personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual or exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles.

Copyright, privacy and digital rights management (DRM)

DAVID LINDSAY AND SAM RICKETSON

The combination of tracking technology and online licensing on the one hand, and extra-copyright limitations based in privacy rights on the other, would in my opinion yield a better copyright regime than many national laws now afford with respect to the problem of private copying.

Jane C. Ginsburg

Introduction

The quotation from Jane Ginsburg provides a useful entry point into the subject of this chapter: the relationship between copyright law, privacy laws and the emerging phenomenon of digital rights management (DRM). There can be little doubt that the production and distribution of copyright-protected material in digital form has created challenges for its owners, in particular new horizons for seemingly endless forms of infringement by users. These challenges have, in turn, spawned DRM systems and technologies that are designed to deter infringement and facilitate management of rights in new and different ways and which may well provide copyright owners with more control over their material and over users than was possible in the non-digital environment. The phenomenon of ‘digital lock-up’ and the restrictions that this may place upon users of copyright material has already received much attention from policy-makers and commentators, but a matter that has received less consideration

This chapter arises from work done pursuant to an Australian Research Council (ARC) grant on online privacy.

1 'Copyright or "Infograh": Comment on General Report on Limitations Found Outside Copyright' in Libby Benck, Michael Green and Mary Wyborn (eds.), The Boundaries of Copyright, its Proper Limitations and Exceptions (Sydney: ALAI Study Days, Australian Copyright Council, 1999) p. 57.

2 For a detailed examination of these issues, see the various national reports and comments in June C. Ginsburg and June M. Beuck (eds.), Adjudicating and Alternatives to Copyright, Proceedings of the ALAI Congress, Columbia University, New York, 13–17 June 2001 (2002).
is the subject of the present chapter: the threat that the development of such systems may pose to the privacy of users.\footnote{For an analysis of the relationship from a Canadian perspective, see Ian R. Kerr, 'If Left to Their Own Devices ... How DRM and Anti-Circumvention Laws Can Be Used to Hack Privacy' in Michael Geist (ed.), In the Public Interest: The Future of Canadian Copyright Law (Ottawa: Irwin Law, 2005) pp. 167–210.}

This chapter begins with a brief overview of what is meant by DRM systems, and then considers the following matters: the relationship between copyright and DRM systems, and the extent to which the latter may promote or hinder accepted objectives of copyright protection; the relationship between DRM systems and the privacy of end users; and the broader relationship between copyright and privacy, with particular focus on how potential tensions between the objectives of copyright protection and the objectives of privacy protection may be resolved.

In the light of this analysis, we then address the question of whether or not there is a need for limitations on DRM systems (legal or otherwise) so as to ensure an appropriate balance between the objectives of copyright protection and the protection of end user privacy. In this regard, we maintain that different conclusions may be drawn, depending upon the perspective from which these questions are approached, namely a common law, utilitarian (or 'interests-based') approach (based on 'marketplace norms') and a civil law, rights-based approach (based on 'personhood norms').\footnote{This distinction draws on Geller’s contrast between ‘marketplace norms’ and ‘authorship norms’ in the copyright context: Paul Edward Geller, ‘Must Copyright Be For Ever Caught between Marketplace and Authorship Norms?’ in Brad Sherman and Alain Strowel, Of Authors and Origins (Oxford: Clarendon Press, 1994) pp. 159–201; Paul Edward Geller, ‘Toward an Overriding Norm in Copyright: Sign Wealth?’ (1994) 159 Revue Internationale du Droit d’Auteur (RIDA) 3. For other views on the contrast between common law and continental copyright traditions see Alain Strowel, ‘Droit d’auteur et Copyright: Between History and Nature’ in Sherman and Strowel, Of Authors and Origins, pp. 235–53; Kamel J. Koehnman, ‘Copyright Law and Economics in the EU Copyright Directive: Is the Droit d’Auteur Passe?’ (2004) 35(6) International Review of Intellectual Property and Competition Law 603.} On the first approach, authors and end users may be regarded as holding only ‘interests’, which are subsidiary to the promotion of social (economic) welfare. In contrast, on the second approach, authors and end users may be regarded as having ‘rights’ derived from the autonomy of persons and respect for human dignity. Although the characterisation of ‘rights’ and ‘interests’, and the relationship between the two, is notoriously complex,\footnote{For an overview, see Frances M. Kamm, ‘Rights’ in Jules Coleman and Scott Shapiro (eds.), The Oxford Handbook of Jurisprudence & Philosophy of Law (Oxford: Oxford University Press, 2002) pp. 476–513.} there is general agreement that a fundamental right, such as a right associated with the autonomous development of a person, will prevail over ‘interests’, such as interests in economic efficiency. Following from this, we conclude that the appropriate form of legal protection – including the potential application of laws to DRM systems – should depend upon whether authors and/or end users are regarded as having ‘interests’, which must be balanced with other ‘interests’, or as having ‘rights’, which will take precedence over mere ‘interests’.

### Digital rights management

Digital rights management is an imprecise term that can be defined in different ways. One definition is provided in a guide prepared by the Australian Department of Communications, Information Technology and the Arts, which states:

DRM is a term used to describe a range of techniques that use information about rights and rightsholders to manage copyright material and the terms and conditions on which it is made available to users.\footnote{Australia, Department of Communications, Information Technology and the Arts, A Guide to Digital Rights Management (Canberra: DCITA, 2002) http://www.dcita.gov.au/drm/.}

Insofar as this definition limits the term to techniques for protecting copyright material, it is too restrictive, in that DRM systems may also deal with rights in material that is not protected by copyright, including material which is now in the public domain through the expiry of copyright protection. A more satisfactory definition, proposed by Niels Rump, is that:

DRM covers the description, identification, trading, protecting, monitoring and tracking of all forms of usages over both tangible and intangible assets.\footnote{Niels Rump, ‘Digital Rights Management: Technological Aspects – Definition, Aspects, and Overview’ in Eberhard Becker, William Bulse, Dirk Gunneweg and Niels Rump (eds.), Digital Rights Management: Technological, Economic, Legal and Political Aspects (Lecture Notes in Computer Science Vol. 2770) (Berlin: Springer, 2003) pp. 3–15 at p. 4. Another useful definition of DRM is ‘the chain of hardware and software services and technologies governing the authorised use of digital content and management of any consequences of that use throughout the entire life cycle of the content. DRM is an access and copy control system for digital content, such that the DRM securely conveys and enforces complex usage rights rather than simple low-level access/copy controls ... These technologies include a range of functions to support the management of intellectual property for digital resources, such as expression of rights offers and agreements, description, identification, trading, protection, monitoring and tracking of digital content’: see Marimena I. Vague, IASTED International Conference on Communication, Network, and Information Security (New York, NY, 10–12 December 2003), available from http://www.iasted.com.}

DRM can therefore be properly understood as a series of functions designed to ensure the security of content in order for it to be capable of being traded. As Rump helpfully explains, DRM consists of two groups
of functions: the managing of digital rights (or 'management') and the
digital management of rights (or 'enforcement'). The functions relating
to the management of digital rights include identifying content, defining
rights in relation to that content, and defining rules about the way in
which that content may be exploited. The functions involved with digital
management of rights are those concerned with enforcing the defined
rules, including the tracking of content, restricting access to content, and
monitoring or restricting use of content.

Following Rump's classification, the typical components of a DRM
system are as follows:6

1. **Secure containers** designed to make content inaccessible, mainly by
means of encryption;

2. **Rights expressions** used to define those to whom access to the secure
containers is permitted;

3. **Content identification and description systems** used to uniquely identify
the content and attach metadata to the content;

4. **Identification** of people or organisations that intend to interact with the
content, usually by means of unique identifiers, so as to limit access to
authorised users;

5. **Authentication** of people or organisations that intend to interact with
the content, often by means of public key cryptography;

6. Means of persistently associating identifiers and other information to the
content, such as **watermarking**. Watermarking is a form of steganography,
namely the art or science of hiding secret information. Inserting
encrypted data into a file is a means of identifying that file, which corre-
responds to the forensic application of watermarks. The non-forensic
application of watermarks involves their use in ensuring compliance
with defined rules. For example, if consumer equipment does not detect
a watermark it may not perform the required functions.

7. A means of **reporting events**, such as payment for content; and

8. **Payment systems**, including credit cards and electronic cash.

It can therefore be seen that DRM systems comprise a set of tools that com-
prehensively define and manage the relationship between content owners
(of which copyright owners are a sub-set) and end users, including mech-
anisms for defining rights over content and mechanisms for enforcing
those rights. It is important to bear in mind that not all DRM systems

will incorporate all of the above functions or components, and that these
may also be combined and ordered in a variety of ways.

**Copyright and DRM**

Before the emergence of DRM systems, the legal relationship between
content owners and users was defined mainly by the substantive norms of
copyright law, in combination with contract law. Inevitably, these placed
limits on what users could do with content; but this was in a 'hard copy'
world, with all the attendant physical limitations on the control of con-
tent that this entailed. The advent of digital technologies and networking,
however, has given rise to a new policy dilemma: do such systems remain
consistent with, and advance, the traditional objectives of copyright pro-
tection, or do they now overreach these objectives?

In considering this issue it is helpful to review the purposes of copy-
right protection, and how these have been seen by different western legal
traditions, in particular by common law and civil law systems. While we
emphasise the clear differences, it is important to note at the outset that
there are also important similarities.

In broad terms, there are two ways in which the objectives of copyright
protection have been framed in western legal systems: first, by reference
to the notion of authors' rights, and secondly by reference to more instru-
mentalist or utilitarian concepts that view copyright protection as provid-
ing incentives for the production of literary and artistic works. The first
of these, which is characteristic of civil law jurisdictions, may loosely be
described as a 'rights-based' approach, in that it emphasises the rights of
authors in their works. The influence of the philosophers Kant and Hegel
has been seminal in this tradition, which received its most systematic for-
matulation in the writings of later German legal scholars, such as Gareis,
von Gierke and Kohler.5 In the civil law tradition, the rights of authors
have both an economic and non-economic aspect, the latter being called
'moral rights'.

The 'moral rights' of authors can be seen as part of the wider person-
ality rights attaching to individuals by virtue of their status as persons.
Indeed, this conception of authors' rights has led civil law jurisdictions
historically to draw sharp boundaries around authors and their creations

---

6 This classification of DRM components is a paraphrase of the classification proposed by
Nick Rump; see Rump, 'Digital Rights Management', above n 7, p 7.

---

5 See, e.g., Edward J. Darnich, 'The Right of Personality: A Common-Law Basis for the
Protection of the Moral Rights of Authors' (1988) 23 Georgia Law Review 1; Neil Netanel,
'Alienability Restrictions and the Enhancement of Author Autonomy in United States and
works and rights in relation to lesser forms of production of a more industrial or corporate kind that are described as 'neighbouring rights' (sound recordings, broadcasts, performances, and the like). Such notions of authors' rights are not completely unknown in common law jurisdictions, where the natural rights labour theories of John Locke, although somewhat different to the natural rights tradition in civil law jurisdictions, were clearly influential in such early copyright decisions as Millar v. Taylor,10 as well as resonating in the early copyright statutes adopted by the newly independent American colonies in the late eighteenth century. But, as explained below, natural rights theories have been much less important in the common law tradition than in the civil law tradition, where the notion of authors' rights has been pervasive.

Authors' rights theories encounter difficulties when the role of the positive laws embodying them is considered in its wider economic and social context. For example, what limitations, if any, are to be placed on the rights so recognised? How wide should rights extend and for how long? If the right in question is a natural right of property, for instance, why should not it be perpetual and universal? Furthermore, authors' rights theories, by definition, have no part to play when considering the scope and duration of neighbouring rights protection. Pragmatic considerations, even in civil law jurisdictions, have therefore always meant that there have been limitations placed on authors' rights that acknowledge a wider public interest in the dissemination and use of the works that have been created.

In contrast to the 'rights-based' tradition, copyright laws in common law jurisdictions have always had a predominantly utilitarian and instrumentalist character in which the grant of exclusive rights has been seen as an essential incentive for the creation and distribution of useful works, rather than as an acknowledgement by positive law of rights already existing in natural law. This notion was neatly encapsulated in the Preamble to the first English copyright statute, the Act of Anne (1709), namely:

An Act for the Encouragement of Learning, by vesting the Copies of printed Books in the Authors or Purchasers of such Copies, during the Times therein mentioned.

Under such an approach, the grant of rights was to be calibrated for the wider social purpose, the encouragement of learning, which clearly underlined the conditional and instrumental character of the rights conferred. Such instrumentalist analysis has become far more sophisticated since

10 (1769) 4 Burr. 2303; 98 ER 201.

activities. At the same time, neither of the approaches has ever envisaged that protection should be indefinite or infinitely extensible; it has always been accepted that they are subject to limitations. As Numa Droz, the distinguished Swiss delegate stated at the first of the Berne Convention drafting conferences in 1884, ‘limits to absolute protection are rightly set by the public interest’. In other words, regardless of whether a ‘rights-based’ or ‘interests-based’ approach is adopted, there is an ultimate need to strike a balance between authors and owners, on the one hand, and users, on the other.

The notion of the copyrightable, however, sits much more readily with the ‘hardcopy’ or analogue world where the nature of physical copies places ‘natural’ limits on what both owners and users alike may do. But the balance begins to shift, or even slide, as we enter the digital world, with its potential for perfect and endless reproduction and dissemination of copyright material, and confront what has been called the ‘digital dilemma’. At first blush this seems to present a problem, as the uncompensated copying of digital material that is now possible appears likely to undermine the traditional objectives of copyright protection: some intervention, legislative or otherwise, therefore seems to be called for to reassert the original balance.

Nevertheless, with every dark cloud there is a silver lining and, even without legislative correction, digital technologies carry with them the potential for exercising far greater control over the activities of users. In the words of one well-known commentator, Charles Clark, the ‘answer to the machine is the machine’. First, the ease with which digital information can be manipulated, such as by encryption, means that access or use of such material can be restricted to those with the necessary authority, such as a decryption key. Secondly, the attachment of ‘meta-information’ to digital material, such as identifying information, establishes the potential for access to, and use of, this material to be closely tracked and monitored. These two categories of response form the basis for all potential DRM systems and, as copyright owners have begun to explore these possibilities, copyright laws at the national, regional and international levels have come to their assistance with additional forms of protection.

This development has been relatively rapid, post-dating the adoption of the TRIPS Agreement in 1994. Separate policy processes at the national and regional level began at this time in such places as the United States, Europe, and Australia, and led, within a very short timeframe, to the adoption of the two WIPO ‘Internet Treaties’ at the Diplomatic Conference held in Geneva in December 1996. Included in these two instruments were two important new provisions that have specific relevance to DRM systems, namely provisions on anti-circumvention measures and rights management information (RM).

The first of these, contained in Article 11 of the WIPO Copyright Treaty and repeated, with necessary modifications, in Article 18 of the WIPO Performances and Phonograms Treaty, provides:

Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights under this Treaty or the Berne Convention and that restrict acts, in respect of their works, which are not authorised by the authors concerned or permitted by law.

12 In practice, these approaches have tended to reinforce each other.
16 Charles Clark, ‘The Answer to the Machine is the Machine’ in Bernt Hugenholtz (ed.), The Future of Copyright in a Digital Environment: Proceedings of the Royal Academy Colloquium (The Hague: Kluwer Law International, 1996). Goldstein points out that, in 1995, when Clark originally coined this term, he was more concerned with the ability of computers to provide new means for connecting authors to users than with allowing content owners to prevent unauthorised reproduction or distribution: Goldstein, Copyright’s Highway, above n. 14, p. 184.

20 Australia, Copyright Convergence Group, Highways to Change – Copyright in the New Communications Environment (Canberra: AGPS, 1994).
As for RML, Article 12(1) of the Copyright Treaty provides that:

Contracting Parties shall provide adequate legal protection and effective legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention:

(i) to remove or alter any electronic rights management information without authority;
(ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority.

It will be seen that both provisions provide for collateral forms of protection for copyright owners that are essentially directed at the new technological environment in which works and subject-matter are exploited. In other words, these two provisions set the international norms for national laws that apply to DRM systems.

As to the first, it will be seen that this is concerned with the actual technological measures that copyright owners may adopt to protect themselves against unauthorised uses and seeks to penalise actions taken by users to circumvent those measures. The international standard to be applied here is somewhat open-ended, leaving considerable flexibility for national implementation. For example, does it cover attempts to circumvent access control devices, bearing in mind that copyright owners’ rights do not include a specific right of access in the non-digital environment? Or is it limited to attempts to circumvent measures that limit use, such as copy controls? And can there be exceptions for certain kinds of circumventing activities, at least where these parallel activities would be allowed in the non-digital environment under the relevant copyright exceptions and limitations in national laws?

These are issues that have received differing responses at national and regional levels, and there has been much controversy as to whether such measures are really consistent with the traditional objectives of copyright

22 This issue, with the associated ambiguous drafting of the current Australian anti-circumvention provision, caused the Australian High Court considerable difficulty in the main Australian anti-circumvention case, Stevens v. Kabushiki Kaisha Sony Computer Entertainment (2005) 221 ALR 448.


The economic rationale for anti-circumvention provisions therefore bears some similarity to the rationale for trade secrets laws, which can be seen as minimising socially wasteful expenditure that would otherwise be incurred in a ‘war’ between owners attempting to protect secret information and intruders attempting to obtain the information. In fact, as Friedman et al. point out, an optimal trade secrets law must balance the relative social costs of keeping and discovering secrets, on the one hand, and the costs of a legal system for protecting secrets, on the other: David D. Friedman, William M. Landes and Richard A. Posner, ‘Some Economics of Trade Secret Law’ (1991) 5 Journal of Economic Perspectives 61. This suggests that, in assessing anti-circumvention laws, the costs of such laws should also be taken into account.

20 To an extent, Ginsburg was referring to this problem when she observed that: ‘Copyright owners have...have eye enhanced prospects for global earnings in an increasingly international copyright market. Accordingly, they have urged and obtained ever more protective legislation, that extends the term of copyright and interferes with the development and
This leads them to the conclusion that, from an economic perspective, the preferred form of anti-circumvention provision would ‘punish the use of circumvention technology only when it was used to infringe copyright, and not when the technology is used to restrict otherwise lawful uses. This distinction, while attractive, is something of a counsel of perfection that has proved difficult for national legislators to implement. The analysis of Landes and Posner also reinforces the difficulties involved in developing an adequate policy framework for regulating the use of technological forms of protection.

For the purposes of our present discussion, it suffices to say that the new provisions at international and national level dealing with circumvention measures are directed at protecting the exploitation of copyright material in the digital environment. They are concerned with guarding the gateways and exit points of the material that is the subject of DRM systems. To date, however, neither an approach based on protecting the dignitarian ‘rights’ of authors, nor an ‘interests-based’ approach, has proved capable of providing clear practical guidance as to the appropriate limits on laws prohibiting circumvention measures.

The provisions dealing with RMI, on the other hand, have a more obvious application to DRM systems themselves, being concerned with the identifying information that is added by owners and the knowing removal or alteration of that information. This is not directly concerned with users at all, but only with owners and their ‘electronic markings’; the requirement of knowledge and the need to link this to an infringing act is a significant limiting factor. Although more detailed than the anti-circumvention provision, implementation at national level does not appear to be particularly onerous.

More generally, it must be said that neither provision, nor their counterparts at national and regional levels, touches upon the potential impact that their application may have upon users of the copyright material that is so protected and marked, in particular with respect to the privacy of these persons. This is hardly surprising, as the provisions appear in treaties and laws concerned with the protection of authors and owners of copyright materials. But the digital environment gives rise to a potential conflict that was not entirely apparent in the hard copy world: the extent to which the privacy of end users may justify legal limits on copyright owners protecting their material in the digital environment. Before turning to this issue, however, we need to explain the relationship between privacy laws, especially data protection laws, and DRM systems.

Privacy and DRM

Privacy is acknowledged to be a complex concept, aptly described as ‘elusive’. While it is almost universally acknowledged that privacy is connected to the protection of human dignity and individual autonomy, there is wide-ranging debate among scholars and practitioners as to how best to define it. As a starting point, however, it should be noted that privacy is protected as a human right in several important international instruments. Thus, Article 17 of the International Covenant on Civil and Political Rights provides:

No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

And at the regional level, Article 8(1) of the European Convention on Human Rights (ECHR) provides that:

Everyone has the right to respect for his private and family life, his home and his correspondence.

None of these general statements, however, provides specific guidance as to the content of the concept of ‘privacy’. We therefore need to consider how this matter has been treated, in practice, by different legal traditions.

Here, as with copyright laws, it is possible to see two broad approaches: those that conceive privacy as a fundamental human right and those that view it in a more instrumentalist or ‘interests-based’ fashion. Again, the first of these is to be found more fully expressed in the civil law tradition,

---


while the second is more typical of common law jurisdictions. The two approaches may be considered in turn.

Continental traditions of privacy protection

The protection of privacy in France can be traced to concerns associated with the liberalisation of the press during the French Revolution. These concerns were concisely expressed by the French philosopher, Royer-Collard, in a well-known 1819 speech, in which he coined the phrase ‘private life must be walled off’.30 From the mid-nineteenth century, in a series of cases, French courts developed the concept of the ‘right to one’s image’ (droit à l’image), which was eventually formulated as a ‘sacred and inalienable right over ourselves, and consequently over the reproduction of our image’.31 From this time on, French courts continued to protect ‘private life’ against undue publicity, regarding privacy as a personality right.32 While this was initially protected through the application of general tort principles, in 1970 an express right to privacy was introduced into French law with the adoption of Article 9 of the French Civil Code, which provides that: ‘Everyone is entitled to respect of private life’.33

One commentator has recently noted that the early French approach to privacy protection developed in response to threats to traditional notions of honour posed by press freedom in the context of increased sexual liberation in mid-nineteenth-century France.34 According to this view, French privacy law effectively replaced duelling as the means of protecting the honour or dignity of a person whose privacy was invaded. In this sense, the general protection of privacy extended to all members of French society a dignitarian interest that was previously the preserve of the aristocracy.

By contrast, the German approach to privacy drew on a more systematic theoretical analysis that conceived of privacy as part of the complex area of personality law. Late nineteenth-century German personality law was the result of the application of German idealist philosophy, and especially Hegelian philosophy, to the Roman law of insult. On this approach, the law was seen in evolutionary terms as extending protection to intangible, non-economic interests. As Whitman has explained this development:

The modern world was now producing what Jhering called, in a famous 1885 article, the law of ‘insulting tortious injuries’. In particular, modern protections were now evolving beyond protections against immaterial verbal insults, to include the protection of such immaterial goods as one’s name and one’s photographed image, one’s control of one’s correspondence, as well as access to modern amenities such as the telegraph and tram.35

The German approach to privacy protection can be traced to much the same nineteenth-century jurisprudential tradition as the development of authors’ rights. Thus, while privacy was concerned to protect the personality of an individual against insult, authors’ rights were designed to protect the personality of the individual qua author as embodied in a particular literary or artistic work. Underlying the civil law tradition of both privacy and authors’ rights protection therefore, are concerns with the protection of the dignity (or honour), and autonomy, of the human subject.

In Germany, following the Second World War, in the case of privacy, this found expression in Article II of the Basic Law (Grundgesetz):

Every person has the right to free development of his personality, insofar as he does not injure the rights of others or offend against the constitutional order or the moral law.36

The constitutional protection of personality rights subsequently formed the basis for the development of German data protection law, especially in the decision of the German Constitutional Court in the 1983 Census case.37 That case concerned the German Census Act of 1983, which required the collection of detailed information for social planning purposes. The Constitutional Court held that, in certain respects, the legislation infringed provisions of the German Basic Law, namely Article I(1) which establishes the central constitutional value of human dignity, and the protection of personality rights under Article II. In recognition of the need for fundamental constitutional values to adapt to technological

31 This formulation was adopted in the famous case of Dumas c. Liebert, CA Paris, May 25 1867, 13 APIAL 247 (1867), cited in Whitman, 'The Two Western Cultures of Privacy', above n. 27, 1177.
33 Code civil [C. civ.], Art. 9 (Fr.).
34 Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1179–80.
35 Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1184 citing Rudolph von Jhering, Rechtsschutz gegen injuriöse Rechtsverletzungen (1886) p. 236.
36 Grundgesetz, Art. II, para. 1 (Ger.).
change, the Constitutional Court authoritatively formulated a constitutionally guaranteed 'right to informational self-determination', essentially meaning 'the authority of the individual to decide fundamentally for himself, when and within what limits personal data may be disclosed'. The decision therefore acknowledged that the preservation of human dignity and individual autonomy required a degree of individual control over data processing. In this respect, the court stated that:

... an individual must be protected against unlimited collection, storage, use and transmission of personal data... as a consequence of the free development of personality under modern conditions of data processing.

The approach adopted in the Census decision is an essential part of the conceptual background to the 1995 European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (the 'Data Protection Directive'), which established new benchmarks for the protection of personal data of European Union citizens. The Data Protection Directive approaches the regulation of data processing from within the European framework of fundamental rights and freedoms, thereby establishing a 'high level' of protection of personal data, treating this as a matter integral to the protection of the fundamental underlying values of human dignity and moral autonomy.

Common law traditions of privacy protection

Common law approaches to privacy protection have been more fragmented and pragmatic than in civil law jurisdictions. Until recently, English-influenced common law systems did not recognise privacy as an independent value deserving of protection in its own right. When faced

83 BVerGE 1 at 42 (1983). The 'right to informational self-determination' was prefigured in earlier decisions, including Microcensus, 27 BVerGE 1 (1989) and Divorce Records, 27 BVerGE 344 (1979).

As Eberle explains the decision: 'At the root of the Constitutional Court's decision was the vision that human dignity and autonomy must be preserved against the onslaught of the modern computer age'; Edward J. Eberle, 'Human Dignity, Privacy, and Personality in German and American Constitutional Law' [1997] Utah Law Review 963 at 1004.

84 BVerGE 1 at 43 (1983).


85 Thus, Recital (10) to the Directive states that: 'Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy... whereas for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community.'

with facts that raised issues relating to personal privacy, courts in such systems adopted the conventional practice of listing all causes of action that might incidentally protect privacy, then attempting to fit the facts within one or more of the listed actions. In the words of two distinguished comparative lawyers, contrasting the protection traditionally according to privacy under English common law with that under German law:

English law, on the whole compares unfavourably with German law... The harsh condemnation of English law, should be mitigated by the fact that many aspects of the human personality and privacy do receive some adequate protection through a multitude of existing torts and specific statutes... this means fitting the facts of each case in the pigeonhole of an existing tort, the process often involving strained constructions or, even, leaving deserving plaintiffs without a remedy.

Although English law failed historically to recognize an express right to privacy, the equitable action for breach of confidence was sometimes relied upon to restrain the publication of private material. Indeed, in one of the well-known early cases, Prince Albert v. Strange, Lord Cottenham LC went so far as to observe that 'privacy is the right invaded'. Moreover, following the introduction of the Human Rights Act 1998 (UK), the protection of privacy under English law has been transformed. Thus, in Campbell v. MGN Ltd, the House of Lords recognized a right to privacy, in the form of protection against the publication of private facts that fell within the expanded parameters of the action for breach of confidence. One way to interpret this development is as a creative, but potentially fraught, fusion of a 'rights-based' conception of privacy, reflecting the influence of the European Convention on Human Rights, with the traditional incremental approach of the English common law.

88 (1849) 1 Mac & G 23 at 47; 41 ER 1171.
89 (1849) 1 Mac & G 23 at 47; 41 ER 1171 at 1179. This statement was made in the context of the rejection of a contention that an injunction could not be awarded until the plaintiff had established proof of title to the property, Lord Cottenham LC pointing out that postponing the injunction would deny the plaintiff's right to privacy.
90 [2004] 2 AC 457.
92 Opened for signature 4 November 1950, 153 UNTS 221 (entered into force 3 June 1952). The continental approach to privacy has been influential in decisions of the European Court of Human Rights interpreting Art. 8; see, e.g., Von Hannover v. Germany (2005) 40 EHRR 1.
The protection of privacy by means of an extended action for breach of confidence under English law may be contrasted with the cautious recognition of a tort of public disclosure of private information under New Zealand law in *Hosking v. Runting*. In that case, a majority of the New Zealand Court of Appeal appeared to adopt a 'rights-based' analysis by referring to a 'shift in emphasis' in tort liability from liability for reprehensible conduct to the protection of identified rights. The New Zealand public disclosure tort, in turn, has clear parallels to much earlier developments in the United States, where aspects of 'privacy' have long been protected under the law of torts.

As is well known, the protection of privacy in the United States received its impetus from the seminal article of Samuel D. Warren and Louis D. Brandeis, entitled 'The Right to Privacy', published in the *Harvard Law Review* in 1890. Although the article cited many earlier English precedents, including *Prince Albert v. Strange*, it was also clearly influenced by late nineteenth-century German personality law, with the central argument in the article being that the proposed right to privacy and an author's rights over literary or artistic works had common roots in 'the more general right to the immortality of the person, the right to one's personality'.

Writing over 70 years after Warren and Brandeis, Prosser was able to categorise four species of privacy-protecting torts that had been developed by US courts in the intervening period: intrusion upon seclusion; misappropriation of name or likeness; public disclosure of private facts; and portrayal of the victim in a false light. Not all of these torts have flowered to full maturity in US law: most significantly, the importance accorded to the First Amendment protection for freedom of expression has rendered the public disclosure and intrusion torts all but illusory. But for our purposes, the influence of the civil law tradition on the initial recognition of privacy as a right under American common law is what is significant.

As Whitman suggests, 'it is best to think of the Warren and Brandeis tort not as a great American innovation, but as an unsuccessful continental transplant'. In an interesting modern parallel, we are now seeing a discernible civil law influence on contemporary developments in the English action for breach of confidence. It can therefore be seen that, while common law courts have sometimes loosely referred to a 'right to privacy', the recognition of privacy as a fundamental 'right' in the common law tradition has been partial at best and, where this has occurred, it has been influenced by conceptions of privacy drawn from the civil law tradition.

The differences between the common law and civil law approaches can also be seen in differences in the legislative reaction to the emergence of large-scale computerised databases in the 1960s and 1970s. Practical concerns that different national standards would inhibit the growth of transborder flows of personal data led to the development of data protection laws, marked by the adoption of the 1980 OECD Guidelines *Governing the Protection of Privacy and Transborder Flows of Personal Data* (the 'OECD Guidelines'). Since then, however, there has been a significant divergence in approaches to data protection laws, seen most clearly in the difference between the European and American approaches.

With its strong 'rights-based' background, the European Union adopted a 'high level' of protection in the 1995 Data Protection Directive. The United States, by contrast, has refrained from legislating comprehensively with respect to information privacy, instead enacting laws on an ad hoc basis to deal with problems as they have arisen in specific sectors. Data processing is therefore largely left to be regulated by the market or by industry self-regulation. As one commentator has explained, under the US approach:

Regulation is perceived to intrude on the commitment to freedom from government interference in information flows. As a result, law emphasizes regulation of the market process rather than the substantive contours of information privacy.

In other common law jurisdictions, such as Australia, data protection laws have been based on the standards established by the 1980 OECD

---

50 [2005] 1 NZLR 1.
51 Ibid. [2] (Gault P and Blanchard J).
56 Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1204.
Guidelines, which were a pragmatic attempt to balance the competing values of information privacy and the free flow of information. This can be seen, for example, in section 29(a) of the Privacy Act 1988 (Cth), which imposes a statutory duty on the federal Privacy Commissioner to 'have due regard for the protection of important human rights and social interests that compete with privacy, including the general desirability of a free flow of information . . . and the recognition of the right of government and business to achieve their objectives in an efficient way'.

In practice, we see a spectrum of approaches across jurisdictions to data protection, ranging from the strong, 'rights-based' approach embodied in the EC Data Protection Directive, to the US preference for relying on market forces rather than the law to protect personal information. But the main point is that legal systems drawing on the common law tradition, when compared with civil law systems, have tended to privacy more as an 'interest' than as a fundamental right, thereby providing weaker privacy protection.

How, then, do these different legal approaches impact on the use of personal information that may be collected through DRM systems?

Application of the two privacy traditions to DRM

Of the identified functions or components of DRM systems, the following may raise privacy concerns:

1. Identification and authentication of end users of protected content;
2. The reporting of events relating to access to, or use of, protected content; and
3. The rule sets as a whole, which define the conditions relating to access to, or use of, protected content.

The three main privacy-related concerns raised by these functions are, respectively:

1. The potential for unconstrained collection and processing of identifying information;
2. The potential for persistent surveillance and monitoring of end users of protected content; and
3. The potential for direct constraints to be imposed on the use of protected content, including restrictions on 'private' uses of content.

Each of these deserves further investigation.

Many DRM systems, like electronic commerce systems more generally, involve the collection and/or processing of information that relates to end users. This information may be collected or processed for purposes such as secure delivery of content, payment mechanisms, customisation or personalisation of content, or user profiling. Potentially identifying information collected by DRM systems takes a variety of forms. It may, for example, consist of credit card information, a digital signature, an email address, an Internet Protocol (IP) number or 'clickstream data'.

The identifying information may be collected or processed either with the knowledge of the end user, or without the end user knowing.

As explained above, the revolution in information processing made possible by the computer led to the development of data protection laws in the 1970s. There are two legal issues that arise in the application of data protection laws to information that is collected or processed by DRM systems:

1. The scope of the information regulated by the laws; and
2. If information is regulated by the laws, the nature of the rules, or principles, that apply to the collection and processing of personally identifying information.

The approach taken to these issues can be seen to depend upon whether a 'rights-based' or 'interests-based' approach is taken to the protection of privacy, and is well-illustrated by comparing the 'rights-based' EC Data Protection Directive with the predominantly 'interests-based' approach embodied in the Australian Privacy Act 1988.

59 'Clickstream data' may be defined as: 'A virtual trail that a user leaves behind while surfing the Internet. A clickstream is a record of a user's activity on the Internet, including every Web site and every page of every Web site that the user visits, how long the user was on a page or site, in what order the pages were visited, any newsgroups that the user participates in and even the e-mail addresses of mail that the user sends and receives'; see http://www.webopedia.com. An indication of the information trail left by internet users may be obtained from the sites: http://privacy.net/analyze/ or http://www.cnii.fr/uk/index.htm.

60 While the Preamble to the Privacy Act expressly refers to Art. 17 of the ICCPR, the substantive provisions of the Act appear to be based on the view that privacy is an 'interest' to be balanced with other interests. The 'interests-based' approach to data protection is confirmed by the terms of reference for the Privacy Commissioner's 2005 review of the private sector provisions of the Privacy Act, which refer to 'individuals' interests in protecting their privacy' and 'important human rights and social interests that compete with privacy'; Australia, Office of the Privacy Commissioner, Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988 (March 2005), Appendix 1.
First, the scope of data protection laws is set by the definition of ‘personal information’ (or ‘personal data’). Laws that adopt a ‘rights-based’ approach to data protection appear to have a broader scope than laws with an ‘interests-based’ perspective. Thus, the term ‘personal data’ is defined by the Data Protection Directive to mean:

... any information relating to an identified or identifiable natural person (‘data subject’); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.\(^{61}\)

The Australian Privacy Act, by contrast, defines ‘personal information’ as:

... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion.\(^{62}\)

Two potential problems have been identified with the Australian definition: it is not clear whether it applies to video images that are not directly referenced to other information identifying an individual; and it does not seem to apply to online information, such as an email or IP address, that does not identify an individual, but allows an individual to be contacted.\(^ {63} \) The first problem seems to be dealt with by the definition of ‘personal data’ in the Data Protection Directive, which expressly applies to information that may indirectly identify the data subject. The second problem is much more relevant to the potential application of data protection laws to DRM systems, which may well collect information that identifies an address or machine, but not the identity of an individual. In this respect, it can be noted that the European Union, in its 2002 Directive on Privacy and Electronic Communications,\(^ {64} \) introduced a form of prior notice and consent for the processing of online ‘tracking’ information that do not necessarily identify the data subject. To this effect, Article 5(3) of the Directive provides that:


A 2005 review of the Australian Privacy Act by a Senate Committee recognised that the definition of ‘personal information’ may need to be extended to deal with new technologies, while recommending that the issue be examined as part of a proposed future review.\(^ {66} \)

In our view, the proper scope of data protection laws should be determined on the basis of whether online privacy is conceived from a ‘rights-based’ or ‘interests-based’ perspective. From a ‘rights-based’ perspective, if information generated by a person online is seen as an expression of the person’s identity, there may be a ‘rights-based’ argument for conferring control over the information to protect the ability of the person to freely develop in the online environment, regardless of whether or not the person can be identified from the information.\(^ {67} \) If online privacy is regarded as an ‘interest’, however, other interests, including the interest of business in being able to freely process online information, and interests in ensuring the accuracy of information, must be given some weight in determining the scope of data protection laws. In that case, it may well be that the interests of business in contacting individuals will outweigh the interests of individuals in being free from unsolicited online communications.

\(^{65}\) Transposed into UK law by Regulation 6 of the Privacy and Electronic Communications (EC Directive) Regulations 2003 (UK). The justification for the requirement is set out in Recital 24 to the Directive which provides, in part, that: ‘Terminal equipment of users of electronic communications networks and any information stored on such equipment are part of the private sphere of the users requiring protection under the European Convention for the Protection of Human Rights and Fundamental Freedoms’.


\(^{67}\) This is part of the broader set of issues relating to identity online, sometimes referred to as the ‘digital persona’ or ‘digital identity’: see, e.g., Roger Clarke, ‘The Digital Persons and its Application to Data Surveillance’ (1994) 10(2) The Information Society, reproduced at http://www.anu.edu.au/people/Roger.Clarke/DC/DigPersona.html.
Secondly, the difference between 'rights-based' and 'interests-based' approaches to privacy may be illustrated by comparing some of the substantive features of the Data Protection Directive with those of the Australian Commonwealth Privacy Act. Thus, the Australian Act includes a complex array of exceptions and exemptions that are not found in the Data Protection Directive, including important exemptions for small business, expressed at minimising regulatory costs, and for employee records. Direct marketing is also treated more liberally under the Australian Act than under the Data Protection Directive. While the former establishes a general 'opt out' regime for direct marketing, it also allows personal information to be used or disclosed for direct marketing without consent of the data subject where direct marketing is the primary purpose of collecting the information. Article 14(b) of the Directive, in contrast, establishes specific rights for the data subject to object to the processing of personal data for the purposes of direct marketing, and to be informed before personal data are disclosed to third parties for the first time for such purposes. Finally, although both regimes generally allow for personal information to be processed with the consent of the data subject, the formal legal requirements for consent differ. While the Privacy Act allows for consent to be implied, the Data Protection Directive requires that the consent of the data subject must be a 'freely given, specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.'

**Electronic surveillance**

In addition to the collection of identifying information, some DRM systems incorporate the ability to monitor, or conduct surveillance of, activities of an end user associated with protected content. There are two main forms of reporting and monitoring that may be part of a DRM system. First, there is reporting and monitoring that occurs as part of a payment mechanism. For example, the system may be designed to require authentication of a user's identity each time that content is accessed or used. The system may then create a record of the user's interaction with the content, so that the user can be billed in accordance with the use, as specified by the digital rights purchased by the user. Secondly, a DRM system may be designed to report back on the activities of the user that are unrelated to the rights purchased by the user. For example, in *Specht v. Netscape Communications Corp.*, software that was made available as a 'plug-in' to the Netscape browser was designed to improve the downloading capability of the browser but, at the same time, recorded every web site visited by the user and relayed the information to Netscape.

Privacy concerns relating to electronic surveillance are distinct from, but related to, information privacy concerns. In its 1983 report, *Privacy*, for example, the Australian Law Reform Commission (ALRC) distinguished between territorial privacy, privacy of the person, information privacy, and communications and surveillance privacy. In doing so, the ALRC noted that breaches of communications and surveillance privacy could, but do not necessarily, involve breaches of the three other aspects of privacy. Information privacy, then, may be regarded as a right to (or interest in) limiting access to the unconstrained collection and processing of personally identifiable information. Surveillance privacy, on the other hand, may be defined as a right to (or interest in) limiting access to unconstrained intentional observation, especially persistent observation, of one's activities by others, in particular where this is accomplished by means of interception or surveillance technologies. Surveillance privacy overlaps with information privacy to the extent that the collection and processing of personal information may amount to the surveillance of the activities, especially the online activities, of the data subject.

---

68 Privacy Act 1988 (Cth), ss 6C(1), 6D.
69 ibid. s. 7B(3).
70 ibid. National Privacy Principles 2.1(c).
72 ibid. s. 6 (definition of 'consent').
73 Data Protection Directive, above n. 41, Art. 2(h).

75 306 F. 3d 17 (2002). This example is cited by Cohen 'Normal Discipline in the Age of Crisis', above n. 74.
77 In its 2001 Interim Report on surveillance, the New South Wales Law Reform Commission (NSWLC), after noting that the term 'surveillance' 'defies precise definition,' observed that 'surveillance involves using a surveillance device to monitor, either through listening to, watching, or collecting data (in whatever form) about people, places or objects. . . . Surveillance may be directed at a particular target or may be random, but is always a deliberate or intentional act of monitoring conducted for the purpose of acquiring information about the subject of the surveillance'. NSWLC, *Surveillance: An Interim Report*, Report no. 98 (Sydney: NSWLC, 2001), paras. 2.37–8.
The growth of surveillance practices and technologies has been a controversial feature of contemporary Western societies. While privacy concerns arising from surveillance tend to focus on the effects of intrusion on individuals, the potentially ubiquitous surveillance within contemporary information societies has given rise to system-wide concerns. Often cited here is Foucault's well-known discussion of Bentham's design for a model prison, known as the panopticon.\(^\text{78}\) The panopticon was designed so that it was possible for individual prisoners to be under observation at any point in time, although the prisoner would not know whether or not this was in fact the case. Social control was therefore maintained through the continual fear of being observed, which eventually ensured that those under observation internalised the desired norms of behaviour.\(^\text{79}\) Foucault used the panopticon as a metaphor for the way in which power is exercised in modern societies by 'disciplinary' practices – such as surveillance, documentation and classification – which ensure that people conform to social norms and, indeed, shape what it is to be a person. These practices are associated with an increasing rationalisation of society, as well as a normalisation of individual identities. Wide-spread surveillance can therefore be seen as undermining autonomous decision-making by conditioning people to conform voluntarily to accepted standards of behaviour. As Cohen, for example, has warned: 'Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream.'\(^\text{80}\)

Laws regulating surveillance are not as developed as data protection laws. In the past, such laws have mainly been directed at limiting the surveillance practices of government. For example, in the important 1967 decision in *Katz v. United States*\(^\text{81}\) the US Supreme Court held that electronic monitoring of a telephone call was a 'search and seizure' within the Fourth Amendment, meaning that interception without a warrant did not comply with constitutional standards. In that case, Harlan Jr pointed out that 'reasonable expectations of privacy may be defeated by electronic as well as physical invasion'.\(^\text{82}\) The potential incorporation of surveillance functions in DRM systems, however, creates the increasing possibility of surveillance by non-government actors. Surveillance by DRM systems must not, therefore, be seen in isolation, but as part of the increasing use of surveillance systems by both public and private sector entities, with possibly worrying consequences for ever more rationalisation and normalisation, and the threat of increased social conformity.\(^\text{83}\)

Just as the level of protection afforded by data protection laws differs, depending upon whether the laws are 'rights-based' or 'interests-based', objections to breaches of surveillance privacy may be formulated in either 'rights-based' or 'interests-based' terms. 'Rights-based' objections to surveillance are concerned with the extent to which surveillance, both overt and covert, may undermine individual autonomy and dignity. In relation to overt surveillance, if one knows that one is being watched, then this will clearly influence decisions about the activities one engages in. Covert surveillance, on the other hand, is even more objectionable than overt surveillance. First, it undermines autonomous decision-making because the person under surveillance is unaware of the single most important feature of the situation the person is in: the fact that he or she is being monitored. Such knowledge might obviously lead to the making of different decisions about what that person does. Secondly, by concealing the fact of surveillance, the person under surveillance is denied the respect due him or her as a fellow human being.\(^\text{84}\)

At the same time, surveillance may have positive as well as negative consequences.\(^\text{85}\) Some degree of surveillance is necessary for the functioning of modern societies, being important for convenience, efficiency and, increasingly, security. The issue is not whether or not there is surveillance, but the appropriate limits to be placed on surveillance technologies and practices. From a 'rights-based' perspective, the degree of surveillance should be strictly proportional to the ends sought to be achieved. This would suggest that DRM surveillance should be as transparent as possible, and limited to that which is necessary to support the interests of content owners. Moreover, in designing DRM systems, the dangers of systematically embedding surveillance systems within everyday life, with the attendant threats of eroding what it is to be a morally autonomous person, should be taken into account.

---


\(^{79}\) As Foucault put it, the effect is to 'induce in the inmate a state of conscious and permanent visibility that assures the automatic functioning of the power'; ibid. p. 201.


\(^{81}\) 389 US 347 (1967).

\(^{82}\) Ibid. 362.


\(^{84}\) For the classic statement outlining deontological objections to covert surveillance see: Stanley I. Benn, *Privacy, Freedom, and Respect for Persons* in Pennock and Chapman, *Privacy*, above n. 29.

From a perspective that regards freedom from surveillance as an 'interest' rather than a 'right', however, concerns at establishing strict limits on surveillance technologies will be less pressing. 'Interests-based' objections to unconstrained surveillance have focused not on the implications of surveillance for moral autonomy, but on the need to avoid socially wasteful expenditure on surveillance technologies and counter-surveillance technologies. This means that 'interests-based' analyses will give more weight to objectives that conflict with the interests of the person subject to surveillance, such as the interests of content owners in efficiently delivering content, and the social interest in minimising enforcement costs. Pure 'interests-based' perspectives are also likely to ignore the potentially negative system-wide effects of the ever more widespread use of surveillance systems.

**Self-enforcement mechanisms**

As well as providing information about individual users, and about their activities in relation to digital content, DRM systems may directly impose technological controls on what users may, or may not, do with digital content. For example, a particular form of content may be programmed to self-delete after being accessed a certain number of times, or may only be able to be used on particular consumer equipment. The 'broadcast flag' proceedings, before the Federal Communications Commission (FCC) in the United States, was a good example of proposals for DRM systems designed to impose direct restrictions on users. The 'broadcast flag' was aimed at promoting technologies that allowed users to make copies of digital broadcast content for their own purposes, but prevented unrestricted distribution of the content, especially by the internet. Increasingly, it seems that copyright owners are interested in building into consumer electronics some constraints on what users may do with copyright material.

Self-enforcement mechanisms embedded in technology may be distinguished from DRM surveillance technologies in the following way: the

---

16 In American Libraries Association v. Federal Communications Commission (No. 04-1037, decided 6 May 2005), the US Court of Appeals for the District of Columbia Circuit decided that the FCC lacked the authority to impose the 'broadcast flag'.

---

former impose *ex ante* restrictions on access to, or use of, protected content, whereas the latter are concerned mainly with detecting, and reporting on, activities after they have occurred. In other words, while DRM surveillance technologies involve intrusions on a person's private activities that fall comfortably within our accepted understanding of what it means to invade privacy, the latter do not involve direct intrusions, but may well remove the need for *ex ante* intrusions.

On this point, Cohen has argued that, if surveillance represents an intrusion into privacy, then direct control of a user's activities, which effectively removes the need for intrusion, must be an even greater invasion of privacy. She goes on to claim that technological self-enforcement mechanisms represent an invasion of privacy in two senses in which it has been recognised in the US tradition: as an intrusion into private spaces, and as a breach of the constitutionally recognised right of individuals to make decisions regarding private matters, as first recognised by the Supreme Court in *Griswold v. Connecticut*.

This argument raises difficult questions about the meaning of the concept of privacy that are beyond the scope of this chapter. It may be that technological restrictions on what a user may do with digital content should be seen as limiting personal autonomy, in the sense of the capacity of a person to make decisions about his or her 'private' life, rather than as invasions of privacy. In any case, in the same way as invasions of privacy, strictly speaking, may be analysed from either a 'rights-based' or 'interests-based' perspective, so too may restrictions on user autonomy.

If promoting autonomy, meaning the ability of individuals to make decisions for themselves, is regarded as desirable, then widespread use of technological restrictions that dictate how digital content is to be used can be seen as problematic. In other words, technologies may be designed in such a way as to either restrict the ability of users to make decisions about what they can do with the technology, or to maximise user choice. Furthermore, embedding behavioural rules within technology may, like pervasive surveillance, promote greater social conformity over time. From a 'rights-based' perspective, therefore, the pervasive use of DRM self-enforcement technologies might be thought to erode the autonomy and dignity of users of copyright material.

---

88 Cohen, 'DRM and Privacy', above n. 74, 582.
89 On this characteristic feature of the American tradition see Whitman, 'The Two Western Cultures of Privacy', above n. 30, 1161.
90 381 US 479 (1965).
From an 'interests-based' perspective, on the other hand, such technological constraints might be seen as useful insofar as they preserve incentives by preventing uncompensated uses of digital material, and reduce enforcement costs for content owners. Furthermore, by helping markets for copyright material to be divided according to individual preferences, technological restrictions may assist price discrimination which, in this context, is usually thought to enhance economic efficiency. Against these considerations, such constraints may pose the danger of content owners extracting uneconomic rents.

To date, there has been no specific regulation of the way in which emerging technologies may restrict what users can do. But there is evidence of support emerging for the idea that the privacy implications of new technologies should be considered at the time at which they are designed or implemented. For example, a 2005 Senate review of Australian privacy laws favoured the introduction of a statutory privacy impact assessment process for new projects that may adversely affect privacy, and proposed that a future review of privacy laws consider the privacy implications of new and emerging technologies to determine whether they are adequately regulated. It appears increasingly apparent that both copyright law and privacy law-making will, in the future, be concerned with the choices made in the design of technologies. Clearly, a 'rights-based' approach to protecting user autonomy will be more concerned about widespread technological constraints on user behaviour, and more favourable to some form of regulation of such technologies, than will an 'interests-based' approach.

Copyright, privacy and DRM

It will be clear that difficult policy issues arise in defining the appropriate relationship between copyright and privacy. The extent to which some form of legal regulation is needed to ensure an appropriate balance in the context of DRM systems is even more difficult. In truth, it is still too early in the development and implementation of these systems for any definitive conclusions to be drawn.

To date, the official policy responses have been limited, with the most detailed examination thus far being undertaken by the European Union within the framework established by the Data Protection Directive. In early 2005, a working document prepared by the Working Party established under Article 29 of that instrument confirmed the application of the EU data protection principles to DRM systems. In particular, the document emphasised the following specific issues:

- the need to preserve anonymous access to network services;
- the desirability of limiting the extent to which a specific individual is linked to a document to circumstances in which it is necessary for the performance of a service or where the individual has consented to the link;
- the importance of establishing the greatest possible transparency in DRM systems, including that users are informed, prior to the collection of personal data, of the identity of the data controller, the purposes of data processing, the recipients of the data and the existence of a right of access and rectification;
- the need to ensure that personal data is used only for the stated purpose of collection and not, for example, for the purpose of direct marketing when the purpose of collection is authentication of payment; and
- the need to ensure that personal data is kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which the data has been collected.

This analysis is clearly based on a particular perspective, viewing the issues through the lens of the EU 'rights-based' approach to data protection. Other jurisdictions, however, may take a different approach, particularly if they adopt an 'interests-based' analysis. Indeed, the main point made in this chapter is that, to understand properly the relationship between copyright and privacy, an essential starting point is to identify and articulate the perspective from which that relationship is to be analysed. Thus, the appropriate level of copyright protection in the digital environment will differ depending upon whether copyright is predominantly regarded as protecting authors' rights (as in civil law systems), or as supporting markets in copyright material (a more peculiarly common legal approach). In the same way, the level of protection accorded privacy will vary depending upon whether this is regarded as a fundamental right that is essential to the autonomy and dignity of persons, or if it is simply regarded as an individual 'interest' (or preference) that is to be balanced.

---

90 Australia, Senate Committee, The Real Big Brother, above n. 66, Recommendations 5 and 8, paras. 7.13 and 7.24. The terms of reference for the ALRC review, referred to at n. 66 above, instruct the ALRC to consider 'the need of individuals for privacy protection in an evolving technological environment'.

with other interests, with the final judgment being made on utilitarian grounds.

For example, adopting a predominantly utilitarian, 'interests-based' analysis might mean that a prospective law regulating the use of DRM systems would fail to be assessed by reference to its capacity to promote markets in copyright material. Under such an approach, potentially privacy-invasive measures might be defensible as being necessary for the reduction of transaction and enforcement costs as well as having possible consumer benefits, including the more accurate tracking and targeting of consumer preferences. By contrast, a 'rights-based' analysis that emphasises the protection of the autonomy and dignity of users may justify limitations on the use of such measures, even where those limits could not be justified from a purely economic perspective. Finally, if 'rights-based' arguments for the protection of authors are factored into the analysis, there is the complex task of balancing two, potentially competing sets of rights: the personality rights of authors and the privacy rights of users.

**Conclusion**

This chapter has argued that, in assessing emerging DRM systems, it is important to distinguish, both historically and conceptually, between the two main western legal traditions for understanding copyright and privacy: a 'rights-based' approach and a utilitarian, 'interests-based' approach. The two approaches reflect quite different views of the relationship between the law and the market. From a 'rights-based' perspective, the role of the law is mainly to establish limits on the market to protect the autonomy and human dignity of both authors and content users. But from a utilitarian/economic perspective, the main role of the law is to support the efficient operation of markets.

At present, it is still far too early in the development of DRM systems to be able to adequately assess such systems from either a 'rights-based' or 'interests-based' perspective. We simply do not have sufficient information about how those systems might work in practice for any sensible conclusions to be drawn.

As these systems are being developed, however, we suggest that it is important to commence a more detailed analysis of some specific issues than has been attempted to date. In our view, the most pressing matters for investigation are:

- the functions or design elements of DRM systems that promote economic efficiency, and those that may undermine efficiency objectives;
- the economic analysis of laws that apply to DRM systems, especially anti-circumvention laws;
- the extent to which it is desirable for copyright laws to promote values other than market-based values, including privacy rights and rights to freedom of expression;
- the extent to which values other than market-based values, especially rights to privacy, should be taken into account in determining the legal framework to apply to DRM systems;
- the adequacy of existing privacy laws, especially data protection laws, for regulating DRM systems, in particular whether these adequately capture all of the privacy implications of DRM systems, or whether they need to be extended to take account of other concerns, such as the potential surveillance of end users; and
- the extent to which the privacy of content users may require the development of specific technical tools, such as Privacy Enhancing Technologies, in addition to legal forms of protection.\(^\text{94}\)

In other words, detailed attention is required to examine the appropriate level of control that owners should have over digital content and the extent to which limits on control may be justified in order to protect content users, including their rights to privacy. While the combination of technological developments and the global trade in digital content may well lead to paradigm shifts in legal traditions as they apply to digital content, it is important, at this stage, that the policy choices available for regulating DRM systems be understood. We also consider it important that, in addressing these new and emerging technologies, the values underlying policy decisions are made more transparent than has been the case to date. It is only when this is done that it will be possible for laws to be formulated that appropriately reflect both the important values served by the protection of authors' rights and copyright material, on the one hand, and the protection of end user privacy, on the other.

\(^94\) The importance of technological measures for the protection of privacy has received official acknowledgement. E.g., the Australian Privacy Commissioner's 2005 review of the private sector provisions of the Privacy Act stated that: 'There is a role for technology itself in protecting privacy, often called Privacy Enhancing Technology or PETS. E.g., a system can be built to allow anonymity, or it can be built in a way that identifies every step a user takes'; Office of the Privacy Commissioner, Getting In or the Act, above n. 68, p. 241.
Author/s:
Lindsay, David; RICKETSON, STANIFORTH

Title:
Copyright, Privacy and Digital Rights Management (DRM)

Date:
2006

Persistent Link:
http://hdl.handle.net/11343/25403

File Description:
Published version