that permeates the Internet, and diffuses from the Internet into the entire social realm', p. 55); Rifkin, *The Age of Access* (Penguin: London 2000) pp. 33-35 (highlighting the decline in physical property); Stefik (ed.), *Internet Dreams: Archetypes, Myths, and Metaphors* (MIT Press: Cambridge 1996) pp. 191-206 (discussing the shift from hierarchical distribution models to market-based structures); Volokh, 'Cheap Speech and What It Will Do' 104 *Yale Law Journal* 1805 (1995) pp. 1833-1838 (suggesting that new technologies 'democratise ... and diversify' the information marketplace, p. 1833); and Whitaker, *The End of Privacy* (The New Press: New York 1999) pp. 72-76 (suggesting that in a 'network society' there is a 'declining emphasis on vertical hierarchical authority structures and a rising emphasis on *horizontal linkages that cut across traditional organisational boundaries*', p. 74 [emphasis original])

[4] To offer just one example, the Recording Industry Association of America revealed in April 2002 that the total unit sales of music was down 12% in the period Jan-Mar 2002 compared to the same period in 2001. A similar pattern revealed itself when comparing sales in 2001 to 2000. This change is mostly attributed to emergent forms of digital copying and distribution. *See* Lieberman, 'Piracy Pillages Music Industry' *USA Today* April 8th 2002 via <http://www.usatoday.com> Also *see* 'Global Music Sales Drop' *BBCi* April 16th 2002 via <http://www.bbc.co.uk> (indicating a similar trend in global music sales) and Azeez, 'Tornado Group' *NewMediaAge* 18th April 2002 via <http://www.newmediazero.com> (indicating that the market for *legal* digital downloads in Europe is approximately 7-8% the size of the market for *illegal* downloads)

[5] *See generally* Lessig, *The Future of Ideas: The Fate of the Commons in a Connected World* (Random House: New York 2001), pp. 180-199

This paper comprises four main sections. Section 2 introduces the fundamentals of DRM, and provides an example of how a DRM enabled system might function. Section 3 then begins with a broad notion of privacy before locating specific privacy interests within the DRM scheme outlined. In Section 4 conventional mechanisms for protecting these interests are discussed and their weaknesses highlighted, whilst the final section offers a perspective on how privacy could be adequately protected. The hope is that some of the lessons learned in examining one aspect of the privacy mosaic may strike a chord in the wider Internet context.

2. Digital Rights Management Systems

2.1 *A Typical Digital Rights Management System (DRMS)*

The term DRMS is used here to denote the most advanced types of copy protection system currently on or near to the market, yet is important to remember that what is now called the DRM industry has grown organically over time and what DRM *is* should actually be read as what DRM might *become*.[6]

At the heart of any DRMS is two modules: a content module and a licensing module. These are intrinsically linked but, in the interests of flexibility, are necessarily separate.[7] The content module contains (or at least links to) digitised media, such as text or audio files, which have been securely packaged using encryption,[8] and are available for

---

[6] *See* Rosenblatt, Trippe, and Mooney, *Digital Rights Management: Business and Technology* (M&T Books: New York 2002) p. 79 ('Many types of technology fall under the rubric of 'DRM', however [few of them] actually enforce rights models'); Gervais, 'Electronic Rights Management and Digital Identifier Systems' 4 *Journal of Electronic Publishing* (1999) 3 available at <http://www.press.umich.edu/jep/04-03/gervais.html> section 'Going Electric'; and Waelde, 'The Quest for Access in the Digital Era: Copyright and the Internet' 2001(1) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/01-1/waelde.html> section 2.1. Terms used to describe the emergent copy protection technologies that form the basis for DRMSs include Copyright Management Systems (CMS), Electronic Copyright Management Systems (ECMS), Trusted Systems and ©-tech.

[7] *See* Rosenblatt et al., *supra* note 6, p. 81

[8] Two uses of encryption are utilised in a DRMS. Content itself, such as an audio or text file, is rendered unintelligible using a method called *single key encryption*. Utilising the content in this form is impossible unless the *same* key is applied to return it to its original form. The weak link in this method of encryption is having to transport the key itself from the client to the end-user. *Public key encryption* provides a solution. By separating a key into two parts - one 'private' and one 'public', *both* of which are needed to perform the encryption/decryption sequence - the client can encrypt a data packet containing both the single key encrypted content and the related key using the end-users 'public' key, who upon receipt can decrypt the data packet using their own

distribution through the DRMS. Before the content is encrypted it is embedded with metadata such as the author's name, copyright owner, date of creation, title, format, size, or some globally unique identifier such as an ISBN number. The licensing module generates digital licenses which automatically grant the end-user access to content by way of *usage rights* or *business rules*.[9] Usage rights have both a 'what' and a 'when' element. The 'what' element describes exactly how a piece of content may be used. This can include the right to view the content or print it out in the case of a text file (render right), the right to move the content from a PC to a portable device or lend it to a friend in the case of an audio file (transport right), or the right to edit the work or embed part of it in another file in the case of a moving image file (derivative work right).[10] The 'when' element attaches particular attributes to *each* right, such as the type of user who can exercise the right, the extent (i.e. length of time or number of times) for which a right may be exercised and the consideration (monetary or other) that must be in order to exercise the right.[11]

Thus, crucial to any DRMS is the ability to make the use of digital content dependant upon authorisation and to express the terms and conditions of access in a computer-interpretable way. It is from these building blocks that the overall picture of a typical DRMS emerges. I

'private' key which no-one else has access to. Public key encryption also allows end-users to 'sign' documents for authentication purposes, a process that may also be utilised in some DRMSs. For a highly readable introduction to cryptography *see generally* Schneier, *Applied Cryptography* (Wiley: New York 1995 2nd ed.) and for discussions on the utilisation of encryption standards in the context of DRMSs *see* Rosenblatt et al., *supra* note 6, pp. 95-102; Kumik, 'Digital Rights Management' *Comp. and L.* Oct/Nov (2000) 14, p. 14; and Stefik, Mark 'Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing' 12 (1997) *Berkeley Technology Law Journal* available at <http://www.law.berkeley.edu/journals/btlj/articles/12_1/Stefik/html/reader.html > section 'Trusted Systems'.

[9] The term 'business rules' is used by some commentators - *see, e.g.,* Garfinkel, *supra* note 2, pp. 202-205 - however the term 'usage right' is preferred here for its techno-legal connotations.

[10] Render, transport and derivative work rights are generic labels for rights that can exist for all types of digital media. *See generally* Stefik, *supra* note 3, pp. 228-235 and Rosenblatt et al., *supra* note 6 pp. 61-63.

[11] *See* Rosenblatt et al., *supra* note 6, pp. 63-64. Other rights called 'utility rights' exist which enable system critical functions such as the making of backup copies and the caching of content, but these exist out of technological necessity and need not concern us here.

shall describe this by reference to a fictional example from the not-to-distant future.[12]

> Sara is a final year law student who wants access to a new publication; the Online Law Journal (OLJ). Content from the OLJ is displayed using the customised DocuReader rendering device that was activated on Sara's system when she registered with the service. When she registers Sara's details are stored in the 'identities database' within the licensing module. Upon publication the contents of the bimonthly OLJ are encrypted and stored on the content module. At the same time usage rights defining types of use, the cost of each use and categories of user are generated and sent to the license module.
>
> When Sara wishes to view the latest issue, her document reader contacts the content module and an encrypted copy is sent to her. At this stage, if Sara wishes to view the contents page she may do so, but any further access is denied. This month's issue of the OLJ is an 'Internet Privacy Special', a subject Sara is currently writing a paper on, and thus is of keen interest to her. She wishes to obtain viewing privileges. At the heart of the DocuReader device lies a ContentControl element that Sara can use to request an extension to her privileges. ContentControl sends this request along with a digitally signed 'certificate' identifying Sara to the license server. The license server verifies the identity against information contained in the identities database (noting that Sara is a student and therefore entitled to a discount) and generates a user license containing information on Sara, her requested usage rights and the necessary content decryption keys. The license is encrypted using Sara's public key and is sent to ContentControl which can then decrypt and execute the license terms and conditions.
>
> Sara has requested a 3-day 'View Only' usage right for the (discounted) price of £4. The charge is added to Sara's billing record which is settled quarterly. 'View Only' allows Sara to view the entire issue on her PC for the specified time period but forbids her from printing content or copying it to any external application (including her DocuMaker word

---

12 Whilst this example is entirely my own it is derived from the descriptions of DRMSs in Bygrave and Koelman, 'Privacy, Data Protection and Copyright: Their Interaction in the Context of Copyright Management Systems' in Hugenholtz (ed.), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (Kluwer Law International: London 2000); Howe, 'Licensed to Bill' *Wired* Oct. 2001; Rosenblatt et al., *supra* note 6; Stefik *supra* note 3; and Stefik, *The Internet Edge: Social, Technical, and Legal Challenges for a Networked World* (MIT Press: Cambridge 2000)

> processor and her DocuReader enabled Portable Document Reader [PDR]).
>
> After three days, Sara is prompted by the system to purchase further rights to the content or lose all viewing privileges. This time she requests the 'Full Access' usage right to two of the articles at a cost of £2 per article. 'Full Access' entitles Sara to view the articles on her PC or PDR indefinitely, print out a maximum of 3 copies of each article and embed up to five 300 word segments in any DocuMaker file. It also allows Sara to send the article (along with the full content listings for the issue), as an e-mail attachment, to any 3 friends who have the DocuReader rendering device (this happens to be most of her law class as DocuReader comes bundled with the latest version of Windows Student) giving them a free 'One-Time-Session View Only' right to the article. If any of these friends go on to purchase a 'Full Access' right to any article from that particular issue Sara receives a £1 rebate.
>
> Finally, because Sara has purchased 'Full Access' to at least two feature articles, she is automatically given an indefinite 'View Only' right to the book review section. Should Sara wish to purchase any of these books in whole or in part at some point in the future the review contains an embedded 'hotlink' that automatically locates the item on the content server.

This description brushes over some of the more complicated technical details that are currently posing problems for the DRM industry, a point I shall return to shortly, however the basic mode of operation should be clear: fine grained control of access to and subsequent use of digital content.

2.2 *What DRM Represents- A Rosy Future?*

Crucially, the model outlined above represents a shift from an industry founded upon copyright to one more closely aligned with licensing and the law of contract.[13] For many legal commentators this change represents, above anything, an erosion to the right of fair use that the law has appended to copyright over time.[14] Others have suggested that

---

[13] *See generally* Bebbington, 'Managing Content: Licensing, Copyright and Privacy Issues in Managing Electronic Resources' 2 *Journal of the British and Irish Association of Law Librarians* (2001) 4, p. 1 (quoting McCracken 'the negotiation of licenses will define the library of the future', *see* fn.1); Bygrave and Koelman, *supra* note 12, pp. 116-118; and Lessig, *supra* note 5, pp. 184-185

[14] In English law many of the rights traditionally associated with fair use are codified under the label 'fair dealing'. *See* Copyright, Designs and Patents Act (CDPA) 1988 ss29-31. Also see Article 5 of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society [hereinafter 'Copyright

this doesn't matter,[15] or that DRM systems can easily account for fair uses when usage rights are defined.[16] This issue aside, there are clearly a number of advantages that a DRMS offers over traditional publishing, all of which derive from the unique flexibility of digital media. One of the most interesting is the idea of differential pricing. The pricing mechanisms in a DRMS are limited only by the imagination of the publisher defining the rules. Apart from the examples of incremental pricing by usage and the referral rebate in the Sara example above, DRMSs could 'subsidise' content distribution to the poor,[17] or offer near real-time pricing alterations as the age and popularity of content is monitored.[18] Furthermore, the system enables consumers to be put in contact with a large repository of content via ones peers, a concept known as 'superdistribution'.[19] In the Sara example above, the possibility of sending an article along with a 'One-Time-Session View

---

Directive'] which details exceptions to the exclusive right of reproduction (and others) that is afforded to the copyright holder. For discussions on how DRMSs can impinge upon such rights *see generally* Cohen, 'Some Reflections on Copyright Management Systems and Laws Designed to Protect Them' 12 (1997) *Berkeley Technology Law Journal* available at <http://www.law.berkeley.edu/journals/btlj/articles/12_1/Cohen/html/reader.html>; Lessig, *Code And Other Laws Of Cyberspace* (Basic Books: New York 1999), pp. 135-139; Samuelson, 'The Copyright Grab' *Wired* Jan. 1996; and Waelde, *supra* note 6. But *compare* Copyright Directive Article 6(4)

15 *See* Stefik, *supra* note 12, p. 98 ('to the extent that fair use is [a] response to market failure, [DRMSs] can help correct that failure and eliminate the ... issue'). Fair use/fair dealing are not rights *as such*, rather they are a defence to infringement (*see* CDPA 1988 s28(1)), and some have suggested that in making it redundant through technology the price of copyrighted works may decrease as *every* use can be accounted for. *See* Bygrave and Koelman, *supra* note 12, p. 118

16 *See* Stefik, *supra* note 12, pp. 89-90, 99-102; and Howe, *supra* note 12, but *compare* Rosenblatt et al., *supra* note 6, p. 45 (suggesting that it will prove too hard to define the contextual nature of such rights in computer code).

17 *See* Stefik, *supra* note 12, p. 250 ('copying a digital work is essentially free and no market share would be lost by giving a work to someone who couldn't afford to buy it anyway')

18 *See generally* Bayers, 'Capitalist Econstruction' *Wired* Mar. 2000. In the broadcasting sector an application called Peak Time allows TV executives to monitor in real time the popularity of various television shows, which can then help determine for how long a particular segment should run. *See* 'No one knows if anyone's watching' *Daily Telegraph* Jan. 11 2002 at p. 20. Of course such possibilities invariably depend on the type of content involved. *See* Rosenblatt et al., *supra* note 6, pp. 20-28.

19 The term 'superdistribution' originated in Japan, its aim being to 'let information flow freely, without resistance': *see* Cox, 'Superdistribution' *Wired* Sept. 1994. For 'superdistribution' in the DRM context *see* Rosenblatt et al., *supra* note 6, pp. 29-30; and 'Digital Rights and Wrongs' *The Economist* 17th July 1999 p. 75

Only' right to a friend is an example of superdistribution, which being *peer-approved* constitutes a new kind of word of mouth recommendation in a world content saturation.[20] How publishers take advantage of these opportunities on offer will substantially affect the success of DRMSs in the next few years.

2.3 *Unresolved Technical Issues*

Despite the above, at present the DRM industry offers unsatisfactory solutions for the majority of consumers. The most obvious reasons for this concern *usability* and stem from a heightened fear of illegal dissemination in the post-Napster age. At present most DRM vendors use proprietary standards in their solutions, particularly within the licensing module, a fact which serves to limit the available content on any given system.[21] Such a position overlooks one of the positive lessons from Napster, namely that users are keen on having a centralised repository of *all* content as opposed to dispersed collections of some.[22] Secondly, most people don't enjoy reading or viewing content on a computer screen, meaning workable solutions must to be device neutral or at least feature usage rights across multiple platforms.[23] Whilst there are signs that the standardisation issue is gradually being resolved,[24] the usability of current DRMSs is in a sense

---

[20] As far back as 1945 Vannevar Bush noted that the growth of human knowledge far exceeds the ability of individuals to utilise it, *see* Bush, 'As We May Think' excerpted in Stefik, *supra* note 3, pp. 15-22. Others have distinctly asserted the need for trusted 3rd party review of content in the digital age. *See* Shapiro, *The Control Revolution* (PublicAffairs: New York 1997) pp. 187-196; and Volokh, *supra* note 3, pp. 1815-1818, 1829-1831.

[21] In traditional media publishers have tended to handle rights and permissions in an *ad hoc* manner, but this has not affected the ease of putting a book, say, on a shelf. With digital content, however, this issue strikes at the very heart of content accessibility. *See* Bygrave and Koelman, *supra* note 12, p. 61; Rosenblatt et al., *supra* note 6, p. 25; Greenleaf, 'IP, Phone Home: ECMS, (c)-tech, and protecting privacy against surveillance by digital works' (1999) available at <http://austlii.edu.au/~graham/publications/ip_privacy/> section 'Standards and pervasiveness'. For a detailed examination of competing industry standards *see* Gervais, *supra* note 6, section 'Standards Issues'.

[22] *See generally* Lessig, *supra* note 5, pp. 130-132

[23] Part of the reason for the success of digital music is the absence of the 'viewing' problem that afflicts digital text and audio-visual work.

[24] Two emergent standards in the DRM industry - the Digital Object Identifier (DOI) and the Extensible Markup Language (XrML) - are discussed in sections 3.4.1 and 3.4.3 below. There are also signs that the World Wide Web Consortium is ready to grapple the issue. *See* Rosenblatt et al., *supra* note 6, p. 137; and *generally* Berners-Lee, *Weaving The Web* (Texere: London 2000). Others have suggested that the WIPO Advisory Committee on Management of Copyright and Related Rights in Global Information

inversely proportionate to the level of security it offers, and thus publishers find themselves in a Catch-22 scenario. In the long term it is expected that DRM-type solutions will be embedded in the hardware or operating system of all rendering devices from PCs to PDRs to mobile phones, a point which will herald the arrival of a DRM utopian in which the negotiation of usage rights is second nature in much the same way as using a graphical user interface is today.[25] However, until this point is reached the landscape of the future is open to interpretation.

2.4 *Summary*

A report published in September 2001 canvassed opinion amongst publishing industry professionals as to the emergence of DRMSs in the near future.[26] Whilst only 7% of respondents said their organisation was currently utilising DRM solutions, just under half indicated that their companies would do so in the future.[27] For some, DRM represents the epiphany of digitisation for the content industries who are finally appreciating the profound changes in business practices that the Internet fosters.[28] Indeed it seems that the DRM industry has entered into what Geoffrey Moore has labelled the 'chasm' of the technology adoption lifestyle: the point between emergence and mainstream adoption of a new technology where the industry slowly takes shape

---

Networks should act as the forum for discussions on standardisation. *See* Gervais, *supra* note 6, section 'The way forward: Interoperability'. The value of interoperability has also been recognised at an EU level. Recital 54 of the Copyright Directive states that in relation to systems for the identification and protection of digital works 'compatibility and interoperability of the different systems should be encouraged. It would be highly desirable to encourage the development of global systems'.

[25] *See generally* Rosenblatt et al., *supra* note 6, pp. 264-268 and *The Economist*, *supra* note 19. In the US the proposed Consumer Broadband and Digital Television Act (formerly the Security Systems Standards and Certification Act) is a step in this direction. The Act stipulates that all digital media devices incorporate copy protection technology by making it a felony to sell devices that don't include and utilise such technology. The text of the draft SSSCA is available at <http://cryptome.org/broadbandits.htm>

[26] *Industry Survey: Digital Rights Management: Usage, Attitudes and Profile of Users* (Seybold Seminars & Publications: Foster City 2001) [hereinafter 'Seybold Report (2001)'] The executive summary is available at <http://www.seyboldreports.com/Specials/DRMsurvey/>

[27] *Ibid.* This proportion rises to two thirds amongst providers of paid digital content.

[28] *See, e.g.*, 'Ten Emerging Technologies that will Change the World' *Technology Review* Jan/Feb 2001 pp. 102-103 via <http://www.technologyreview.com>

amid a plethora of failed ventures and confusion.[29] Yet for others, implementing DRM solutions is viewed as a waste of time. Anything that can be experienced or perceived by the human senses is liable to be copied, they argue, making the effort of copy protection a redundant one.[30] It is in response to this last point that the virtues of DRMSs are voiced most strongly. Perfect replication, instant access to content, elastic pricing models, community benefits, and marketing opportunities all suggest an added value to the copy protection effort, and here we arrive at the crux of this paper. The control over distribution and particularly the use of digital content may excite publishers, but should it concern consumers? In short, what are the *privacy implications* of the model outlined above.

3. Privacy And DRM

3.1 *The Concept of Privacy*

3.1.1 *Privacy*

In an oft-quoted statement from the dissenting judgement of Justice Louis Brandeis in *Olmstead -v- United States*[31] privacy was described as 'the most comprehensive of rights and the right most valued by civilised men'.[32] Why then, one must ask, can it be that discussions and discourse on privacy have become so complex, so convoluted and so filled with competing axioms that one commentator has remarked that 'sometimes [I] despair whether it can be usefully addressed at all.'[33] Indeed, in the United States very few States have adopted general rights of privacy,[34] whilst in Europe, despite legislative attempts to frame privacy as a fundamental right,[35] the plethora of exceptions and

---

[29] *See* Rosenblatt et al., *supra* note 6, p. 269; and Stefik, *supra* note 12, pp. 163-166.

[30] *See* Seybold Report (2001) (finding that half of all respondents felt that DRMS were a waste of time as it is impossible to fully protect against the unlawful copying of digital works) and *generally* Schneier, 'The Futility of Digital Copy Protection' *Cryto-Gram Newsletter* May 15th 2001 available at <http://www.counterpane.com/crypto-gram-0105.html#3>

[31] 277 U.S. 438 (1928)

[32] *Ibid* p. 478

[33] Post, 'Three Concepts of Privacy' 89 *Georgetown Law Review* [2001] 2087, p. 2087

[34] Reidenberg, 'Privacy in the Information Economy: A Fortress or Frontier for Individual Rights' 44 *Fed. Comm. L. J.* 44 [1992] 195, pp. 227-229.

[35] *See* European Convention on Human Rights [hereinafter 'ECHR'] Article 8(1) and Directive 95/46/EC on the protection of individuals with regard to the processing of

exemptions merely serve to highlight the word 'fundamental' as illusory.[36] In the United Kingdom, there is no general right to privacy- a position that has been criticised by some[37] - instead the courts have traditionally relied on an array of mechanisms, such as the law of breach of confidence; the torts of defamation and malicious falsehood; and even the law of copyright, to deal with privacy violations via the common law and the law of equity.[38] Recent developments suggest that the judiciary may be ready to endorse a general right to privacy at common law,[39] this being the result of - according to the Lord Chancellor in 1997 - the making of decisions 'on a more overtly principled, and perhaps moral, basis' due to the Human Rights Act and by regarding conduct, not against the bare letter of the law, but in light of the spirit behind it.[40] Whilst these predictions specifically concerned judges evaluating the behaviour of public authorities, Lord Bingham has recently stated that '[It is] likely that in years to come we shall see some development in the law of privacy even in actions between

---

personal data and on the free movement of such data [hereinafter 'Directive 95/46/EC'] Article 1(1)

[36] See ECHR Article 8(2) and Directive 95/46/EC Arts. 7 and 13

[37] *See generally* Markesinis, 'Our Patchy Law of Privacy - Time to do Something about It' 53 *Modern Law Review* [1990] 802. Furthermore, the Data Protection Act 1998 makes no reference to the word 'privacy' whereas Directive 95/46/EC upon which it is modelled states that 'Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data' [Art 1(1)]. The divergence between the Directive and the UK implementation has led to suggestions that the Directive has not been fully incorporated into UK law. *See* Charlesworth, 'Data Privacy in Cyberspace: Not National vs. International but Commercial vs. Individual' in Edwards and Waelde, *Law and the Internet: A Framework for Electronic Commerce* (Hart Publishing: Oxford 2000), pp. 89-90 and Warren et al., 'Sources of Literature on Data Protection and Human Rights' 2000(2) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/01-2/warren.html/> section 5

[38] *See generally* Bainbridge and Pearce, 'Tilting the Windmills – Has the New Data Protection Law Failed to Make a Significant Contribution to Rights of Privacy' 2000(2) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/00-2/bainbridge.html>; Bingham, 'The Way We Live Now Human Rights in the New Millennium' [1998] 1 Web Journal of Current Legal Issues available at <http://webjcli.ncl.ac.uk/1998/issue1/bingham1.html>; and Warren et al., *supra* note 37.

[39] *See, e.g.,* the speech of Sedley LJ in *Douglas and others -v- Hello Ltd* [2001] 2 All ER 289 pp. 316-325 ('the law ... can recognise the privacy itself as a legal principle drawn from the fundamental value of personal autonomy' at p. 320e)

[40] *Quoted in* Bingham, *supra* note 38.

private citizens'.[41] Despite such statements by those at the pinnacle of the judiciary it is clear that the common law is advancing in a tentative fashion at best and thus one must ask why this is so.

Unravelling what privacy means is a multifaceted and contextual endeavour.[42] Central to this task is the need to realise that the various other interests of various other individuals and institutions enter the fore. Thus while we all may regard the *concept* of privacy as inherently good,[43] there are relatively few people who would regard fighting crime as bad. Similarly within the ambit of the human rights legislation there is a sensitive tension between the right to privacy and the right of free expression.[44] At other times there can be a conflict between the interests of the individual and the interests of the collective. For example, public authorities may share data for convenience and for the mutual benefit of all taxpayers but in doing so, the *source* of such data may become further removed from the process.[45] Finally, revelation may result in many perceived benefits for the individual concerned. To take but one example for now: store loyalty cards record information relating to the buying habits of individuals to an extent that one commentator has described the process as a 'multi-variable science experiment',[46] yet the targeted offers that arrive through the door every month are welcomed by many. This balancing of competing interests has been labelled by Nissenbaum as the 'normative knockdown

---

41 *Ibid*. Also *see* Bygrave and Koelman, *supra* note 12, p. 70; and Warren et al., *supra* note 37, section 3.2.

42 *See* Reilly, 'Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward' 6 *Richmond Journal of Law and Tech*nology 6 (1999) available at <http://www.richmond.edu/jolt/v6i2/article1.html> para.7, Samuelson, 'Privacy as Intellectual Property?' 52 (2000) *Stanford Law Review* 1125, pp. 1170-1172; and Walker, 'Where Everybody Knows Your Name: A Pragmatic Look at the Costs of Privacy and the Benefits of Information Exchange' (2000) *Stanford Technology Law Review* 2 available at <http://stlr.stanford.edu/STLR/Articles/00_STLR_2/fsarticle.htm> para. 61

43 This point should be qualified for those approaching the issue from a purely economic standpoint, for example *see generally* Posner, 'The Right of Privacy' 12 *Georgia Law Review* [1978] 393, but *see* section 3.3.2 below for evidence to support the basic argument.

44 *See Douglas and others -v- Hello!* [2001] 2 All ER 289 at p. 322. Also *see* Bainbridge and Pearce, *supra* note 38, section 1 and Bingham, *supra* note 38, text accompanying fn.18

45 *See* Blume, 'The Citizens' Data Protection' 1998(1) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/infosoc/98_1blum/> section 2

46 Garfinkel, *supra* note 2, p. 158

argument',[47] and crucially, for the purposes of the discussion to follow, she notes that in respect of personal information 'it does not take much for a person's claim to privacy with respect to this information to be outweighed by countervailing claims, even ones that themselves are not terribly weighty'.[48]

Up to now this discussion has addressed many questions, but provided few answers. This has been necessary, however, to demonstrate that in attempting to dissect an issue as complex as privacy, the starting point for any enquiry should confine itself to the context and the specific interests at stake. The following section shall attempt to narrow the focus of our discussion on DRMSs in such a way.

3.1.2 *Three Areas of Privacy Interest*

In a 1998 article Professor Kang identifies three areas in which privacy interests arise.[49] These are grouped under the headings 'space', 'decision' and 'information'.[50] The idea of 'space' revolves around physical territory, thus a neighbour playing loud music late into the night would fall within the confines of spatial privacy. The term 'decision' is used by Kang to describe the notion of choice free from outside interference. Here the paradigm example would be the secret ballot. Finally the area of 'information' encompasses the collection, use and dissemination of personal information. Hence, one talks of a privacy violation occurring when someone obtains sensitive details about another person's medical condition without permission. Whilst Kang's subsequent enquiry focused on the third of these interests, he observed that on many occasions they are 'simultaneously implicated

---

47 Nissenbaum, 'Protection Privacy in an Information Age: The Problem of Privacy in Public' 17 *Law and Philosophy* (1998) 559, pp. 570-575

48 *Ibid* at p. 571. Also *see* Cohen, 'Privacy, Ideology, and Technology: A Response to Jeffrey Rosen' 89 *Georgetown Law Review* [2001] 2029 p. 2043 (noting the difficulty courts in the US face in creating a privacy interest from the disclosure of seemingly innocuous transactional level data). But *compare* 'Recommendation 3/97 Anonymity and the Internet' of the European Working Party on the Protection of Individuals With Regard to the Processing of Personal Data [hereinafter 'the Article 29 Committee'] ('*All* personal information is a potential threat to an individual's privacy...' at section 'The Privacy Perspective' [emphasis added]).

49 Kang, 'Information Privacy in Cyberspace Transactions' 50 *Stanford Law Review* (1998) 1193, pp. 1202-1205

50 *Ibid* at p. 1202.

by the same ... practice'.[51] This is an important observation for our discussion. DRMSs are predominantly used to deliver ideas and expression to individuals in the form of content. As will be demonstrated more fully below, such systems have an inherent potential to monitor the individuals use of such content (informational privacy interests), and can enable content providers to act on such data through highly targetted marketing and emerging practices such as price differentiation[52] in an attempt to influence our information consumption choices in the future (decisional privacy interest).[53] Thus, by narrowing the focus of our enquiry to the overlap between informational and decisional privacy and by pinpointing DRMSs as a specific contextual threat it should be possible to gleam more concrete insights into what solutions should be pursued.

3.2 *Informational Privacy*

3.2.1 *General*

Informational privacy emerged as an issue during the late 1960s and early 1970s, when seminal works by Westin and Miller laid down the issues and offered definitions that remain influential to this day.[54] Westin states that informational privacy lets individuals 'determine for themselves when, how and to what extent information about them is communicated to others',[55] whereas Miller framed the concept as giving 'individuals [the] ability to control the circulation of information relating to [them]'.[56]

---

[51] *Ibid* at p. 1203. Kang uses the term 'clusters' as opposed to 'areas' in an attempt to convey this overlapping methodology.

[52] For information on price differentiation in the broader Internet context *see generally* Bayers, *supra* note 18; Ward, 'Amazon's Old Customers "Pay More"' *BBCi* Sept. 8th 2000 via <http://www.bbc.co.uk>; and Walker, *supra* note 42, paras. 32-33

[53] It should be noted that the term 'decisional privacy' is often only used in connection with intrusive government interference, for example, in areas such as reproductive freedom. Here it is employed in a wider context to implicate the actions of external agents designed to influence any individual choice.

[54] *See* Warren et al., *supra* note 37, section 2

[55] Westin, *Privacy and Freedom* (Atheneum: New York 1967) p. 7

[56] Miller, *The Assault on Privacy* (University of Michigan Press 1971) p. 25

The United States Supreme Court gave informational privacy qualified backing in 1977 in *Whalen -v- Roe*.[57] In it's judgement the court explicitly noted the threat to privacy 'in the accumulation of vast amounts of personal information in computerised ... files'[58] This led to claims that the US Constitution embodies a right to informational privacy,[59] although further developments through the courts and the legislature in the US have remained relatively scarce.[60]

By contrast, the efforts to protect informational privacy at an EU level have been relatively recent and certainly more encompassing than the measures in the US. Originating as a purely economic entity, in the 1970's the European Commission was keen to promote computerised data processing as a means of bolstering the emerging IT and communications infrastructures. Informational privacy was a threat to this goal, and so personal data was treated in the same manner as other goods and services.[61] With the signing of the Maastricht Treaty in 1992 the European Community was transformed from an economic entity to a profoundly political one in a shift which necessitated formal protection for the rights and freedoms embodied in a democratic society.[62] With this structural change the Commission was unable to maintain its earlier stance and eventually, through Directive 95/46/EC,[63] informational privacy was characterised as a fundamental

---

[57] 429 US 589 (1977)

[58] *Ibid* p. 605

[59] *See* Froomkin, 'Flood Control in the Information Ocean' *Journal of Law and Commerce* 15 (1996) 395, p. 495 fn..381

[60] *Ibid* p.496 and Long, 'Who Are You? Identity and Anonymity in Cyberspace' 55 *University of Pittsburgh Law Review* [1994] 1177, pp. 1189-1193 (highlighting the limited number of subsequent judicial decisions); Rosen *The Unwanted Gaze* (New York: Vintage Books 2001) p. 167 and Reidenberg, supra note 34, pp. 201, 208-209 (noting the limited and context specific legislative enactment's); and Thompson, 'The Digital Explosion Comes With a Cost: The Loss of Privacy' 4 *Journal of Technology Law and Policy* (1999) 3 available at < http://journal.law.ufl.edu/~techlaw/4/Thompson.html> paras. 24-30 (explaining the concept of 'fair information practices' which have served as a guide for the public sector and several areas within the private sector)

[61] *See* Simitis, 'From the Market to the Polis: The EU Directive on the Protection of Personal Data' 80 *Iowa Law Review* (1995) 445, p. 446 and Charlesworth, *supra* note 37, pp. 84-85

[62] *See* Simitis, *ibid*, p. 447

[63] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

right and placed on a wide legislative footing.[64] So pronounced has been this shift that recently the protection of personal data was included in the 'Charter of Fundamental Rights of the European Union'.[65]

3.2.2 *The Problem of 'Attention Span'*

In a recent attempt to offer a coherent rationale for informational privacy, Jeffrey Rosen has argued that we require protection 'from being misdefined and judged out of context in a world of short attention spans ...'.[66] Rosen believes that because we, as individuals, have less chance to 'present ourselves publicly in all of our complexity', we run the risk of being 'unfairly defined by isolated pieces of information that have been taken out of context'.[67] Rosen's point about being judged out of context has been keenly debated,[68] yet it is the point about limited attention span that I wish to pursue here.

In 1987 the video rental records of Robert Bork were obtained by journalists at the time of his US Supreme Court confirmation hearings. It seems that those opposed to his appointment hoped the records would reveal some salacious details about his private life. Despite the fact that the records actually revealed a penchant for mild fare such as Disney movies and Hitchcock films, the reputation of Bork was still somewhat damaged, because, as Garfinkel notes, '[some] accounts ... erroneously [gave] the impression that Bork was a fan of porn'.[69] Thus, for some people the mere *hope* that these records would reveal some

---

64 *See* fn.35 above and section 4.2 below. *See generally* Cate, 'The EU Data Protection Directive, Information Privacy and the Public Interests' 80 *Iowa Law Review* (1995) 431; and Simitis, *supra* note 61. Also *see* Samuelson, *supra* note 42, p. 1170 (suggesting European policy offers some 'useful lessons' for the US in constructing an information society 'in which people will want to live'), but *compare* Petersen, 'Internet Privacy Concerns and the Need for Regulation' 5 *Michigan Telecommunications and Technology Law Review* (1998) available at <http://www.mttlr.org/forum/petersen.html> text accompanying fns.24-27 (suggesting that the European regime is becoming overly bureaucratic and is too inflexible to account for changes that technology brings)

65 *See* 'Charter of Fundamental Rights of the European Union' 2000/C *Official Journal of the European Communities* 364/01 Art 8

66 Rosen, *supra* note 60, p. 8

67 *Ibid* p. 158

68 *See* Cohen, *supra* note 48, pp. 2029-2030 and Post, *supra* note 33, p. 2088. Rosen's response to these critiques can be found in Rosen, *supra* note 60, pp. 228-230.

69 Garfinkel, *supra* note 2, pp. 72-73

salacious details was enough for them to form a "complete" picture of the incident.

In the English defamation case *Charleston -v- News Group Newspapers*,[70] a sexually explicit photograph on the front page of a national newspaper which had been superimposed with the faces of a famous actor and actress, was held to not be defamatory because of a portion of explanatory text lower down the page. Lord Bridge admitted that some readers would not read the accompanying text but went on to note that such people could not be regarded as 'ordinary, reasonable, fair minded readers' for the purpose of the defamation test.[71] Whilst this case has been criticised as exemplifying existing deficiencies in the English law of defamation,[72] for present purposes the judicial appreciation of Rosen's 'attention span' is of interest..

However, it is here that we must differentiate between the informational privacy interest in these two examples and that threatened by DRMSs. The examples above concern sensationalist reporting and matters of general public interest. In relation, the informational privacy threat of DRMSs appears a distant cousin. Julie Cohen has remarked that Rosen's chapter on cyberspace privacy 'sits uneasily in relation to the rest of [his] book'[73] and suggests that private entities are more concerned with turning personal information into profit than satisfying the prurient interest of the public.[74] Thus it becomes vital, if we are to confine our discussion to a specific context, to differentiate between the informational privacy interests of the victims of a gossip hungry media and those that are implicated by the actions of profit seeking private entities.

3.2.3 *Profiling*

It is somewhat ironic that despite popularist perceptions of the surveillance capabilities of the state in movies such as *Brazil* and *Enemy of the State* and novels like *Nineteen Eighty Four* and *We*, the main thrust of the initiative that resulted in Directive 95/46/EC was data collection

---

[70] [1995] 2 AC 65

[71] *Ibid* p. 73

[72] *See* Bainbridge and Pearce, *supra* note 38, section 3.1.1

[73] Cohen, *supra* note 48, p. 2029. Much of Rosen's book deals with the issue of sexual harassment and monitoring in the workplace. *See generally* Rosen, *supra* note 60,

[74] *See* Cohen, *supra* note 48, p. 2031

by private entities.[75] That the public and private sectors proved impossible to separate in the resulting legislation[76] need not concern us here. Instead, it should be understood that, as Joel Reidenberg has remarked, the 'private sector has precisely the type of dossiers that the public has long feared government would abuse'.[77] Whilst, the state may be seen an easy target and is, to an extent, 'personified' by the electoral process,[78] much of the data processing performed by private companies is seemingly invisible[79] and, at first glance, inconsequential.[80] Thus it is hardly surprising that the exchange of *information* is increasingly seen as an accepted part of the bargain between a merchant and a purchaser.[81] Furthermore, the value that many companies attach to personal information is such that in some instances companies have been pursued as merger partners because of their customer lists.[82]

In today's marketplace the real value attached to data comes when various sources are stored, aggregated, compared and matched. In short: when we are profiled. As far back as 1985 it was remarked, '[o]ur

---

75 *See* Simitis, *supra* note 61, p. 452. For a useful overview of the technological developments that encouraged this shift in emphasis *see generally* Mayer-Schönberger, 'Generational Development of Data Protection in Europe' in Agre and Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press: Cambridge 1997). Similarly, the plethora of privacy-related pressure groups in the United States have, as their primary concern, the use of personal data by private entities. *See, e.g.,* Charlesworth, *supra* note 37, p. 97

76 Simitis, *supra* note 61, p. 452

77 *Quoted in* Sovern, 'Opting In, Opting Out, Or No Options At All: The Fight For Control of Personal Information' 74 *Washington Law Review* (1999) 1033, p. 1036. Also *see* Charlesworth, *supra* note 37, pp. 80-82 (listing reasons why this is the case); Garfinkel, *supra* note 2, p. 3 ('The future we're rushing towards isn't one where our every move is watched and recorded by some all-knowing "Big Brother". It is instead a future of a hundred kid brothers that constantly watch and interrupt our daily lives'); Whitaker, *supra* note 3, p. 71 ('Only in the for-profit private sector are there resources to produce sophisticated [personal] information')

78 *See* Whitaker, *supra* note 3, pp. 133-134

79 *Ibid* and *see* Bayers, 'The Promise of One to One (A Love Story) *Wired* May 1998 and Skok, 'Establishing a Legitimate Expectation of Privacy in Clickstream Data' 6 *Michigan Telecommunications and Technology Law Review* 61 (2000) available at <http://www.mttlr.org/html/volume_six.html/skok.html> para. 8

80 *See* Nissenbaum, *supra* note 47, p. 587 and Reidenberg, *supra* note 34, p. 207

81 *See* Sovern, *supra* note 77, p. 1040

82 *Ibid* at p. 1045-1046

revolution will not be in gathering data ... but in analysing the information that is already willingly shared'.[83] This comment can be attributed to Larry Hunter, a computer scientist, which leads us directly to the root cause of the profiling phenomenon: information technology. Dramatic increases in processing power and storage capacity of computers have created an environment in which profiling becomes so easy as to become a ubiquitous part of the business environment.[84] But, it is on the Internet where data is *generated* in digital form that the ability to profile is most apparent. Every action we take and reaction we make in cyberspace can be seamlessly collected, analysed and viewed by those who are inclined to do so. The term 'clickstream data' has even been coined to account for the amount of data that is available through the medium, in a form that is ripe for processing.[85] Such a label is apt precisely because it characterises this data source as a *by-product* of Internet usage, and in the same sense that carbon monoxide emissions are an inevitable yet threatening result of motorised transport, clickstream data poses a threat that has invigorated privacy activists everywhere. Michael Froomkin has described our current situation as akin to living in an 'information fishbowl'[86] and the consequences of such an environment warrant careful discussion.

In the United States in 2000 a class action suit - alleging 'trespass to privacy and property' - was filed against RealNetworks when it became apparent that the company's software product RealJukebox was designed to facilitate the monitoring of users activities.[87] RealJukebox allows users to play and record music CDs on their computers,[88] but, by utilising a Globally Unique Identifier (GUID) contained within each copy of the software, information about recently recorded music; types of portable music player; and even web-sites visited via the 'Sites' menu could be communicated on a daily basis to

---

[83] *Quoted in* Nissenbaum, *supra* note 47, p. 560

[84] *See* Cohen, Julie E. 'A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace' 28 *Connecticut Law Review* 981 (1996), p. 981; Froomkin, *supra* note 59, p. 480; Kang, *supra* note 49, pp. 1238-1241; and Skok, *supra* note 79, para. 7

[85] *See* Skok, *supra* note 79, para. 6

[86] Froomkin, *supra* note 59, p. 507

[87] *See* Preston, 'Finding Fences in Cyberspace: Privacy, Property and Open Access on the Internet' 6.1 *Journal of Technology Law and Policy* (2000) 3 available at <http://grove.ufl.edu/~techlaw/vol6/Preston.html> section III.B

[88] RealNetworks software which incorporates the RealJukebox component is installed on an estimated 190-200m PCs world-wide. *See* Howe, *supra* note 12, and Rosenblatt et al., *supra* note 6, p .25

RealNetworks.[89] RealNetworks denied that it monitored users activities, but admitted the existence of a GUID in the application which is stored in a database alongside the users name and e-mail address.[90] Soon after this 'feature' was uncovered RealNetworks released a software patch allowing users to disable it, and hired a privacy officer to monitor the use that was made of the data already collected.[91] For present purposes, however, we need only note the surreptitious nature of the mechanism and the consternation that its discovery aroused.

It is suggested by some that digital technologies, such as RealJukebox, may merely act as a quantitative multiplier in the informational privacy debate.[92] However, such a view can be regarded as incomplete for failing to account for the fact that when discrete pieces of data are woven into a profile, the result is certainly more valuable than the sum of its parts. Here, individual pieces of data act as reference points for each other, and help to colour the processors' "picture" of the individual. Thus a *qualitative* shift in the informational privacy tug-of-war between commerce and individuals takes place.[93]

3.2.4 *Data, Knowledge, Risk-Aversion and Prediction*

As Reidenberg has noted, the disparity between the views of industry and individuals on profiling 'reflects the inchoate sense that privacy harms can occur incrementally by the increased processing of personal information ... and does not require a series of singularly offensive abuses to warrant consideration and review of legal protection'.[94] In short, profiling, whilst seemingly innocuous, can 'describe' us in a profound manner, by garnering a rich tapestry of data on what we

---

[89] For a technical summary of how the GUID could be utilised in this manner *see* Smith 'The RealJukeBox Monitoring System' 31st October 1999 at <http://users.rcn.com/rms2000/privacy/realjb.htm>

[90] *See* Spring, 'Privacy 2000: In Web We Trust?' *PC World* June 2000 via <http://www.pcworld.com/>

[91] *See generally* Robinson, 'CD Software Said to Gather Data on User' *New York Times* Nov. 1st 1999 C1

[92] *See* Cohen, *supra* note 48, pp. 2036-2037 for an explanation of this viewpoint

[93] *See* Skok, *supra* note 79, paras. 22-23 (arguing that this qualitative shift manifests itself in allowing the 'underlying circumstances of [a] transaction' to be known). Also *see* Cohen, *supra* note 48, p. 2037; Kang, *supra* note 49, pp. 1239-1240; and Nissenbaum, *supra* note 47, pp. 588-590

[94] Reidenberg, *supra* note 34, p. 207

seemingly care about in a number of different contexts.[95] Recall, the discussion above on what Rosen regarded as an 'attention span' problem.[96] For Rosen, the root cause of the problem he outlined was in confusing data with knowledge.[97] Knowledge, he argues, 'cannot be rushed' and requires a 'slow process of mutual revelation'.[98] The assimilation of packets of mere data on the other hand is simply a haphazard short cut that creates 'an inaccurate picture of the full range of our interests and complicated personalities'.[99] The story of Owen Lattimore is striking example to support Rosen's hypothesis. In the United States in 1950 Lattimore, an academic who specialised in Chinese affairs, was named by Senator Joe McCarthy as a spy. He eventually stood trial in 1955 for perjury, in a case that was ultimately dismissed for a complete lack of evidence. In recounting the affair later he noted that the FBI had compiled a profile of a 'man who might have existed'.[100] This phrase encompasses perfectly the dangers of confusing information with knowledge.

Despite this, the commercial mantra '*know* your customer' suggests that the dangers inherent in this confusion are a two-way street. Businesses don't make money by second-guessing their customers. Instead it is on the hard evidence of individual propensities and habits that business plans are formulated. Thus it is only by reducing uncertainty and limiting ambiguity that the private sector can hope to maximise its profits.[101] In essence, individuals may be misjudged through the confusion of data and knowledge, but it is in the interests of the private sector to make sure that this doesn't happen. Reg Whitaker has classified this business need as a form of risk aversion in which

---

[95] *See* Nissenbaum, *supra* note 47, pp. 588-590 and Cohen, *supra* note 48, at p. 2037. Nissenbaum has also suggested that viewing actions across multiple contexts is a breach of 'contextual integrity' which safeguards the right of individuals to behave differently in a variety of settings. *See further* Nissenbaum, *supra* note 47, pp. 581-586.

[96] Section 3.2.2 above

[97] For an interesting example of how metadata can be confused with knowledge, refer to the Stefik's anecdote of the 1996 chess match between the, then world champion Gary Kasparov, and the rest of the chess playing world. *See* Stefik, *supra* note 12, pp. 154-155

[98] Rosen, *supra* note 60, p. 8

[99] *Ibid* at p. 167

[100] *Quoted in* Whitaker, *supra* note 3, p. 26

[101] *See* Castells, *supra* note 3, p. 101; Cohen, *supra* note 48, p. 2032; Dyson, *Release 2.0: A Design for Living in the Digital Age* (Broadway Books: New York 1997), p. 20; Garfinkel, *supra* note 2, p. 35; and Post, *supra* note 33, p. 2088

companies are ever more concerned with 'the predictive power of the information [they] gather'.[102] It is this future-orientated approach to data collection that signals the meeting point between informational and decisional privacy. This is the point where the extension of information gathering technologies eventually shifts from data collection to data use. The furore over RealNetworks monitoring and the corporate necessity of transforming mere data into knowledge are clearly incompatible, a tension which, it is suggested here, is defined by the positive and negative aspects of predictability. The positive aspect is characterised by risk aversion, but it is the negative side - a subtler argument - that must now command attention, before any solution to the threat posed by DRMSs can be suggested.

3.3 *Decisional Privacy*

3.3.1 *Anti-Privacy*

Anne Branscomb has written of information, that it 'is the lifeblood that sustains political, social and business decisions'.[103] Thus any laws which attempt to regulate or control the free flow of information will seemingly have a negative impact somewhere along the line.[104] When this impact hampers business a type of friction is applied to commerce. Indeed, junk mail may only be labelled junk because by imposing controls on the monitoring of information flows, the costs of matching interested buyers and sellers is increased.[105] Similarly, the health of our economy rests upon those who offer credit being able to process the personal information of data subjects for the assuagement of risk.[106] However, for present purposes, I wish to focus on a very specific aspect of what can be very loosely termed the anti-privacy critique: when privacy rules impose costs on the very individuals they are designed to protect. In an article from 1978 Richard A. Posner concluded that 'the trend has been toward expanding the privacy protections of the

---

[102] Whitaker, *supra* note 3, p. 45

[103] *Quoted in* Cate, *supra* note 64, p. 440

[104] *See* Posner, *supra* note 43, p. 394 (characterising both privacy and 'prying' as intermediate economic goods). Also *see* Blume, *supra* note 45, section 3; Froomkin, *supra* note 59, pp. 402-407; and Reilly, *supra* note 42, para. 18

[105] *See* Kang, *supra* note 49, pp. 1217-1218 and Bayers, *supra* note 79

[106] *See* Blume, *supra* note 45, section 3 ('Credit reporting illustrates a situation where the collective interest overrides the interests of the individual') and Walker, *supra* note 42, para. 64 (noting that monitoring spending patterns is a necessary fraud prevention mechanism)

individuals while contracting those of organisations ... [t]his trend is the opposite of what one would expect if efficiency considerations were motivating privacy legislation'.[107] Inherent in Posner's conclusion is the view that the transaction costs of uncovering concealed information stifle the efficiency of the market by hindering the optimal allocation of resources. Hence, the existence of comprehensive databases containing personal information is not necessarily a bad thing, and may indeed contribute to consumer satisfaction on several fronts.[108]

According to Walker, privacy is misunderstood, because it far easier to dramatise invasive technological advances 'than to assess the widely dispersed benefits of a thousand people who [receive] products more cheaply and easily'.[109] Similarly, Solveig Singleton believes that those who trumpet the loss of privacy as 'morally shocking' are simply inexperienced in the new information economy and have failed to grasp that automation is merely a more efficient method of doing what we've always done.[110] Such sentiments, on at least one level, seem to ring true. If your local baker recalls that you prefer to have your loaf of bread sliced thickly, is the scenario really that different if your on-line bookstore remembers that you like to browse in the 'law and technology' section, and are either really privacy issues at all? And whilst we must note the *qualitative shift* argument,[111] it would be presumptuous to conclude that changes along these lines are automatically a bad thing.

The dissemination of personal information in the Internet context often leads to a customised experience, the notion of which emerged as an solution to the realisation a lack of hierarchical organisational structure on the World Wide Web was hindering its growth.[112] As advertising revenues dropped off, new business models emerged which try to bolster the "efficiency" of the enterprise.[113] By offering customised

---

[107] Posner , *supra* note 43, p. 422

[108] *See* Froomkin, *supra* note 59, p. 481

[109] Walker, *supra* note 42, para. 13

[110] *Quoted in* Reilly, *supra* note 42, para. 20

[111] Section 3.2.3 above

[112] *See* Kelly and Wolf, 'Push!' *Wired* Mar. 1997 ('The best part of the Web is its worst: it's a web. You don't know where the good stuff is...'). Castells has suggested that usage of the Internet impacts negatively on sociability when a user is new to the medium in part because of information overload: *see* Castells, *supra* note 3, pp. 123-124

[113] *See* 'A Short Life for Ads at the Top of Web Pages' *New Media Live* Aug. 28th 2000 via <http://www.newmedialive.ie>; Wearden 'Internet ad slump forces Marketwatch to

content such as stock portfolios, personalised news, and localised weather reports or entertainment listings, online businesses hoped that they would be in a better position to capture the attention of users.[114] Results would suggest that new approaches such as these have been successful. *Business Week* has reported that '[at] Excite Inc. ... customers who exchange titbits about themselves in return for a personalised experience ... return to the site roughly twenty times more often than those who don't'.[115] Similarly, in recent years, Amazon - a company at the forefront of online customisation initiatives - has seen its proportion of repeat purchasers grow even as its customer base has broadened significantly.[116] None of this would be possible without the use of personal information, which, according to Walker '[lets] you [enjoy] all that society and the market have to offer'.[117]

However, it is here that we must draw a line between customisation and personalisation, which is a fine one. The former acts upon the users *express* desires whereas the latter takes the initiative without the subjects input, and *implies* preferences on the basis of past conduct.[118] This distinction can be characterised in another way, as the difference between 'push' and 'pull' media.[119] With the former, information is sent to the user without his asking, whereas the operation of pull technologies is instigated by the user. Thus search engines are a form of

---

slash jobs' *ZDNet UK News* June 4th 2001 via <http://news.zdnet.co.uk>; and Nerney 'A Stumbling Giant' *internetnews.com* Mar. 13th 2002 via <http://www.internetstockreport.com>

114 Examples of such services include *My Yahoo!* <http://my.yahoo.com/ > and *My MSN* <http://my.msn.com/my.ashx >

115 Baig et al. 'Privacy' *Business Week* April 5th 1999 p.86. Also *see generally* 'Personalisation Increasingly Popular' *NUA Internet Surveys* Jan. 5th 2000 via < http://www.nua.ie/surveys/>

116 *See* Bayers, *supra* note 79, (between early 1997 and early 1998 the number of Amazon's customers who had previously purchased from Amazon.com before rose from 40% of 340,000 to 58% of 1.5m).

117 Walker, *supra* note 42, para. 3. Walker goes on to list the advantages of information exchange. These come under the headings Cost, Access, Convenience, Collective Benefits, Community, Security, Accountability and Trust (*ibid* paras. 26-82).

118 *See generally* Nunes and Kambil, 'Personalization? No Thanks.' *Harvard Business Review* April 2001 32. Also *see* Bayers, *supra* note 79, p. 3 and Walker, *supra* note 42, para. 43

119 For a lucid introduction to 'push' media *see generally* Kelly and Wolf, *supra* note 112. Also *see* Safier, 'Between Big Brother and the Bottom Line: Privacy in Cyberspace' 5 (2000) *Virginia Journal of Law and Technology* 6 available at <http://www.vjolt.net/vol5/issue2/v5i2a6-Safier.html> paras. 65-69

pull technology, whilst 'cookies' are an example of push methods. It is push media that highlight most starkly the distance between those who view new technologies as inherently privacy invasive and those who only see the new opportunities they offer.[120]

The dream for 'push' enthusiasts is simple. User participation may be required at the outset to delimit a profile of likes and dislikes (or it could be derived from past conduct) after which the technology does the rest, delivering a stream of profile matched content, including advertisements and promotions, to whatever networked device happens to be on at a given time. It is suggested by some commentators that such technologies 'create a *fundamentally different* paradigm in marketing' by offering people to products rather than the reverse,[121] and for those who regard market efficiency as the crucial gauge of the new economy, push methods of content delivery mark the future direction of the Internet. Of course, such a view is not ubiquitous, in fact views on privacy in general and 'push' media in particular encompass a diverse spectrum, a point to which I now turn.

3.3.2 *Survey Evidence*

People tend to regard the *concept* of privacy very highly. For example, in a 1996 survey commissioned by Equifax, 89% of Americans were concerned about threats to personal privacy.[122] Furthermore, substantial number of consumers believe that their privacy interests are threatened

---

[120] 'Cookies' represent the most well known push media. A cookie is a small pieces of software code which is downloaded to and stored on a users computer when he first visits a web site. They are used to store information concerning the user (e.g. a credit card number) so that it can automatically be retrieved and reused in the future. Recent surveys suggests that the majority of web users do know what cookies are, yet relatively few people go to the trouble of disabling them. *See* 'Personalization and Privacy Survey' [hereinafter 'Personalization Survey'] April 5th 2000 at <http://www.personalization.org/SurveyResults.pdf> and Kelsey 'Almost No One Rejects Cookies - Study' *Newsbytes* April 3rd 2001 via <http://www.newsbytes.com>. Nevertheless, the European Parliament has recently voted in favour of an amendment to the proposed Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector [COM (2000) 385] that would block the placing of a cookie on a users computer without his permission. *See* 'Europe Tackles Internet Privacy' *BBCi* Nov. 13th 2001 via <http://www.bbc.co.uk>. The cookie debate represents an interesting aside to the point made about the invisible nature of much automated data processing.

[121] Safier, *supra* note 119, para. 70 [emphasis original]. Also *see* Rifkin, *supra* note 3, pp. 97-101

[122] *See* Sovern, *supra* note 77, p. 1057. UK consumers tend to feel the same. *See* Costanzo 'Understanding Customers in an E-age' *IIBFS* June 2000 via <http://www.leeds.ac.uk/iibfs/> section 3.1

by marketers and advertisers.[123] Indeed, a recent report by Forrester, predicted that the US economy would lose $15bn in online sales (or 27% of the projected revenue) in 2001 as a direct result of consumer privacy fears,[124] whilst in the UK research by the National Consumer Council found that approximately one third of consumers fear that the Internet is the riskiest place to shop with privacy fears accounting for much of the concern.[125] According to one poll, consumers in the US are more concerned with the potential loss of privacy online than they are about healthier, crime and taxation,[126] and in 1998 it was revealed that online privacy had overtaken censorship as the primary concern among Internet users.[127] Given these statistics then, it is hardly surprising that as many as two thirds of Internet users tend to abandon web sites when asked to provide personal information,[128] and that nearly four fifths of Americans agree with the proposition that privacy should rank alongside 'life, liberty, and the pursuit of happiness' as a fundamental right enshrined in the Declaration of Independence.[129]

This, however, is not the end of the story. Steven Miller has commented that the apparent concern the public have for privacy is 'like the River Platte, a mile wide but only an inch deep',[130] and the fact that nearly

---

123 *See* Sovern, *supra* note 77, p. 1057. But *compare* Blume, *supra* note 45, section 3 (suggesting that many forms of marketing are not privacy infringing). The backlash that greeted the proposed merger in the US between the Internet advertising firm DoubleClick and the market research firm Abacus - a deal that would allow the linking of on-line and off-line browsing and purchasing habits with actual identities - would appear to support the proposition put forth here. *See* Garfinkel, *supra* note 2, p. 274 and Rosen, *supra* note 60, pp. 163-164

124 *See* 'Privacy issues inhibit online spending' *NUA Internet Surveys* Oct. 3rd 2001 via <http://www.nua.ie/surveys/>

125 *See* Vergnes 'E-commerce - overcoming consumer fears' *PSCA* Mar. 22nd 2001 via <http://www.publicservice.co.uk>

126 *See* 'E-Consumer Confidence Study' Aug. 30th 2000 at <http://www.nclnet.org/downloads/results.pdf>. An Australian poll survey from 1995 reports a similar finding: *see* Davies (1997) p.147 (ranking privacy second in importance only to education)

127 *See* 'Privacy Top Net Concern' *NUA Internet Surveys* Mar. 27th 1998 via <http://www.nua.ie/surveys/>

128 *See* 'Consumers wary of giving personal information' *NUA Internet Surveys* Mar. 27th 1998 via <http://www.nua.ie/surveys/>

129 *See* 'Equifax Executive Summary 1990' [hereinafter 'Equifax 1990 Summary' via <http://www.privacyexchange.org>

130 *Quoted in* Reilly, *supra* note 42, para. 19

every Internet user has provided personal information to a web site at some point reveals that there is a disparity between conceptual and practical views of privacy.[131] In fact there is strong evidence to suggest that for many people general privacy concerns make way for pragmatic choices when it boils down to specifics. For example, a survey by personalization.org found that 73% of a 4500 sample agreed or strongly agree with the proposition that it was helpful and convenient for a web site to remember basic information about them.[132] More tellingly only 20% of respondents disagreed in any form to the suggestion that web sites should remember more detailed personal information such as musical preferences.[133] Similarly, the idea of receiving tailored advertisements is, according to a number of surveys, appealing for the majority,[134] even when it is clearly spelt out that this may involve the collection and aggregation of online surfing and shopping patterns.[135] Question framing is obviously an important factor in judging responses,[136] but what seems clear is that consumers seem willing to divulge personal information provided that its use is seen as mutually beneficial.[137] In view of the multiplicity of responses that privacy

---

131 *See* Personalization Survey qu.4

132 *Ibid* qu.5(4)

133 *Ibid* qu.5(5). Also *note* qu.5(8) (51% of respondents either strongly agree or agree that they are willing to provide personal information 'in order to receive an online experience truly personalised for me') and qus.6-7 (demonstrates that people are more willing to divulge personal information of any sort to a web site offering a personalised experience than to one that does not). Also *see* 'Business Use of Consumer Information for Direct Marketing: What the Public Thinks' Aug. 2001 [hereinafter 'Direct Marketing Survey'] via <http://www.piac.ca> pp.9-10 (table 3.1) and pp.13-14 (table 3.3)

134 *See* 'Europeans Willing to Provide Personal Data' *NUA Internet Surveys* May 28 1999 via <http://www.nua.ie/surveys/> (also note that younger generations, particularly in the UK, are more willing to share information for what they perceive as benefits) and 'Privacy & American Business Survey Executive Summary' July 1999 [hereinafter 'Privacy & American Business Survey'] at <http://www.pandab.org/doubleclicksummary.html> section 'Key Messages of the Survey'

135 *See* Privacy & American Business at section 'Willingness to have Personal Information Used for Ads' and fn.120 above. But *compare* Direct Marketing Survey pp.14-15 (tables 3.4a-b) (finding that this is the case only for the minority)

136 *See, e.g.*, Sovern, *supra* note 77, p. 1061 and Walker, *supra* note 42, para. 94

137 *See* Equifax 1990 Summary ('[people] want the opportunities which the collection and use of personal information make possible') and 'Privacy Versus Personalisation: New Consensus' *NUA Internet Surveys* Aug. 25 2000 via <http://www.nua.ie/surveys/> ('while 71 percent of users will personalise a web site, 49 percent believe that a site which shares their personal information with another site is violating their privacy')

surveys invariably tend throw up, privacy expert Alan Westin has split consumers into three broad groups; privacy fundamentalists, privacy unconcerned and privacy pragmatists. Westin believes that privacy pragmatists, who account for roughly 60% of all consumers, vary their views on information usage according to factors such as the type of industry, the value attached to the use of data, the relevance of the information and the privacy policy of the business in question.[138] It is these people who make the area of data regulation so complicated and necessitate recourse to a more general principle, labelled here 'decisional privacy', before we can fully understand the ramifications of DRMSs.

3.3.3 *Dangers*

In 1998 the *New York Times* columnist Russell Baker wrote, 'I hear it said that people who have nothing to hide need not fear this strangulation technology of surveillance. And where are they, these people with nothing to hide?'.[139] Such sentiments resonate strongly against the perception, discussed above, that it is only by the collection of more personal information that a mutually beneficial 'truth' can be uncovered.[140] I use the word 'truth' here to mean the articulation of an individual's real preferences and desires, as opposed to the 'manufactured truth' that results when third parties, basing their actions on a profile, pre-empt choice by imposing their own view of what that choice would be.[141] This section is an exploration of the dangers inherent in the latter of these 'truths'.

In a 1983 decision by the German Constitutional Court on the constitutionality of the national census, it was said that if individuals are generally ignorant as to the use of their data they will tend to conform to the expectations of the processor and in doing so these individuals will renounce the power to freely express their own views

---

138 *See* Sovern, *supra* note 77, pp. 1061-1062.

139 *Quoted in* Whitaker, *supra* note 3, p. 158

140 The term 'truth' is borrowed from Julie Cohen: *see* Cohen, *supra* note 48, p. 2036

141 *See* Kang, *supra* note 49, pp. 1214-1215 (noting that 3rd party evaluation of data can miss much of the complexity inherent in its generation) and Whitaker, *supra* note 3, p. 137 ('the simplified, perhaps simplistic, data profiles are patterned to answer corporate needs'). The word 'choice' is used here guardedly. Much discussion of the so-called 'privacy-as-choice' model focusses on the number of possible choices (i.e. A, B or C), *see, e.g.,* Cohen, 'Examined Lives: Informational Privacy and the Subject as Object' 52 *Stanford Law Review* (2000) 1373, pp. 1391-1402. Here, however, the term 'choice' refers to the construction of *each particular* choice (i.e. what is A).

and opinions.[142] The case gave rise to the expression 'informational self-determination' as a mechanism for countering the danger alluded to, a term which has been very influential in framing contemporary European data protection rules.[143] However, for present purposes it is the symptom, not the cure, that deserves our attention. Furthermore, it is important to bear in mind throughout this discussion that the threats to 'decisional privacy' are not simply the result of the collection of intimate or sensitive details, rather the collection of details, period.[144]

The Panopticon and Power

In Jewish law, the doctrine of *hezzek re'iyyah* (injury caused by seeing) is a crucial backbone to privacy. The doctrine is framed by the recognition that protection is not simply needed to guard against unwanted observation, but to guard against the possibility of observation itself. This is because Jewish law has recognised that a person, uncertain of whether or not they are being observed, is likely to be inhibited and constricted in his actions.[145] Jeremy Bentham's Panopticon was based on just such a principle. By incorporating uncertainty of observation into the structure of the prison itself, Bentham felt that behaviour could be controlled and ultimately shaped.[146] For contemporary writers, Michel Foucault's critique of the Panopticon, and particularly his writings on power, have been especially instructive,[147] yet it is Reg Whitaker's reclassification of contemporary society as the 'participatory panopticon', that is most enlightening.[148] According to Whitaker it is the perceived benefits of the modern day decentralised panopticon - as discussed above - that set it apart from dystopian visions from the past. By emphasising the benefits of inclusion in the emerging panoptic

---

142 *Volkszählungsurteil* 65 BVerfGE 43 at II(1)(a) (*translated in* 5 *Human Rights Law Journal* (1984) 94, 100-101)

143 *See* Bygrave and Koelman, *supra* note 12, p. 70 and Stefik, *supra* note 12, p. 205

144 *See* fn.48 above. Also *see* Bygrave and Koelman, *supra* note 12, p. 64

145 An analysis of this doctrine is offered by Rosen. *See* Rosen, *supra* note 60, pp. 18-19. Also *see* Cohen, *supra* note 48, pp. 2034-2035

146 *See* Dinwiddy, *Bentham* (OUP: Oxford 1989), pp. 91-96

147 *See* Foucault, *Discipline and Punish: The Birth of the Prison* (Penguin: London 1991). pp. 195-228

148 *See* Whitaker, *supra* note 3, pp. 139-159

market, and by extension the disadvantages of exclusion, the dangers are glossed over, minimised and innocuously disregarded.[149]

Rosa Ehrenreich has recently attempted to redefine the potential zero privacy extension of this panoptic market as a power issue.[150] Privacy and power, she argues, are 'intimately bound up with each other',[151] it being 'no accident that absolute power demands absolute privacy for [oneself] and zero privacy for others'.[152] For Ehrenreich informational privacy lies on the same continuum as more conventional privacy issues, such as the disclosure of intimate details (labelled as 'privacy violations causing dignitary harm'[153]), but it is the *consequential* harm, or in keeping with the labels being used here, the ensuing impact on decisional privacy, as opposed to an*y inherent* harm, that distinguishes the two.[154] Thus to view privacy here as a predominantly dignitary interest is to miss the subtle interference that power can have on an individual's freedom to choose. Power is deliminative of the point where persuasion becomes an undue influence,[155] and whilst we sometimes profess to value the attention, the parameters of profiling are ultimately set by corporations to answer corporate needs.[156] It is only with an appreciation of this structural significance that we can address the resulting threats.

---

149 *Ibid* pp. 139-146 ('now when the panoptic gaze addresses or interpellates subjects, it is on the basis of understanding their needs and serving their desires', p. 144) Also *see* Cohen, *supra* note 48, p. 2038 (suggesting that this not only shapes our behaviour but our contemporary perception of privacy itself) and Samarajiva, 'Interactivity As Though Privacy Mattered' in Agre and Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press: Cambridge 1997), p. 302 (the same: offering the routine collection of social security numbers in the USA as an example)

150 *See generally* Ehrenreich, 'Privacy and Power' 89 *Georgetown Law Review* [2001] 2047

151 *Ibid* p. 2058

152 *Ibid* p. 2060

153 *Ibid* p. 2055

154 *Ibid generally*. Ehrenreich formulates this idea without expanding upon it, however it serves a useful starting point for the discussion to follow here.

155 *See, e.g., Royal Bank of Scotland -v- Etridge (No. 2)* [1998] 4 All ER 705, p. 712 ('The equitable doctrine of undue influence ... is brought into play whenever one party has acted unconscionably in exploiting the power to direct the conduct of another ...')

156 *See* fn.141above

Resulting threats

Whilst the United States does not have a comprehensive regime of data protection as in the EU, several areas have been deemed important enough to warrant specific attention. Crucially, the schemes in question address the industries involved in the distribution of information, such as libraries,[157] cable television,[158] and video rental stores.[159] Data such as these can be regarded as deserving special attention for two main reasons. Firstly, it can reveal an individuals association with particular beliefs, views, causes and organisations and secondly because reading[160] 'contribute[s] to an ongoing process of intellectual evolution'.[161] Thus the proliferation of monitoring technology, and particularly DRMSs, as will be demonstrated below, threaten to impose a type of control over individuals that may ultimately impinge upon the mental faculties of self-definition, creativity, and differentiation. The following section examines this claim.

James Madison, a key figure in the drafting of the First Amendment to the US Constitution, once famously wrote that '[k]nowledge will forever govern ignorance; and a people who mean to be their own Governors, must arm themselves with the power that knowledge gives'.[162] If, as Madison urges, we are to arm ourselves with the benefits of knowledge, then a right to read must necessarily be viewed as a natural precursor to the right to speak.[163] Indeed in an atmosphere as dynamic as cyberspace, readers and writers alike are perpetually immersed in an organic cycle of knowledge creation, elaboration and, ultimately, reconstruction. Thus, as Julie Cohen has persuasively argued, 'the creation of at least some speech in cyberspace ... reflects the

---

157 This is addressed at state level. For a list of these measures *see* Cohen, *supra* note 84, p.1031-1032, fn.213

158 Cable Communications Privacy Act 1984 47 USC § 551

159 Video Privacy Protection Act 1988 18 USC § 2710

160 'Reading' here denotes all forms of information consumption including reading, viewing and listening.

161 Cohen, *supra* note 14, section IV.B

162 *Quoted in* O'Neil, 'Libraries, Liberties and the First Amendment' 42 *Cincinnati Law Review* [1973] 209, p. 220

163 *See* Ault, 'The FBI's Library Awareness Program: Is Big Brother Reading Over Your Shoulder?' 65 *New York University Law Review* [1990] 1532, p. 1540; Froomkin, *supra* note 59, pp. 498-499; and Lessig, *supra* note 3, p. 105. Also *see generally* Rifkin, *supra* note 3, pp. 138-140

combined efforts of both authors and readers'.[164] Viewed this way, it is easy to regard the right of free speech as encompassing the right to read.[165]

The right to read *anonymously* has, however, been harder to ascertain. It may be that the issue is not controversial at all, merely new. Hence, the relative inefficiency of monitoring technology may have, up until now, provided the 'protection' that law has thus far failed to make explicit.[166] Furthermore, the accountability argument that can be levelled at speakers who wish to remain anonymous does not apply to readers, whose mere act of reading cannot cause harm.[167] Nevertheless, the closest a court has come to affirming a right to read anonymously is the US Supreme Court decision in *Lamont -v- Postmaster General*[168] which struck down a rule requiring post offices to refuse to deliver foreign-mailed communist propaganda unless the addressee specifically requested it. However, this case can be viewed along more traditional First Amendment lines by regarding the condition (specific request), as opposed to any resulting restriction, as unconstitutional.[169] Nevertheless, in the case Justice Clark noted that the condition was very likely to have a 'deterrent effect' on the ability of individuals to choose what they read,[170] a comment that highlights the potential dangers in mandating monitored reading: the 'chilling effect'.

The essence of the so-called 'chilling effect' is that rules should be designed to avoid deterring people from engaging in legitimate conduct.[171] Implicit in the classic account of the problem is a realisation

---

[164] Cohen, *supra* note 84, pp. 1005-1006

[165] *See, e.g., Board of Education -v- Pico* 457 US 853 (1981) ('the right to receive ideas is a necessary predicate to the recipient's meaningful exercise of his own rights of speech, press and political freedom', at p. 867)

[166] *See* Cohen, *supra* note 84, p. 1012; Froomkin, *supra* note 59, p. 504; and Nissenbaum, *supra* note 47, p. 578

[167] The accountability argument states that society has a legitimate interest in redressing harm caused by speech, and implies identification of speakers as a prerequisite. *See* Froomkin, *supra* note 59, pp. 404-405

[168] 381 U.S. 301 (1965)

[169] *See* O'Neil, *supra* note 162, p. 218

[170] 381 U.S. 301 (1965), 307

[171] *See generally* Schauer, 'Fear, Risk and the First Amendment: Unravelling the "Chilling Effect"' 58 *Boston University Law Review* [1978] 685

that speech on the margins of legality - where it may be most needed[172] - is hindered through fear of punishment by an imperfect legal system.[173] When it comes to reading, notions of imperfect law enforcement don't apply, yet the principle holds firm by extension: the reading of fringe material that the majority of the public are resistant to is deterred through monitoring,[174] and hence the decision by individuals to read such materials is abridged by external factors. It is submitted that such a result is damaging to the public discourse of a given society in itself, but, further still, that it can fundamentally affect the long term dynamics of choice and self-definition that are the mark of a free society. It is to this latter point that I now turn.

Andrew Shapiro's Internet commentary *The Control Revolution* has a chapter entitled 'In Defense of Accidents'.[175] Here he laments the loss of unintended consequences- those random encounters in life that can affect us profoundly- in an age when our experiences are 'plotted' in advance.[176] When it comes to expression, the dangers in 'talking only to the like-minded' have been noted by some,[177] however, for the purposes of articulating the impact on decisional privacy, this threat has to be rephrased. Human interests seem to fluctuate on a whim. This facet of our personality may at times be infuriating, but it characterises our complexity and reduces our predictability. Short term and long term goals constantly shift in and out of focus as we react to something as innocuous as the weather. Robert Post has stated that privacy plays a vital role in safeguarding these 'uniquely individual aspects of self',[178] whilst Edward Bloustein has suggested that privacy guards our

---

172 *See* Cohen, *supra* note 84, p. 1007 (suggesting that public discourse in politically and socially controversial issues is 'most sacrosanct'). Also *see generally* Sunstein, *Republic.com* (Princeton University Press: Princeton 2001), pp. 23-50

173 The word 'imperfect' here merely relates to the fact that, in Schauer's words, 'the law often makes mistakes'. *See* Schauer, *ibid*, p. 694

174 The opinions of the public at large should not be underestimated here, and although the 'punishment' may be less tangible, it 'penetrat(es) much more deeply into the details of life ... enslaving the soul itself': *see* Mill, *On Liberty* (Penguin: London 1985), p. 63

175 *See* Shapiro, *supra* note 20, pp. 197-207

176 *Ibid* p. 198

177 *See* Froomkin, *supra* note 59, p. 413; Rifkin, *supra* note 3, pp. 54-55; and Volokh, *supra* note 3, p. 1849 and *see generally* Sunstein, *supra* note 172.

178 Post, *supra* note 33, p. 2095

individual wants against conformist pressure.[179] The ability of external actors to capture *and act upon* our influences at any given point threatens to extend the present at the expense of the future. Thus the danger lies not in talking only to like minded individuals, rather in *noticing* only the 'like'.[180]

3.4 *The Privacy Implications of DRMSs*

DRMSs such as those outlined in section 2 are not inherently privacy invasive, rather they have a staggering *potential* to impinge upon the informational and decisional aspects of privacy described above.[181] Few developers deliberately set out to diminish the privacy and autonomy interests of consumers, instead these effects tend to emerge as a subtle by-product of the immediate benefit that a given technology offers.[182] With DRMSs, however, this side affect is positively endorsed by many vendors who trumpet the marketing possibilities their systems offer as a valuable return on investment.[183] InterTrust for example states that a benefit of its RightsSystem is that the '[c]onsumer experience is transparent',[184] whereas RightsMarket extols the fact that '[a]ccess to your real-time sales, customer and usage reports [is] only a click away'.[185] These possibilities are, according to Gervais, 'a key issue in discussions between rights holders and access providers',[186] discussions

---

[179] *See* Bloustein, 'Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser' 39 *New York University Law Review* [1964] 962, pp. 1000-1007

[180] Also *see generally* Raz, *The Morality of Freedom* (OUP: New York 1986), pp.203-207 (casting autonomy as an ultimate value contingent upon 'having a sufficient range of acceptable options', p.205) and Sunstein, *supra* note 172, pp. 107-110 (arguing that freedom is contingent upon the shape and form of social institutions)

[181] *See* Cohen, *supra* note 84, pp. 983-989 and Bygrave and Koelman, *supra* note 12, p. 65

[182] *See* Garfinkel, *supra* note 2, pp. 82-83 (offering examples of automatic toll collection systems for bridges in the USA and the extent and types of personal information that is generated as a result)

[183] This can be viewed as a product of DRMSs being introduced initially at the publisher end of the supply chain as opposed to the consumer end.

[184] *See* <http://www.intertrust.com/main/products/rights_system2.html>. Also *see* <http://www.elicense.com/clients4.asp> (detailing how ViaTech Technologies *eLicense System* 'benefits digital product marketing managers') and <http://www.microsoft.com/windows/windowsmedia/wm7/drm/benefits.asp> (Microsoft states that through its system 'the license acquisition process allows companies to gather targeted customer information') [all sites visited 13/03/02]

[185] *See* <http://www.rightsmarket.com/rightspublish.htm> [site visited 13/03/02]

[186] Gervais, *supra* note 6, section 'Interactive Transmissions'

which, it is suggested here, are conspicuous for their absence of consumer representation.

To demonstrate the potential privacy implications of DRMSs I shall return to the example of Sara and the Online Law Journal from section one. I shall follow this with an analysis of the individual components of the system that threaten user privacy. Here the focus is on the client side of the technology.

> Before the contents of each issue of the OLJ are encrypted, a descriptive piece of metadata called a Digital Object Identifier (DOI) is inserted into each section of every article, case note and book review in the journal. All DOIs are globally unique and the level of content granularity (i.e. every article, every section or every paragraph) to which they are applied is determined by the publisher. The result is that the encrypted data in the content module is linked to pieces of identifying metadata, that remain with the content when it is distributed.
>
> Each time Sara accesses paid-for content from the OLJ via her DocuReader she is online. From Sara's point of view this is important as it allows her to follow hotlinks directly to source material and related content. For the OLJ this enables the internal clocks of the licensing module and Sara's DocuReader to be synchronised, thus ensuring that time controlled access (for example a 3-day 'View Only' usage right) expires at the correct time. Furthermore, the integrity of the rendering device in question is validated using a 'challenge-response' protocol initiated by the licensing module. Here the licensing module challenges Sara's system to identify itself, by way of a digital signature, for the purposes of verifying access on that *particular* device.
>
> Whenever Sara manipulates the content using her DocuReader (e.g. 'Open' Smith article; 'View' conclusion; 'Print Section') the ContentControl element sends a data packet to the licensing module. This packet comprises of the DOI and details of the action taken by Sara. These data packets are stored in a logging program within the licensing module itself.
>
> By accessing the licensing module the publisher can easily compile aggregate statistics for content usage or view the profile of a specific user by matching the appropriate audit trails contained in the logging program with information stored in the identities database. This leaves the publisher of the OLJ with a detailed portrait of Sara's use of the content and an open channel for the marketing of 'suitable' content.

From this description four points emerge which combine to 'describe' us in detail and offer vendors the opportunity to influence our

consumption choices in the future. These aspects of a DRMS are *granular object labelling*, *online system use*, *usage tracking* and *marketing channels*.

3.4.1 *Granular Object Labelling*

Imagine downloading the latest computer game on your DRM enabled games platform. After vanquishing the final enemy boss you sit down to enjoy the end game sequence only for a pop up window to appear offering you extra levels to explore at a discounted price. Such a scenario is made possible within a DRMS via a flexible method for labelling discrete game modules. Thus, as the gamer enjoys his reward, the games system sends data on the most recently accessed game segment to the client server (see 'Usage Tracking' below) which - noting that the game has been completed - issues the 'extra levels' promotion.[187] An emerging standard for this type of identification scheme is the Digital Object Identifier (DOI). The DOI is a culmination of several years of research in America and elsewhere aimed at establishing a generic standard for content identification.[188] The stated aims of this research included the development of a standard that could apply to content of any type, on any device and to any degree of granularity.[189] These aims have, in the main, been met by utilising the DOI as a flexible *structure* for identification as opposed to an identifier *per se* and by enabling individual publishers to construct the precise form of the label themselves.[190] Currently the adoption of the DOI standard has advanced furthest in the field of online book and journal publishing,[191] yet its universal adoption remains in doubt. Nevertheless, a means for remotely identifying specific segments of content will pervade the industry so long as it enables strict control over usage.

---

[187] Another example can easily be envisaged. Say a player is having real trouble getting past a certain point in the game, a DRMS could "realise" this computationally and automatically offer access to an online players guide for a small fee.

[188] *See generally* Gervais, *supra* note 6; Rosenblatt et al., *supra* note 6, pp. 109-114; and <http://www.doi.org/> for information on the current status of the standard

[189] *See* Rosenblatt et al., *supra* note 6, p. 109

[190] This means that different labelling schemes, such as the ISBN or the ISSN, can be amalgamated within the DOI standard without necessarily being replaced.

[191] *See* Rosenblatt et al., *supra* note 6, p. 268

3.4.2 *Online System Use*

When DRMSs are used in an off-line environment, issues of both security and usability emerge. Mark Stefik has outlined a number of 'attacks' that can be made on DRMSs when off-line, including the simple act of tampering with a system's clock to avoid the expiration of time limited license.[192] Furthermore, when off-line the issue of transferring rights to different, and possibly new, devices becomes convoluted and cumbersome as the attributes of every usage right for every possible device have to be determined in advance.[193] DRMSs can be designed to overcome these difficulties by way of online system clock synchronisation and through the real-time granting of permissions for new or previously undefined uses. Finally, secure digital payment mechanisms, be they credit/debit cards or emerging forms of eCash, usually require online verification for security purposes.[194]

Broadband 'always on' connections into the home are gaining popularity throughout Europe and the United States as prices fall, and in the future mobile broadband will allow for the permanent networking of *all* devices.[195] As this infrastructure emerges it seems increasingly likely that the DRM industry will dispense with off-line distribution/usage models all together in many contexts.[196]

---

[192] *See* Stefik, *supra* note 12, p. 75 (also noting that 'most computers do not have tamperproof clocks')

[193] *See* Kumik, *supra* note 8, p. 15 and Rosenblatt et al., *supra* note 6, pp. 86-88.

[194] Whilst this was not an issue in the OLJ example given here, many people believe that real-time micro payments for content are a prerequisite for the acceptance of digital content distribution. Such solutions, named 'eCash', have an inherent 'double spend' problem which usually necessitates online transaction verification. *See generally* Chaum, 'Achieving Electronic Privacy' *Scientific American* Aug. 1992, p. 96 and Froomkin, *supra* note 59.

[195] *See* Stefik, *supra* note 12, pp. 33-40. In the US mobile phone operators are under a legal duty to be able to pinpoint *at all times* the location of phones for emergency purposes: *see* Garfinkel, *supra* note 2, p. 233.

[196] *See* Healey 'On a PC Near You - Downloadable Films' *latimes.com* Feb. 20th 2002 via <http://www.latimes.com> (noting that many video-on-demand services are only available for those with a broadband network connection) and Boulton 'RealNetworks' RealOne Goes Gold' *internetnews.com* Mar. 5th 2002 via <http://www.internetnews.com> (highlighting some of the advantages that subscribers to RealOne receive if they are connected via broadband)

3.4.3 *Usage Tracking*

The International Federation of Reproductive Rights Organizations (IFRPO) has described an ideal DRMS as being capable of 'detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on', resulting in a 'captured record of what the user actually [does]'.[197] As a World Wide Web Consortium working paper from January 2001 recognises, this captured log can be very valuable, often more so that the object whose use is being monitored.[198] This logging is made possible in a DRMS by specifying access rights in a computer-interpretable way.[199] From here it is a simple step to usage tracking. A foundational standard for building rights specifications is the Extensible Rights Markup Language (XrML) which offers components for defining the structure of rendering, transport and derivative work rights.[200] Crucially, for present purposes, XrML contains a 'track' function, which can be attached to any usage right. The track function details what information to send to a logging program and when it is to be sent. Thus, rather than regarding usage tracking as an afterthought in the operation of a DRMSs, it can be embedded within the process of accessing a digital work itself.

3.4.4 *Marketing Channels*

The term 'disintermediation' is often applied to the Internet to convey the idea of a global marketplace where we, as individuals, can deal directly with publishers and rights-holders.[201] DRMSs can be viewed as an enabling architecture in this process. However, by creating a direct link between producers and consumers, the economic interests of the former may well hinge upon the *secondary use* of data concerning the latter.[202] Rosenblatt et al. suggest that the 'killer app' of a DRMS may be

---

197 *Quoted in* Greenleaf, *supra* note 21, section 'Copyright-protecting Technologies'. Also *see* Bygrave and Koelman, *supra* note 12, pp. 108-109 (describing the monitoring of non-commercial private use of copyrighted works as 'unprecedented')

198 *See* Vora, Reynolds, Dickinson, Erickson and Banks, 'Privacy and Digital Rights Management: A Position Paper for the W3C Workshop on Digital Rights Management' January 2001 available at <http://www.w3.org/2000/12/drm-ws/pp/hp-poorvi.html> section 2

199 Section 2.2 above

200 *See generally* Rosenblatt et al., *supra* note 6, pp. 114-121 and <http://www.xrml.org/about.asp>

201 *See generally* Shapiro, *supra* note 20, pp. 53-59 and 142-149

202 *See* Greenleaf, *supra* note 21, section 'Privacy Issues in ©-tech and ECMS'

its use as a marketing tool,[203] a view, as shown above, that is supported by many in the industry. But, in a world where 'seven multimedia mega-groups control most of the global media',[204] this marketing effort is potentially extensive and pervasive.[205] What's more, when these companies also control the architecture for transmission, access to particular content can be preferred by a network which is, in the eyes of the consumer, neutral.[206] Or in the words of Larry Lessig: '"Policy-based routing" replaces the neutral "best efforts" rule'.[207]

3.5 *Legal Protection for DRMSs*

At the heart of Bentham's Panopticon lies the following paradox: any mechanism designed to produce control via coercion is only sustainable through first having perfected control itself. Put simply, why would the prisoners in the Panopticon unconditionally accept the uncertainty of observation, would they not - being the sort deemed to require controlling - simply break out from the panoptic gaze before their behaviour could moulded?[208] This principle can be extended to DRMSs because the control offered through copy protection mechanisms is susceptible to being broken by a determined 'cracker'. Indeed, it only requires one successful crack before the 'solution' can be broadcast world-wide over the Internet to anyone willing to listen. This, according to Bruce Schneier, means that any method of copy protection will ultimately fail.[209]

In recognising this salient point, stakeholders in the publishing industry have long been petitioning for the *legal protection* of DRMSs *per se*.[210]

---

[203] Rosenblatt et al., *supra* note 6, p. 178

[204] Castells, *supra* note 3, p. 191. Furthermore, these global corporations tend to have joint ventures with one another: *see* Rifkin, *supra* note 3, p. 221 ('the ten largest global media companies have, on ... average, joint ventures ... with six or more of the other companies')

[205] *See generally* Klein, *No Logo* (Flamingo: London 2001) pp. 143-164; Lessig, *supra* note 3, pp. 116-117; Rifkin, *supra* note 3, pp. 177-182, 219-223 and 248.

[206] *See* Lessig, *supra* note 3, pp. 159, 165-166

[207] *Ibid* p. 156

[208] *See generally* Whitaker, *supra* note 3, p. 32-45

[209] *See generally* Schneier, *supra* note 30. Here the promulgation of the DeCSS decryption tool is a prominent example.

[210] *See generally* Samuelson, *supra* note 14 and Samuelson, 'Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to Be Revised 14 (1999) *Berkeley Technology Law Journal* 2 available at

Such measures were eventually embodied in two WIPO treaties in the mid-1990's,[211] which are to be implemented in the EU through Chapter III of the Copyright Directive.[212] Article 6(1) of the Directive states that EU member states are to provide legal protection 'against the circumvention of any effective technological measures', a provision which certainly encompasses a DRMS like the one outlined above.[213] Similarly, the manufacture, distribution or advertisement of any device whose primary purpose is the circumvention of technological measures is prohibited.[214] Finally, and most significantly, Article 7(1) prohibits the removal or alteration 'without authority' of 'rights-management information' from a copyrighted work if in doing so the 'person knows, or has reasonable grounds to know, that by so doing he is [permitting] an infringement of *any* copyright or any rights related to copyright as provided by law ... .'[215] Rights-management information (RMI) is defined in Article 7(2) as:

> 'any information provided by rightholders which identifies the work ... the author or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.'

Whilst the provisions in Article 6 protect the overarching nature of copy protection technology itself, it is suggested here that from a privacy perspective the provisions in Article 7 are of more significance. The net effect of this provision would appear to be that any tampering with the

---

<http://www.law.berkeley.edu/journals/btlj/articles/14_2/Samuelson/html/reader.html> pp. 528-534

211 The WIPO Copyright Treaty 1996 Articles 11-12 and the WIPO Performances and Phonographs Treaty 1996 Articles 18-19

212 Directive 2001/29/EC. The associated provisions in the US are contained in the Digital Millennium Copyright Act 1998 17 USC §512 [hereinafter DMCA]

213 Art 6(3) ('the expression "technological measures" means any technology, device or component that ... is designed to prevent or restrict acts ... which are not authorised by the rightholder ... [they] shall be deemed "effective" where the use ... is controlled by the rightholders through application of an access control or protection process, such as encryption ... .'). Also *see* section 2 above and *see generally* Waelde, *supra* note 6, section 2.5

214 Art 6(2). Whilst the generic term 'devices' was used here, the actual wording of the Directive is 'devices, products or components or the provision of services'. A provision that would appear to cover everything apart from the DIY cracking prohibited in Art 6(1).

215 Emphasis added

granular object labelling aspect or the *usage tracking* aspect of a DRMS is illegal as the data involved can be classified as types of RMI, specifically 'information ... which identifies the work' and 'information about the terms and conditions of use' respectively.

It is true that tampering with *usage tracking* RMI *solely* for the purposes of safeguarding ones privacy[216] could be interpreted as failing the 'without authority' criteria,[217] or the second limb of the Article 7(1)(a) test, namely that of tampering to allow infringement of any of the owners rights. However, it is submitted here that the issue is not clear cut. The actual rights of the owner include, through Article 4(1), '*any form* of distribution to the public'.[218] It could plausibly be argued that through the double use of the word 'any' in Articles 4(1) and 7(1)(a), the decision by a publisher to apply a track function to a usage right, intrinsic as it is to the right itself,[219] is at first permissible under Article 4(1) and secondly, legally enforceable under Art 7(1)(a). This argument is reinforced if one considers that data sent to the logging program via the track function may not *in itself* be personally identifiable. The data will invariably say "what" was done and "when", but the "who" element may only be derived *later* when the audit trail from the logging program is matched with information in the identities database.

What remains clear is that Article 7 of the Copyright Directive, however narrowly construed, is open for interpretation, a fact that will make implementation in the UK a thorny and keenly debated matter.

---

[216] Section 1202(c) of the DMCA specifically defines 'copyright management information' (the equivalent to RMI) as excluding 'any personally identifying information about a user of a work'. By contrast, in the Directive, the explicit threat to privacy posed by the use of RMI is noted but relegated to a recital. *See* Recital 57 of the Copyright Directive

[217] According to the European Commission the word 'authority' can refer to permission from the rights-holder or as derived from law. *See* De Kroon, 'Protection of Copyright Management Information' in Hugenholtz (ed.), *Copyright and Electronic Commerce: Legal Aspects of Electronic Copyright Management* (Kluwer Law International: London 2000), p. 254. If this is read in conjunction with Article 9 of the Copyright Directive, which states that 'this Directive shall be without prejudice to provisions concerning in particular ... data protection and privacy ...', then a strong case can be made for the lawful tampering of RMI to protect ones privacy.

[218] Emphasis added

[219] *See* section 3.4.3 above

3.6 *Summary*

Here then is a summary of the privacy implications of Digital Rights Management systems. In the age of digitisation, tight control over works is necessary for risk averse companies, who, engaged as they are in a commercial arms race, seek the maximum return on investment from such systems. Individual profiling is an easy step in this direction and can be seamlessly incorporated into the schematics of a DRMS itself.

Protection, in the broadest sense, for DRMSs is multilayered. Foremost is the general invisibility of digital data processing operations, which helps to construct the second layer: the apparent public endorsement of the benefits offered by personalisation. This construction, however, is a flimsy one: RealNetworks' GUID demonstrates how easily passive acceptance can give way to public outrage if the veil of invisibility is cast aside and 'privacy' is mentioned. Yet, for those with the know-how to disable these monitoring functions, the final layer - that of legal protection - stands in the way.

DRMSs as construed represent the ultimate form of 'push' technology in a manner which threatens to cast individuals as a likely means of satisfying the ends of another. Combined with a reactive link between behavioural 'conformity' and observation, and one can postulate a move towards a society in which cognisable choices are mainstream-centric and where individual abstractions, predilections and eccentricities are at first eroded and eventually subsumed.

In the end, the issue can be reduced to one word: context. DRMSs can offer publishers the "what", the "when" and the "where" of individual propensities, but they fail to ask "why". It is submitted here that any solutions to the problem outlined in this section must, at their core, address this principle of contextualisation.

4. Pre-Existing Solutions

4.1 *Introduction*

Michael Froomkin has commented that data protection rules and anonymity are each powerful tools 'to combat the compilation and analysis of personal profile data'.[220] Likewise Directive 95/46/EC, whilst predominantly concerned with the establishment of legal data protection rules, encourages the development of technical measures to

---

[220] Froomkin, *supra* note 59, p. 398

enhance privacy.[221] The aim of this section is to examine how these complimentary approaches to privacy protection may impact upon the informational and decisional aspects of privacy threatened by the development of DRMSs. Throughout this discussion regard should be had of two crucial points that emerged in section 3. Firstly, whilst all transactions conducted through a DRMS generate data, the vast majority of this is likely to be mundane and innocuous 'facts' pertaining to an individual. Secondly, any resultant privacy threat does not arise upon collection of data *per se*, rather it emerges over time as data is used. By keeping these notions close at hand one should be able to demonstrate how legal and technical solutions as presently construed fail to adequately deal with the privacy implications of DRMSs.

4.2 *Data Protection*

In the United States, academic debate has tended to address the question of the nature of the individuals interest in personal data,[222] whereas in Europe there exists a clear conception of the interest as the fundamental right to informational privacy.[223] The question therefore turns to how this interest manifests itself under the new data protection regime. Peter Blume has cautioned against being 'impressed by the drafting of formal rules' because the devil lies in the details of practical application.[224] In taking heed of such advice, this section attempts to demonstrate the frailties inherent in the regime as applied to an industry with its own legitimate interest (enforcement of copyright) and characterised by multiple innocuous transactions. A word of caution from the outset. Presently, one of the greatest areas of concern in the field of data protection law is in the transfer of data to countries outside the EEA, so-called 'transborder data flows'. The Directive prohibits such flows unless an 'adequate' standard of data protection is in place in the country concerned and the EU has been in negotiation with several countries to determine how this standard is to be implemented.[225] My concern is not with this debate despite its

---

[221] Directive 95/46/EC Article 17 and Recital 46

[222] *See generally* Cohen, *supra* note 141; Safier, *supra* note 119; Samuelson, *supra* note 42; and Walker, *supra* note 42,

[223] Section 3.2.1 above

[224] Blume, *supra* note 45, section 3. Also *see* Simitis, *supra* note 61, pp. 451-452 (commenting that many of the compromises reached during the formulation of Directive 95/46/EC lessen the privacy protection it offers)

[225] *See generally* Charlesworth, *supra* note 37, and Schwartz, 'European Data Protection Law and Restrictions on International Data Flows' 80 *Iowa Law Review* (1995) 471

tremendous significance at a time of global media conglomeration, although it should be borne in mind when analysing any aspect of informational privacy.

4.2.1 *The Data Protection Act 1998*[226]

General

Under the Act the processing of personal data by a data controller (or data processor on their behalf) must conform with the eight data protection principles. From this starting point the details unravel. 'Personal data' within the Act means data relating to a living individual who can be identified from the data itself or in conjunction with other data in the data controller's possession.[227] This is a broad definition which would likely encompass encrypted or anonymised data within a DRMS, such as a GUID, which could at some point be cross referenced with data in an identities database, such as an e-mail address.[228] 'Processing' is a wide term encompassing 'obtaining, recording or holding the information or data or carrying out any operation or set of operations on the information or data'.[229] Such a wide definition self-evidently covers the operation of a DRMS which at a minimum obtains and records data to ensure compliance with usage rules and for billing purposes.[230] A 'data controller' is a person who 'determines the purposes for which and the manner in which any personal data are, or are to be, processed'.[231] The word 'determines' in this definition would suggest that the role is assumed by the party who exercises factual control over the processing of data, namely the client implementing a DRM solution.[232] It is this party that is obliged to ensure that the operation of the system conforms with the data protection principles.

---

226 Hereinafter 'the Act'

227 Section 1(1)

228 *See* Bebbington (2001), *supra* note 13, and Bygrave and Koelman, *supra* note 12, pp. 71-73. Also *see* Smith, *Internet Law and Regulation* (Sweet & Maxwell: London 2002 3rd ed.) §7.022-7.023 (noting the view taken by the Information Commissioner)

229 Section 1(1)

230 On the breadth of this provision *see* Lloyd, Ian *Information Technology Law* (Butterworths: London 2000 3rd ed.), §5.15-5.17 and Smith, *supra* note 228, §7.024

231 Section 1(1)

232 *See* Bygrave and Koelman, *supra* note 12, pp. 73-74 (also noting the possibility of multiple data controllers)

Data Protection Principles

The principles are contained in Schedule 1 of the Act and are summarised here:

1. *Processing shall be fair and lawful*
2. *The processing shall be for specified and lawful purposes*
3. *The data shall be adequate, relevant and not excessive in relation to such purposes*
4. *The data shall be kept accurate and up to date*
5. *Data shall be kept for no longer than the specified purposes require*
6. *Processing shall be in accordance with the rights of the data subject*
7. *Measures shall be taken to ensure the integrity and security of the data*
8. *Transborder data flows shall occur only if there an adequate level of protection within the country in question*

In the discussion to follow no reference will be made to principles four and seven as they relate to the quality and integrity of data as opposed to its actual collection and use, and principle eight for the reason noted above.

Processing is deemed *fair and lawful* if the data subject consents to the processing having been given information as to the type of processing intended by the data controller.[233] This information must be given at 'the relevant time' which is regarded as the time when processing first takes place.[234] In a DRMS the most likely time to ensure compliance with this principle is through the use of a license containing an opt-out check box for nonessential purposes (e.g. direct marketing) during the registration phase. Sensitive data - that being primarily of relevance, data consisting of information as to racial origin or trade union membership; regarding religious or political beliefs; or concerning physical or mental health[235]- may well be processed by a DRMS when a consumer acquires usage rights to copyrighted works of a certain theme. The issue is not clear cut and any link may well be too remote, in the sense that my purchasing the Bible in e-book format is merely

---

[233] On consent *see* Schedule 1 Part I para.1 and Schedule 2 para.1. On notification of types of processing *see* Schedule 1 Part II para.3

[234] Schedule 2 Part II para.2. Also *see Innovations (Mail Order) Ltd. v Data Protection Registrar* Case DA/92 31/49/1

[235] Section 2

suggestive of my racial origin and not determinative of it.[236] Nevertheless, one might argue that irrespective of the actual nature of my racial origin, any DRMS that predicts the answer, whether rightly or wrongly, and responds through the flavour of its marketing effort should be regarded as processing sensitive data. Thus to be on the safe side the data controller should ensure that such processing only occurs following *explicit* consent from the data subject.[237] Meeting such a requirement would require the inclusion of an opt-in check box for this type of data processing during the registration phase or through a separate procedure prior to the processing.[238]

The *specified and lawful purpose* principle can be easily met by a DRMS data controller who follows the guidance above in relation to information disclosure *or* who discloses the types of use that will be made of data to the Information Commissioner under the Act.[239] From this it may appear that the mere act of registration under the Act will suffice, but when examined in conjunction with the fair and lawful principle it becomes apparent that consumer notification is a paramount principle of and by itself.[240]

The *adequacy* and *time limitation* principles are both a direct corollary of the 'specified and lawful purpose' principle, in that the quantitative and temporal aspects of data collection and retention must derive from the actual use of the data. The Act offers no further guidance on the issue but two points can be postulated here. Firstly, for a purpose such as direct marketing data is gathered as a resource to help shape a profile and thus the principles are somewhat redundant at least whilst the commercial relationship exists.[241] Secondly, within a DRMS, records of what has been purchased may be kept indefinitely for restoration

---

[236] *See* Bygrave and Koelman, *supra* note 12, p. 79

[237] Schedule 3(1)

[238] *See* Bygrave and Koelman, *supra* note 12, p. 80 (suggesting 'formally separate process' be initiated prior to the processing of sensitive data) and Lloyd, *supra* note 230, §7.10-7.12

[239] Sections 16-18 and Schedule 1 Part II para.5(b). Also *see* Cate, *supra* note 64, p. 435

[240] *See, e.g., British Gas Trading Ltd. v The Data Protection Registrar* (reported in the 15th report of the Data Protection Registrar). Also *see* Bygrave and Koelman, *supra* note 12, p.83 ('the [registered purposes] must *also* be notified to the data subject' [emphasis added])

[241] *See* Bellotti, 'Design for Privacy in Multimedia Computing and Communications Environments' in Agre and Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press: Cambridge 1997), p. 93

purposes in the event of, for example, a hard disk failure or the need to authorise usage rights across differing devices.[242] Satisfying this purpose may not require highly detailed usage records in many circumstances but one can envisage a situation - say, if the extent of a usage right is defined in terms of the total number of uses allowed - where this may be necessary.

The *rights of the data subject* principle is expanded in part II of the Act which sets out substantive rights alongside remedies for non-compliance. Here the interest is with the former. Of relevance includes the right of access to personal information in an intelligible form - along with information about its use, source, subsequent disclosure, and the logic behind any wholly automated processing - within forty days of such a request and upon payment of a fee;[243] the right to prevent processing for the purposes of direct marketing;[244] and the right to ensure that no decision that significantly affects the individual is made by way of a wholly automatic process.[245] Such rights must be instigated by the data subject in the form of a written notice (satisfied by one in electronic form[246]) to the data controller, and as such DRMS operators need to ensure that procedures are in place to facilitate compliance.

Exceptions

Alongside consent, Schedule 2 of the Act contains a number of provisions which may legitimise many types of data processing within a DRMS.[247] Most importantly, if the processing 'is necessary ... for the performance of a contract to which the data subject is a party', then it is considered fair and lawful.[248] This provision is not relevant to a user license which explicitly states that processing shall occur as this a manifestation of the consent principle. Rather, if the license is silent on the matter (the details perhaps being contained within a privacy statement on the vendors web site), processing could nevertheless be

---

[242] *See, e.g.,* RightsMarket Demo 'Our Privacy Policy' online at <http://demo.rightsmarket.com/>

[243] Sections 7-8. The maximum fee is set at £10 by the Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000, SI 2000/191, reg. 3

[244] Section 11

[245] Section 12

[246] Section 64

[247] The exceptions discussed here do not apply to the processing of sensitive data

[248] Schedule 2 para. 2(a)

legitimised under the guise of guaranteeing compliance with the usage rights as defined in the license.[249] The nature of this exception turns on the word 'necessary' which in other contexts has been strictly interpreted by the European Court of Human Rights to mean close to essential.[250] Here it is useful to introduce a subtle distinction between the possible ways in which a DRMS operates. In the OLJ example used thus far, the user license, when generated, is sent to and stored on the end-users computer. Here the 'performance of the contract' occurs wholly within the confines of such a computer, without the need for the transmission of any details concerning usage to an external location. Therefore, it is suggested, such transmissions would never satisfy the necessity criteria. However, in an attempt to address the usability issue of permissions across multiple platforms,[251] emergent DRMSs often keep the license stored at a central repository, namely the clients server, which is contacted for permission by a rendering device when work is accessed.[252] In such a system the contract is effectively performed across the network, and it becomes possible to construe the transmission of usage information as an essential feature of the systems normal operation.

The second relevant exception is for processing which is 'necessary for the purposes of legitimate interests pursued by the data controller ... except where the processing is unwarranted ... by reason of prejudice to the rights and freedoms or legitimate interests of the data subject'.[253] The issue here is really one of balance and it is likely that recording usage for an essential trading activity such as marketing initially lies firmly on the side of the data controller's interest.[254] The point at which this exception becomes unwarranted is likely to depend upon the quantity of the data being processed, the range of uses to which it is put, and the intrusiveness of any resulting marketing effort.

---

[249] *See generally* Bygrave and Koelman, supra note 12, pp. 116-118

[250] *See, e.g., Barthold v. Germany* (1985) 7 EHRR 383, 401-404 (holding that the caveat 'necessary in a democratic society' in Article 10(2) of the European Convention on Human Rights must be 'convincingly established', p. 403)

[251] Section 2.3 above

[252] *See generally* Kumik, *supra* note 8

[253] Schedule 2 para. 6(1)

[254] *See* Ustaran, 'Data Protection Regulation: The Challenge Ahead' 1997(3) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/dp/97_3ust/> section 2.3 (suggesting that the UK government treats core trading activities more favourably as a way of promoting electronic commerce)

4.2.2 *What's Wrong With This?*

The data protection regime outlined above should be commended for its clear conception of the value in informational privacy and the conscious attempts it makes at casting the individual as an actor within the process,[255] yet there is something deeply wrong with it. That something, I believe, is an imbalance in the bi-directional flow of duties and responsibilities between data controllers and data subjects. Consider the following: for a DRMS operator to process data for marketing purposes the majority of his principle obligations under the Act are be met upon registration with the Information Commissioner, the placement of a notice (or at least a link to the notice) on the front page of the system explaining the intended processing, and the inclusion of an opt-out check box in the user license. Conversely, each and every individual who merely wishes to examine data used to construct a profile must initiate a written request for access which may only be granted upon the payment of a fee and a potential wait of forty days. Furthermore, this whole process is conditional upon an awareness of the processing itself and preliminary to any act of getting data modified or erased.[256]

Of course, spanning this imbalance is the notion of data subject consent, without which the idea of individual pro-action becomes unnecessary. Thus a brief look at the mechanics of consent in context will sharpen the argument put forth.[257] The use of non-sensitive data under the Act is contingent upon the data subject not opting-out of the uses in question. In effect, the *default* position here is any registered use. Market-speak would have it that the precise nature of such default settings are irrelevant as an 'efficient' result would be bargained to by the parties.[258] However, this view is contingent upon factors that are rarely present: namely, perfect information and zero transaction costs.[259] Rather, the

---

[255] This latter point is directly derived from the German 'informational self-determination' case discussed above at section 3.3.3. For further discussion *see* Mayer-Schönberger, *supra* note 75, pp. 229-232

[256] Furthermore section 8(3) of the Act exempts the data controller from having to comply with repeated request for access unless there has been a 'reasonable interval' between such requests.

[257] *See generally* Sovern, *supra* note 77, and Kang, *supra* note 49, pp. 1246-1291

[258] *See generally* Coase, 'The Problem of Social Cost' 60 *Journal of Law and Economics* (1960) 1, pp. 6-8

[259] *Ibid* pp. 15-19

traditional view holds that the default rule should be set at that which the majority of the parties *would* have chosen if they could have costlessly planned ahead (the 'majoritarian default').[260] In light of the survey evidence above on the *specific uses* of personal information, a majoritarian default of any registered use could be viewed as uncontroversial.[261] However, in 1989 a seminal article by Ayres and Gertner offered a new perspective on the notion of such a default.[262] The authors argue that merely accounting for the costs imposed on those who contract around the default position is not enough, and instead the overall cost of the default position must include the burden imposed on those who would like to flip from the default but who, for whatever reason, *don't*.[263] The inclusion of this latter category of social 'costs' may fundamentally alter the paradigm of opt-in as a default. I use the word 'may' because this paper is not an empirical study, however a couple of points should at least sow the seeds of doubt.

We start by assuming DRMS operators want to utilise potential information flows for marketing purposes and that individuals hold a diverse range of - often uninformed - preferences. A default of any registered use creates little incentive for a data controller to fully inform the data subject of anything that may alter this position, especially when the information in question addresses such a thorny issue as privacy.[264] The legal obligation to notify obviously impinges upon this "ideal", but there are degrees of notification, and all that is suggested here is that the *degree of least information* is likely to be an attractive option for many data controllers.[265] What would be the implications of reversing the default to a position of opt-in? In this scenario if a data controller is to satisfy his goal of utilising personal data then the onus is on him to inform. Crucially this burden is slight because of the ease of communication.[266] Consider a DRMS with an open channel of

---

[260] *See* Kang, *supra* note 49, p. 1251

[261] Section 3.3.2 (text accompanying fns.130-138) above. Also *see* Blume, *supra* note 45, section 3 and Walker, *supra* note 42, paras. 44-50

[262] *See generally* Ayres and Gertner, 'Filling Gaps in Incomplete Contracts: An Economic Theory of Default Rules' 99 *Yale Law Journal* (1989) 87

[263] *Ibid* pp. 112-115

[264] *See* Kang, *supra* note 49, p. 1255 and Sovern, *supra* note 77, pp. 1072-1074

[265] Consumers are further disadvantaged in this regard owing to the sheer volume of comparisons and decisions they must compute. *See* Sovern, *supra* note 77, p. 1091

[266] *See* Ayres and Gertner, *supra* note 262, pp. 98-99 ('when the rationale is to inform the relatively uninformed contracting party, the ... default should be against the relatively

communication in which regular interactions occur as work is licensed. This is an ideal environment for information disclosure and the fostering of choice.[267] Alas, opt-out is not the preferred default under the Act, perhaps realising the fears of some that it is incapable of providing an organic model of protection capable of adapting to technological developments.[268]

With *fully informed* consent minimised, we return finally to the initial assertion that the Act represents an obligatory imbalance in favour of DRMS operators. Such an imbalance in effect consolidates the 'power as persuasion' argument made above,[269] by defining commercial interactions on the terms of the data controller. Yet, perhaps more fundamentally, it singularly fails to address the ideal of contextualisation being promoted here. The issue is reduced primarily to one of collection vs. non-collection through concepts like registration, notification, and the prevention of processing for marketing purposes. The individual may be part of the process, but he does not figure in the data use equation after collection has been mandated. It is the *use* of data that primarily impinges upon the dignitary interests of self-definition and intellectual freedom, and it is here where the Act is at its most tame.

4.3 *Anonymising Data Exchanges through Technology*

The possibility and desirability of anonymous transactions over the Internet has gained much credence over the last few years.[270] For some, this represents a counterbalance to the imponderable corporate

---

informed party', p. 98) and Kang, *supra* note 49, p. 1258

[267] This idea will be examined more thoroughly in Section 5

[268] *See, e.g.,* Safier, *supra* note 119, para. 96. Also *see* Opinion 7/2000 on the European Commission Proposal for a Directive of the European Parliament and of the Council concerning the processing of personal data and the protection of privacy in the electronic communications sector of 12 July 2000 COM (2000) 385 adopted by the Article 29 Committee on Nov. 2nd 2000 (advocating opt-in as a 'well-balanced and efficient solution', section 2)

[269] Section 3.3.3 (text accompanying fns.150-156) above

[270] *See generally* Cohen, *supra* note 84; Froomkin, *supra* note 59; Grijpink and Prins, 'New Rules for Anonymous Electronic Transactions? An Exploration of the Private Law Implications of Digital Anonymity' 2001(2) *Journal of Information, Law and Technology* available at <http://elj.warwick.ac.uk/jilt/01-2/grijpink.html>; and Long, *supra* note 60

pressure I have attempted to deconstruct in section 3,[271] whilst for others anonymity is nothing more than subterfuge for those with something to hide.[272] Regardless of one's persuasion, the Article 29 Committee established under Directive 95/46/EC has recognised an intrinsic benefit in anonymity noting that '(t)he ability to choose to remain anonymous is essential if individuals are to preserve the same protection for their privacy on-line as they currently enjoy off-line' and has recommended that most transactions for goods and services made over the Internet be possible anonymously.[273] One must immediately ask what is meant by anonymity here. Anonymity and privacy are different concepts meaning that the perfection of the former does not automatically equate to the perfection of the latter. Nevertheless, anonymity is often regarded as an adequate solution to privacy conundrums thrown up by the Internet. Anonymity addresses identification whereas the privacy interest under discussion here concerns choice. The possibility of shaping choices exists independently of the capacity to identify those whose preferences are being moulded, consider television advertising for example. This simply means that privacy violations can occur irrespective of whether a system identifies us by our actual name or via a unique identifier such as an IP address or a pseudonym.[274] Of course, the intrinsic value in anonymity reveals itself across multiple applications as third party aggregation of multiple data sources is made immeasurably harder. The focus here, however, is on self-contained DRMSs and thus the concept of anonymity needs to be reconfigured to address not whether data generated through a system *identifies* a certain individual but rather how the data *relates to* that individual.

4.3.1 *Pseudonymity and 'Nyms'*

The German Teleservices Data Protection Act 1997 states that teleservice providers shall offer the user anonymous or pseudonymous 'use and payment' options to the 'extent technically feasible and reasonable'.[275] Similarly, in concluding her review of the value of built-in anonymity safeguards within DRMSs, Julie Cohen has stated that

---

[271] *See, e.g.,* Froomkin, *supra* note 59, pp. 407-408

[272] *See, e.g.,* Walker, *supra* note 42, paras. 69-77

[273] *See* 'Recommendation 3/97 Anonymity on the Internet' adopted by the Article 29 Committee on 3rd December 1997

[274] *See* Safier, *supra* note 119, para. 126

[275] §4(1). An English language version of the Act is available at <http://www.iid.de/iukdg/iukdge.html#a2>

'protection ... should recognise that initial collection of reader identity data may occur, but should require copyright owners to preserve an anonymous payment option for readers who desire it'.[276] These observations serve as a basis for a possible technical solution to the privacy dangers outlined. Suppose that when registering with a DRMS the user is assigned two pseudonyms (or 'nyms'), call them nymA and nymB. NymA is static in the sense that the personal information to which it relates concern only operationally necessary matters such as content delivery and billing. In its most basic form this could simply mean a credit card number.[277] NymB meanwhile is dynamic. The details to which it relates encompass those to which nymA is linked alongside data accumulated over time such as content preferences and usage. When a work is purchased a check box appears asking whether it is nymA or nymB that is to be assigned to that particular piece of content.[278] If nymA is selected then the establishment of a concrete link to an identifiable individual is only permissible if operationally necessary (i.e. for billing) or if required by law (i.e. upon the serving a police warrant). At the same time pseudonymous monitoring of usage is permissible so that DRMS operators or third parties receive what is effectively an anonymised aggregate of data to use as they see fit.[279] Alternatively, if nymB is the preferred option then the monitoring potential of a fully fledged DRMS can swing into action and begin (or continue) the construction of a user profile for marketing or promotional efforts.

4.3.2 *A Step Forward?*

Several commentators have suggested that for electronic commerce to prosper, systems must incorporate safeguards akin to the dual nym

---

[276] Cohen, *supra* note 84, p. 1037

[277] It is likely, however, that most DRMSs would require more information than this. In the hypothetical example of Sara and the OLJ used in this paper information as to Sara's status as a student was necessary. Also, at present the most popular way of delivering electronic books is by sending the customer, via e-mail, a link which leads to a download site. Clearly an e-mail address is functionally necessary in such a system.

[278] Clearly, some customers would find such a level of control annoying and hence a ubiquitous 'Don't ask me this again' check box could also be incorporated within the system.

[279] *See generally* Gervais, *supra* note 6, section 'Technology Issues' ('If [a DRMS is] correctly designed, the system would return to rights holders aggregated information on use of his/her works' p. 13)

suggestion put forth here.[280] In effect, the argument is that a technical solution coded into the system itself is a better device for preserving privacy than any legal device such as a data protection regime. In light of Froomkin's observation that data protection laws work best when data controllers are few in number or operate in industries that are already highly regulated, such a view seems reasonable.[281] Indeed a system development process which includes privacy protection functionality from the outset has much to commend about it,[282] and with regards enforcement, the power of code - as DRMSs themselves demonstrate in the context of permitting usage of copyrighted works - is significant. But what of the values embedded within the system itself? Utilising techniques of pseudonymity is not much different from the opt-in / opt-out issue discussed above. A slightly higher degree of contextualisation occurs because each transaction relating to an individual can be either i) secret or ii) non-secret, but the problem remains of people engaged in a repetitive string of innocuous transactions and not valuing an abstract concept like anonymity.[283] Fundamentally the notion of anonymity belongs to a 'one-off transaction' model, which is ill-suited to a time when a customer *relationship* may be the most valuable business asset.[284] The main aim of any privacy safeguards should lie in contextualising the relationship itself as opposed to merely asking whether a relationship can be struck up.

---

[280] *See, e.g.,* Bygrave and Koelman, *supra* note 12, pp. 82-83 and Stefik, *supra* note 12, p. 222

[281] *See* Froomkin, *supra* note 59, pp. 490-491

[282] This claim is made in light of the point made above on the privacy invasive aspects of technology being a by-product of systems design (see text accompanying fn.182). Also *see* Cohen, *supra* note 48, p. 2044 ('privacy self-help technologies do not alter ... commercial and technological infrastructures, nor do they alter the process by which technical standards enter the commercial mainstream') and Directive 95/46/EC Recital 46 (urging that mechanisms for privacy protection be conceived at the design stage)

[283] *See* Opinion 1/98 on the Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS) [Working Document] adopted by the Article 29 Committee on 16th June 1998 ('A technical platform for privacy protection will not in itself be sufficient to protect privacy on the Web') and Cohen, *supra* note 84, pp. 998-999

[284] *See generally* Muther, *Customer Relationship Management: Electronic Customer Care in the New Economy* (Springer: Berlin 2002) and Rifkin, *supra* note 3. The shift from the one-off model to the customer relationship model will be developed more fully in Section 5

5. Conclusions and Suggestions

Whilst the solutions examined in the previous section are flawed, and as such are incapable of sustaining an adequate counter-thrust to the dangers inherent in DRMSs, they contain the seeds for a more appropriate and robust manner of protection. The final section of this paper expands this claim by developing two separate strands of argument, the first built upon notions of what intellectual property in the digital arena actually represents and the second through observations on the data/knowledge conundrum highlighted above. In merging these strands it is hoped that a coherent and logical answer to the questions posed in earlier sections of this paper will have been developed which can serve as a starting point for those whom regard privacy protections as an integral part of DRMS development.

* * *

Esther Dyson believes that the value in much intellectual property is no longer the content itself, rather it is derived from the attention consumers pay *to* it.[285] The dynamics of this shift are simple: content production and distribution have greatly reduced barriers to entry in the digital environment; demand (as measured in the time available for consumption) has largely remained the same; value derives from exploiting the scarcest resource; therefore value no longer derives from content but via its use. In effect, Dyson argues, business models should adopt a relational perspective of content as merely one aspect of a larger 'intellectual process'.[286] The most prominent example of this shift is the distribution of software for free over the Internet because of the 'network effects' generated through a large installed user base.[287] The goal here becomes the creation of a lasting relationship through which value added services are offered. The challenge for DRMS operators, therefore, is to find new ways of adding value to the simple process of distribution[288].

---

[285] *See generally* Dyson, 'Intellectual Value' *Wired* July 1995 and Dyson, *supra* note 101, pp. 131-163. Also *see* Rifkin, *supra* note 3, pp. 85-91 (reflecting on this shift in all areas of commerce: 'In a sense, the product becomes more of a cost of doing business than a sale item in and of itself', p. 86)

[286] Dyson, *supra* note 101, p. 156

[287] 'Network effects' are the change in the benefit, or surplus (and by extension, value), that a distributor derives from a good when the number of people consuming the same kind of good changes. Prominent examples of 'free' software distribution in this regard are 'Hotmail' from Microsoft and 'Netscape Navigator' from Netscape. For an introduction to the concept *see* Randsell, 'Network Effects' *Fast Company* Sept. 1999 via <http://www.fastcompany.com>

[288] This is precisely the issue currently gripping the music industry. The proliferation of decentralised music download sites post-Napster has merely heightened this necessity.

This is not to suggest that all content will ultimately be free - such an assertion would render much of the previous discussion mute - rather it points to a future in which contracts (or licenses) for goods and services are inverted. Here, the sale of a book will no longer end when Sara successfully completes her download. Instead, corrections, 'click-through' references, online readings, and auto-updates may all come to represent what 'buying a book' actually means.[289] The point is this: for businesses, engaging customers in an interactive dialogue may be the only way of guaranteeing loyalty in a 'buyers market'.

Many businesses understand the significance of this observation, and have responded accordingly. The collective range of responses is often grouped under the heading Customer Relationship Management (CRM).[290] At worst CRM systems should be regarded as nothing more than a basic tool for direct marketing, but if fully utilised they offer businesses an unparalleled opportunity to converse with consumers at all phases of a relationship.[291] Features such as twenty-four hour service, graphical representations of data, price comparisons, user-friendly comments and complaints forms, online access to account information, and user discussion forums all form part of this process.[292] Where all this becomes relevant, however, is through the observation that DRMS *already include* much of the necessary technical infrastructure to incorporate CRM feature sets. Thus as one team of industry experts has observed, 'some DRM packages may have their own modest CRM functionality'.[293]

* * *

See generally Kelly 'Where Music Will Be Coming From' *New York Times* Mar. 17 2002 via <http://www.nytimes.com> and King 'New Song: Subscriptions, Plus' *Wired News* Feb. 4th 2002 via <http://www.wired.com/news/>

[289] *See* Rifkin, *supra* note 3, pp. 203-208 (distinguishing regular text as a product and hypertext as a process) and Volokh, *supra* note 3, pp. 1823-1826 (describing the features of a 'Cbook')

[290] For an introduction to CRM *see generally* Muther, *supra* note 284, and Davis and Harvey 'Time to Talk' *NewMediaAge* Apr. 18th 2002 via <http://www.newmediazero.com>. Predictably, the digital subset of CRM is termed eCRM.

[291] *See* Muther, *supra* note 284, pp. 12-17

[292] *Ibid* pp. 24-43

[293] Rosenblatt et al., *supra* note 6, p. 223

In the view of this author, data collection *per se* under DRMSs is not a concern of an order of magnitude comparable to that of how the data is subsequently used.[294] In other words: *in this context* the conception of 'privacy as dignity' appears muted when viewed alongside the conception of 'privacy as freedom'.[295] It has only been possible to construct such a clear distinction recently, but within a DRMS the mere collection and storage of routine transactional information relating to an individual via a wholly automated process and involving no human interaction, would seem to discount the possibility of a dignitary interest arising because dignity is necessarily a communitarian component derivative of the respect afforded between individuals, not between an individual and a machine.[296] Nissenbaum has suggested that there is a 'distinction between exposing something for observation ... and yielding control over it',[297] and it is submitted that it is upon this axis that the flaws in data protection regulations or technology for pseudonymity, discussed above, reside.

Section 12 of the Data Protection Act 1998 sets out a general rule (subject to a number of exceptions) that 'individuals [may] require that no decision taken by ... the data controller which significantly affects that individual is based solely on the processing by automatic means of personal data [relating to] the data subject'. The word 'significantly' in this definition would clearly exclude most data processing within a DRMS,[298] but nevertheless the provision highlights how we find something disturbing, even unnatural about a system in which people are 'reduced to little more than a cipher'[299] through a mix-and-match scheme of variables within a standard profiles. Such a feeling would appear to stem from a lack of trust in any system without an embedded degree of intelligence. Or to put this another way: the ideal of

---

294 Furthermore, 'functionally necessity' *collection* of personal information within a DRMS could be interpreted broadly under the guise of fraud prevention. For example, the Distance Selling Directive (97/7/EC) might require detailed records of transactions be kept by a DRMS operator for evidential purposes under the 'fraudulent use' provision in Article 8 or the compliance provision in Article 11(3)(a).

295 *See* Section 3.3.3 above

296 *See* Post, *supra* note 33, p. 2092 ('dignity depends upon intersubjective norms that define the forms of conduct that constitute respect between persons')

297 Nissenbaum, *supra* note 47, p. 596

298 *See* Cate, *supra* note 64, p. 436 ('the decision must be adverse to the individual; the simple fact of sending a commercial brochure to a list of persons selected by a computer does not constitute an adverse decision' [footnote omitted])

299 Lloyd, *supra* note 230, §8.68

contextualisation is impossible when the parameters of operation are predetermined.

This observation has plagued the field of Artificial Intelligence (AI) for decades.[300] The term AI is a contentious one and in recent years more neutral labels such as 'expert systems' or 'knowledge systems' have been used instead. Stefik has observed that 'networks carry mostly data, not knowledge - low-level facts, not high level memes',[301] and 'without a context, it is not realistic to expect knowledge systems to integrate and effectively use a wide range of facts'.[302] In effect, Stefik's argument is that data *use* within a system requires a context which must be hand crafted externally. DRMSs are very good at collecting data, but they lack the intelligence necessary to interpret it at the most epistemological level.[303] The mutual benefits of risk aversion for companies and an enhanced level of 'privacy as freedom' for individuals would naturally accrue if systems' developers appreciated this.[304] The implication is that efforts to involve individuals in the entire loop of data processing operations are needed, rather than merely at the point where data collection begins.

Such efforts should primarily focus on establishing the individual as a first class participant in data processing. A recent W3C position paper on DRM sets out what this would entail, specifically:

> 'user authentication should not assume that the consumer would not wish to be anonymous; the consumer should be allowed to choose from a range of methods with different degrees of anonymity; ...

---

300 *See generally* Stefik, *supra* note 12, pp. 133-161

301 *Ibid* p. 150. A meme is a 'unit of cultural transmission' which facilitates the non-genetic replication of human culture: Dawkins, *The Selfish Gene* (OUP: Oxford 1989), pp. 189-201. In the present context, memes are what imbue data with a meaning.

302 Stefik, *supra* note 12, p. 154 . For a more optimistic outlook *see* Berners-Lee, *supra* note 24, pp. 191-215

303 Also *see* Berners-Lee, *supra* note 24, p. 186 ('Computers help if we use them to create abstract *social machines* on the Web: processes in which people do the creative work and the machine does the administration' [emphasis original])

304 *See, e.g.*, Bonabeau, 'Predicting the Unpredictable' *Harvard Business Review* Mar. 2002 109, p. 110 (advocating a 'bottom-up' approach when trying to predict behaviour by 'making each participant a distinct individual' which in turn helps to capture 'the heterogeneity of the real world')

> 'rights clearing should not assume that the consumer can be tracked to any degree; the consumer should be allowed to participate in the degree of tracking established;
>
> 'consumer profiles should be treated as consumer assets in the system'[305]

From this description it becomes clear that individual choice and involvement are prerequisites of participation, however, it is suggested that another principle is needed to complete the loop. *Consumers should actively participate in the construction and modification of profiles within a system*. This is the only way in which dispersed attitudinal and contextual privacy preferences can be properly accounted for.

This final principle is really an advocation of feedback. A recent study on individual perceptions of automated (or AI-based) personalisation of Web sites demonstrated 'overwhelmingly [that users] wanted to be in control of the filter' and that the initial effort required of users for customisation was not a significant barrier 'when they sense a real payback'.[306] Feedback can (and should) occur at all stages of data processing but the crucial nature of such feedback must be its cyclical nature.[307] Sara's interest in articles on privacy may not last, and at such a time she should be able to let the system know. Manuel Castells has noted that the explosive growth of the Internet was caused by a 'virtuous feedback between the diffusion of technology and its enhancement',[308] and the point here is a microcosm of this effect. For Castells multi-directional interactivity was a precondition of this development,[309] and likewise for Sara participation must be an option which is both diffused and 'always on'. Again, and it is worth reiterating, data collection is an aspect here, but it only one component of a larger scheme.

Providing consumers with preference options at all stages of the processing cycle is a start, but could the options themselves not also be determined by users? Recall that usage rights within a DRMS are

---

[305] Vora et al., *supra* note 198, section 2

[306] Nunes and Kambil, *supra* note 118, p. 34 (finding that 93% of those surveyed had customised at least one Web site, 25% having done so for four or more sites)

[307] For an overview of the elements in a data processing cycle *see* Bellotti, *supra* note 241, pp. 76-78

[308] Castells, *supra* note 3, p. 28

[309] *Ibid*. Also *see* Rosenblatt et al., *supra* note 6, p. 55 (suggesting that DRMSs can make 'negotiation' possible)

defined by a scripting language such as the Extensible Rights Markup Language (XrML).[310] As the acronym suggests, this is in turn a derivative of the Extensible Markup Language (XML), which offers a great deal of flexibility when it comes to labelling data. Tim Berners-Lee, the inventor of the World Wide Web, notes that XML 'allows anyone to create any kind of tag that can capture the intent of a piece of information',[311] and whilst standardisation and interoperabilty issues obviously abide, a great deal of focus in the computing industry is currently directed at making such rich semantic tapestries work.[312] If a users profile is supposed to mirror his individual propensities, then such a step is vital. A computer representation of an individual is a patchwork of discrete, externally defined, and static data elements, whilst human beings are not static creatures.[313] By allowing individuals to, in effect, participate in the process of defining data the gap between 'truth' and 'manufactured truth' can be minimised.

* * *

If these two chains of thought could be brought together through a DRMS, how might the system look? Here we return to the example of Sara and the Online Law Journal for the final time.

> Whenever Sara transacts with the OLJ she is given the option of whether the transactional level data can be added to her 'Reader Profile'. The check box is explicit in the sense that the default position is an informative option 'Tell Me More' - a link to a page describing how profiles are generated and used. If Sara declines the request, the usage tracking function does not send any data to Sara's specific entry in the logging program. Otherwise, such data collection is permitted. If Sara wishes, this process can be applied to each piece of content within a single transaction or the check box can be disabled for all transactions after an explicit choice of 'always profile' or 'never profile' is made.

---

310 *See* section 3.4.3 above

311 Berners-Lee, *supra* note 3, p. 173. Also *see* Dornfest and Brickley, 'Metadata' in Oram (ed.), *Peer-To-Peer: Harnessing the Power of Disruptive Technologies* (O'Reilly: Sebastopol 2001), pp. 191-202 ('Hopefully we'll see peer-to-peer applications emerging that empower both the content provider and end user by providing semantically rich environments for the description and subsequent retrieval of content. This should be reflected both in the user interface and in the engine itself.', p. 197)

312 For a concise introduction to the technical issues *see generally* Dornfest and Brickley, *ibid*

313 *See generally* Agre, 'Beyond the Mirror World: Privacy and the Representational Practices of Computing' in Agre and Rotenberg, *Technology and Privacy: The New Landscape* (MIT Press: Cambridge 1997), pp. 46-52

> Through her DocuReader Sara can view the data in her reader profile by clicking the 'My Account' button on the OLJ homepage. Here, every piece of content that Sara has bought and assigned to her profile is chronologically listed. Alongside each listing is information on the usage rights attached to the content (if any remain), a six point 'relevancy' scale, a 'remove from profile' button, and a 'comments' text entry box. At the top of the screen are two further options, the first being a 'How is this data used?' link and the second being an 'Editors Choice' check box with an opt-out default.
>
> The relevancy scale represents an opportunity for Sara to indicate how much weight should be attached to the particular content when she receives recommendations. The default position is three on a scale from zero to five. Selecting zero attaches no relevance to the content but is different from the 'remove from profile' option because it can be changed later.
>
> The comments box allows for more detailed preference indication if Sara wishes. Statements such as 'Everything by Author X' or 'Any piece by an American author that mentions the EU Copyright Directive' can be entered (or altered) at any time. This data is fed into the logging program which transforms the requests into metadata fields which are, in turn, matched to content metadata.
>
> Finally, so long as the feature is not disabled by Sara, editors choices are derived, not from Sara's individual data, but from aggregated information such as the content with the most user downloads or the content which has generated most comment in the user discussion forum.

Albert Bressand has remarked that 'the time has come to shift from the engineering approach of information technology ... to the human and relationship approach'.[314] In a similar vein, Jeremy Rifkin has argued that until recently cultures have necessarily preceded markets, because it is only through the tacit recognition of behavioural norms that trust can emerge as the foundation for commercial relationships.[315] The example above represents a conscious effort to recreate a trusting environment through a bi-directional process of information generation and disclosure.

* * *

---

[314] *Quoted in* Schwartz, 'R-Tech' *Wired* June 1996

[315] *See* Rifkin, *supra* note 3, pp. 11-12

Is it reasonable to place our faith in system designers alone to produce privacy enhancing technologies such as the one outlined? Probably not. The inertia of the status quo is likely to make such initiatives rare. Private ordering works well in a well-defined, close knit community of repeat players,[316] and whilst the new customer relationship approach to IP licensing may exhibit some of these characteristics to a degree, the media industry's size negates much of the immediacy of interdependence.[317] Rather, it is suggested, a legal backbone is needed to stimulate architectural remedies.[318]

The concept of 'informational self determination' embodied in European data protection law is, in principle, a wonderful answer to many of the dangers lurking at the intersection of informational and decisional privacy interests. However, as we saw, its present conception under the Act is woefully inadequate in the context of DRMSs.[319] A more appropriate conception would be to derive a sectoral Code of Practice from the framework legislation. This type of legal mechanism has been labelled the 'fourth generation' of data protection and is seen as a powerful tool for coping with the diversifying range of data processing methods.[320] Furthermore, it is endorsed in the UK under the 1998 Act.[321]

A Code of Practice should primarily focus on reconfiguring the right of access under the 1998 Act to a two way interactive environment, and on encouraging the development of user interfaces which nullify the significance default settings have in determining degrees of privacy. Furthermore, the Article 29 Committee should play a role in

---

316 *See* Cohen, *supra* note 84, pp. 995-998.

317 *Ibid*

318 Whilst reduced to a paragraph here, there is currently intense legal debate in the US over the merits of such a proposition. For the views of the chief protagonists *see generally* Lessig, *supra* note 14 and Post, 'What Larry Doesn't Get: Code, Law, and Liberty in Cyberspace' 52 (2000) *Stanford Law Review* 1439

319 On the difference between concepts and conceptions *see* Dworkin, *Taking Rights Seriously* (Duckworth: London 1977), pp. 134-136 (arguing that a fundamental principles at an abstract level are properly termed 'concepts' whose embodiment in a manner of behaviour or discrete rule are 'conceptions' of it)

320 Mayer-Schönberger, *supra* note 75, pp. 233-235. It is crucial here to appreciate the hierarchical predominance of general principles, thus 'under fourth-generation developments *general* data-protection norms are *supplemented* by specific sectoral ... regulations', *ibid* p. 233 [emphasis added].

321 Data Protection Act 1998 section 51

formulating such specifics, as it has already demonstrated its willingness to offer interpretative guidance on specific issues.[322] Indeed, the Committee has commented that in the area of Internet based software the data subject '[should] freely decide about the processing of ... personal data by offering user-friendly tools to filter (i.e. to reject or to *modify*) the reception, storage or sending of ... information'.[323]

Finally, care should be taken to avoid an analogous situation to that which emerged from early Internet defamation cases in the US.[324] If vanguard firms face a greater threat of prosecution by offering a higher standard of privacy protection, promising initiatives may stagnate. Here the non-binding nature of Codes of Practice under the 1998 Act may serve as an advantage, and compliance should be regarded, not as part of an exact determination as to whether a business has satisfied its obligations under the Act, but as a more abstract component of morality of business practices.[325]

* * *

We live today in a inter linked society where opting-out is not really a viable option. Instead, individuals should be able to shape participation on their own terms. This, in turn, may be the only way to relieve the burden from an overworked and underdeveloped principle of consent. DRMSs are based on a technological infrastructure that supports such participation and utilising it in the manner described is perhaps the best way of fulfilling Gervais' prophecy that DRMS themselves are 'probably the best tool'[326] to protect privacy.

---

322 *See, e.g.*, 'Opinion 1/2000 on certain data protection aspects of electronic commerce' adopted by the Article 29 Committee on 3rd February 2000

323' Recommendation 1/99 on Invisible and Automatic Processing of Personal Data on the Internet Performed by Software and Hardware' adopted by the Article 29 Committee on 23rd February 1999 , recommendation 4

324 *Cmp. Cubby Inc -v- CompuServe Inc* 776 F Supp 135 (SDNY, 1991) and *Stratton Oakmont Inc -v- Prodigy Services Co* 23 Media L Rep 1794 (NY Sup Ct, May 25 1995). It should be noted, however, that these cases are no longer valid law in light of the US Communications Decency Act 1996, 47 USC § 230

325 For initiatives in the US that seek to address the privacy issues discussed in this paper at an ethical level *see* Garfinkel, *supra* note 2, pp. 252-253 (suggesting that the concept of 'compilation copyright' might be 'extended to cover individual components of a person's life', p. 253) and Samuelson, *supra* note 42, pp. 1151-1159 (arguing that principles embodied in trade secret law could be adapted to afford individuals specific moral-based rights in their personal data)

326 Gervais, *supra* note 6, section 'Technology Issues'

As generations accustomed to the ubiquity of computer controlled environments come of age, never has the need been so pressing to educate and inform individuals about their rights and responsibilities in an information society. Relationships premised on a mutual trust form a large part of this society, and only through access to personal information and meaningful choice can trust properly flourish.