

Becker, E.; Buhse, W.; Günnewig, D. et al. (Hg.), 2003: Digital Rights Management – Technological, Economic, Legal and Political Aspects. Berlin: Springer

Bing, J.; Dreier, Th. (eds.), 2005: Clark, Charles: “The answer to the machine is in the machine” and other collected writings. Oslo: Norwegian Research Center for Computers and Law

Dressel, Ch.; Scheffler, H. (Hg.), 2003: Rechtsschutz gegen Dienstpiraterie – Das ZKDSG in Recht und Praxis. München: Beck

Gottschalk, E., 2003: Das Ende von „fair use“? – Technische Schutzmaßnahmen im Urheberrecht der USA. MultiMedia und Recht (MMR) 2003, S. 148-156

Lessig, L., 1999: Code and other Laws of Cyberspace, New York: Basic Books

Peukert, A., 2002: Digital Rights Management und Urheberrecht, UFITA 2002/III, UFITA 2002/III, S. 689-713

Pfitzmann, A.; Sieber, U., 2002: Anforderungen an die gesetzliche Regulierung zum Schutz digitaler Inhalte unter Berücksichtigung der Effektivität von technischen Schutzmechanismen. VPRT-Gutachten

Trayer, M., 2003: Technische Schutzmaßnahmen und elektronische Rechtswahrnehmungssysteme – die Umsetzung der Art. 6 und 7 der EU-Urheberrechtsrichtlinie in deutsches Recht und der Schutz des Nutzers urheberrechtlicher Werke. Baden-Baden: Nomos

Kontakt

Prof. Dr. Thomas Dreier
 Universität Karlsruhe (TH)
 Institut für Informationsrecht
 Am Fasanengarten 5, 76131 Karlsruhe
 Tel.: +49 (0) 721 / 608 - 33 95
 Fax: +49 (0) 721 / 608 - 65 06
 E-Mail: recht@ira.uka.de

»

A Short Policy Analysis of Copyright Law and DRM in the United States

by Bill Rosenblatt, GiantSteps Media Technology Strategies, New York, USA

The United States is the source of a good deal of both the content owned by major media companies¹ and the technology used to distribute it securely. Its progress in adopting DRM to protect content owners' intellectual property is therefore of interest to concerned parties in Europe, even though market and legal conditions are different. The first part of this article introduces the US legal background and assesses recent legal developments that apply to digital content and attempts to impose DRM technology through legislation. In the second part, the perspective of the assessment is extended to three relevant issues an assessment of DRM would have to consider: the function of DRM with respect to the copyright system, consumer concerns with respect to DRM, and the overall economic value of DRM.

1 Legal Background and Legal Developments

The legal context for DRM is copyright law. Some relevant aspects of US copyright law have similarities with those of EU countries by virtue of their common derivation from the WIPO Copyright Treaty of 1996 (WIPO 1996), which were enacted in the US and EU via the Digital Millennium Copyright Act (DMCA 1998) and European Union Copyright Directive (EUCD 2001) respectively.

However, there is an important difference between the two laws, which leads to divergent ways of contextualizing DRM within the legal framework. Most EU countries have Private Copying provisions in their copyright laws, which allow consumers to create copies of legitimately obtained content for their own use or that of family members. Private Copying laws can conflict with DRMs that restrict such activities.

1.1 Fair Use and First Sale

The US has no broadly applicable Private Copying concept in its copyright law.² Instead,

it has two relevant concepts: Fair Use (USC 17, §107) and First Sale (USC 17, §109).

Fair Use is similar to Fair Dealing in UK copyright law. It is a set of principles that guide courts when deciding whether uses of copyrighted works are defensible against infringement charges. The principles include such considerations as the purpose and character of the use, including whether the use is of commercial nature, and the effect of the use on the market for the work.

US case law has established precedents for types of uses being considered presumptively fair, such as criticism, parody, and academic research. However, because Fair Use is based on abstract principles (not facts) and decided by courts, it is impossible to conceive of a DRM scheme that “upholds Fair Use”. This has been a source of contention between US advocacy organizations – such as the Electronic Frontier Foundation, Public Knowledge, and DigitalConsumer.org – and the media industry.

Contention over Fair Use also affects another part of US copyright law, the aforementioned DMCA. Although the primary purpose of DMCA was to bring the US into compliance with the WIPO Treaty, it is mainly known as shorthand for one of its provisions (USC 17, §12.01, also known as “DMCA 1201”), which criminalizes distribution of technology for circumvention (hacking) of DRM schemes – which are known as Technical Protection Measures (TPMs) in the law.³

DMCA 1201 forbids circumvention of TPMs even if the purpose of the circumvention turns out to be one that a court finds to be Fair Use. It comes down to a question of whether content rights holders or consumers should get the benefit of the doubt about content uses. The media industry feels that allowing exceptions to the anticircumvention law (beyond the current narrow and temporary exceptions for things like encryption research and accessing content in obsolete data formats) undermines DRM by making those exceptions subject to court decisions, and therefore, as a practical matter, gives the benefit of the doubt to consumers.

First Sale, on the other hand, says that once someone has legitimately obtained a copyrighted work, the publisher of that work can have no further claim or influence on any further distribution of the work. First Sale law

has thus enabled such services as public libraries, video rental stores, and so on. Media industry interests argue that First Sale does not apply to digitally distributed works (as opposed to physically distributed digital works, such as CDs and DVDs) because they are made available under license agreements⁴ and not via copyright. Therefore, First Sale currently does not apply to content packaged with DRM.

1.2 Secondary Infringement Liability

The other primary principle in US copyright law that bears on DRM is the theory of secondary infringement liability. If someone infringes copyright and another party is somehow involved, the latter party could be legally liable; this is called secondary liability.

Most countries have some form of secondary copyright infringement liability law. US case law has established two types of secondary liability, known as contributory and vicarious infringement. Contributory means knowingly aiding and abetting infringement, while vicarious means being able to control infringing activities but choosing not to for one’s own gain.

A key legal principle that governs applicability of secondary liability to technology providers in the US is the 1984 Supreme Court decision in *Sony vs. Universal* (Sony 1984), known as the *Betamax* case because it established the legality of Sony’s Betamax videocassette recorders (which, ironically, lost out to the VHS format in the market) over the film industry’s objections. With *Betamax*, the Supreme Court established the principle of “significant noninfringing uses”, meaning that if a technology can be shown to have significant uses that do not infringe copyright, the maker or distributor of that technology should not be liable for infringement.

Despite *Betamax*, a federal appeals court (one level below the Supreme Court) found that both contributory and vicarious liability applied to centralized peer-to-peer (P2P) file-sharing networks (i.e., file-sharing services that maintain central directories of files available) in its 2001 decision in *A&M Records vs. Napster* (Napster 2001). As a result, developers created file-sharing network software that did not rely on central directories, such as Grokster, Morpheus, BearShare, and LimeWire. There was no theory

of secondary liability that applied to the developers of the client software for these networks.

The foregoing should set the scene for recent developments on the legal front in the US.

1.3 The Future of Fair Use?

Regarding Fair Use, there is a growing recognition of a fundamental incompatibility between Fair Use guidelines (and the fact that only a court can decide on them) and technological means of controlling access to copyrighted works.

In his book *Free Culture*, Lawrence Lessig of Stanford University laments that while Fair Use is meant to be a narrow “wedge” between infringement and non-infringement that applies to a small set of borderline content use cases and helps courts decide on them, it has been overburdened with responsibility of determining the legality of many digital content use cases because they all happen to involve copying (of bits), thereby making them subject to copyright law (Lessig 2004). Some of these use cases are analogous to content uses in the physical world that do not involve copying: for example, broadcasting music over a standard radio signal does not require copying, while streaming it over the Internet does.

In general, because digital technology can be used to implement an almost infinite variety of content distribution models instantaneously, it becomes counterproductive to rely on Fair Use principles – let alone case precedents from the physical content world – to judge whether each and every case infringes: it would overload the court system, make it necessary to hire lawyers where ordinarily none would be necessary, and generally superimpose a physical-world timeline on a digital paradigm.

Some legal scholars and advocacy groups argue that Fair Use should be kept intentionally principle-based – i.e., imprecise – because it is meant to handle exactly those cases that precise laws cannot handle. Yet in an era where technology underpins more and more content uses, this attitude seems increasingly outmoded.

Someday, someone is going to have to do something about Fair Use – either scrap it in favour of more *a priori* decidable criteria (perhaps along the lines of Private Copying) or augment it with such. Without this, it becomes

very difficult to enable technology to control access to technologically distributed content; there are too many fallbacks into the traditional legal system. (Of course, this is precisely what some of those legal scholars and advocacy groups intend.)

With this in mind, the state of California enacted a law in 2004 that requires anyone who digitally transmits copyrighted works (e.g., through e-mail) to more than 10 other people to include the identities of the sender and the work (California 2004). In other words, California has decided that private copying is probably acceptable for up to 10 “friends,” beyond which it is probably not. Unfortunately, this law attracted very little attention. But it is the kind of law that seems inevitable in the future.

There is some momentum in Congress to amend DMCA 1201 to allow for circumvention of Technical Protection Measures to facilitate Fair Uses of content. One piece of legislation along these lines that has been introduced is the Digital Media Consumer Rights Act (DMCRA 2003), which (among other things) would roll back DMCA to allow circumventions for non-infringing purposes. The bill has some chance of passage in the near future; its sponsors are bipartisan. The IT and telecoms industries as well as many of the aforementioned advocacy groups back DMCRA; the media industry opposes it.

As for First Sale, there is a sense that some digitally-distributed content products could someday fall under it if a judge decides that a particular license agreement has terms that are similar enough to copyright usage terms that the product should be judged as if it were copyright (this is known in America as the “If it looks like a duck, waddles like a duck, and quacks like a duck, it must be a duck” principle), thereby setting a precedent. This has not happened yet, however.

1.4 Grokster and Secondary Liability

The media industry has tried to get US government to do something that would bring decentralized P2P networks like Grokster and Morphueus under the regime of secondary infringement liability. The first attempt was to lobby Congress to pass a law that would make it illegal to “induce infringement of copyright”. This was known as the “Induce Act” (Induce 2004).

It failed: Senator Orrin Hatch, the bill's sponsor, decided not to take the bill forward when the various sides in the debate could not agree on reasonable criteria for judging "inducement".

Around the same time, a federal appeals court dealt the media industry a setback when it ruled that secondary liability did not apply to the decentralized P2P networks Grokster and Morpheus, and that the *Betamax* principle of significant noninfringing uses did. The media industry responded to these setbacks by getting the Supreme Court to hear the *Grokster* case.

In June 2005, with its decision in *MGM vs. Grokster* (Grokster 2005), the Supreme Court unanimously did what the lower court and Congress would not do: establish an "inducement" principle in copyright law. "Inducement to infringe" is, in fact, a well-known principle in patent law (USC 35, §271(b)). An implementer of technology that infringes a patent may not actually infringe itself; it may "induce" someone who uses the technology to infringe the patent.

The Supreme Court established a set of criteria that determine inducement to infringe copyright: the developer of the technology must actively market the technology for infringing purposes, and its business model must depend on infringement. Those who merely invent technology that could possibly be used for infringing purposes but do not meet those criteria, are not liable. The court did not overturn *Betamax*, but the line between "substantial noninfringing uses" and "inducement" has yet to be explored in the courts.

The Supreme Court found that both Grokster and Streamcast (the firm that developed the Morpheus software) met the inducement criteria. It vacated the lower court's summary judgment in the case, which means not that the two firms were found guilty, but that the case is referred back to the lower court, which must now hold a trial and take the Supreme Court's decision (i.e., the inducement principle) into consideration.

Soon after the *Grokster case*, the music industry sent cease-and-desist letters to many P2P network software developers based in the US, and most of them chose to shut themselves down quickly. One that did not, LimeWire, is implementing a hash-based filtering scheme to show that it "respects copyright", although the scheme it intends to use has been shown to be

easily hackable. Grokster settled the case by selling its assets – essentially its list of subscriber information – to a service called Mashboxx, while BearShare sold its assets to iMesh. Streamcast intends to fight the case, which could take years.

1.5 Mandating DRM

The media industry has also been lobbying Congress to pass legislation that makes DRM technology mandatory in digital media rendering hardware and software. A previous attempt, the so-called Hollings Bill of 2002 (after its sponsor, Sen. Ernest Hollings), failed over forceful opposition from the IT industry (led by Intel) and even some media companies with their own interests in IT (Hollings 2002). The negotiations over this bill revealed a schism in the media industry between companies with hard-line attitudes towards DRM, mainly Disney and News Corp., and those with more liberal attitudes, such as Time Warner.

The latest attempts to impose DRM-type technology on IT and consumer electronics industries are the Broadcast Flag and the so-called Analog Hole bill. A lineup of "usual suspects" has formed around these bills as well as past ones mentioned above (e.g., the Induce Act): the media industry is in favour, while IT, telecoms, and consumer advocacy groups are against.

Broadcast Flag would require digital television receivers to detect a simple "flag" (bit of data) that would act as a signal that the content is not to be copied. This was established in late 2003, not as a law but as a regulation through the Federal Communications Commission (FCC), the body that regulates radio, television, telecoms, and so on. The FCC chose to adopt the regulation (FCC 2003), but a federal appeals court found that it was overstepping its authority in doing so (USCA 2005).

Now Congress is considering legislation that would explicitly empower the FCC to adopt Broadcast Flag. This legislation is considered unlikely to pass this year, mainly because it is a small provision tacked onto a major telecommunications reform bill in which much larger-scale differences have yet to be reconciled between the two houses of Congress. But it could be reintroduced next year,

along with related legislation that would extend the Broadcast Flag concept to satellite radio.

The so-called Analog Hole bill (Analog Hole 2005; formally known as the Digital Transition Content Security Act of 2005) is meant to address illegal analogue copying of video content, such as through analogue outputs of video players. The bill would require certain types of video playback equipment to include digital video watermarking technology – specifically that of a startup company called VEIL Interactive – that can forensically catch pirated content once it has been distributed, even if it was converted to high-quality analogue.

The Analog Hole bill is problematic because it effectively enshrines a specific technology firm's products into law, even though the technology has established competition and has not even really been used in the situations that the bill covers. Additionally, the bill purports to solve a problem that is shorter-term and narrower than that envisioned in the Hollings Bill. For these and other reasons, the Analog Hole bill is also deemed unlikely to pass.

2 Assessing the Impact of DRM – Three Research Topics

DRM is roughly the same age as related technologies that have become well-established in the market; it dates back roughly to the mid-1990s. But its success has been relatively limited, especially when compared to technologies for unfettered distribution of unprotected content, such as MP3 audio files. Therefore it is difficult to assess the impact of DRM from social, economic, political, or environmental perspectives.

Here we propose three main sets of criteria that a proper assessment of DRM might measure. These are: the functionality of DRM with respect to the copyright system, consumer issues beyond copyright, and the economic value of DRM.

2.1 Assessing the Functionality of DRM with Respect to the Copyright System

Copyright systems are intended to preserve a balance of interests between content creators and the public, so that the public domain is enriched while creators have sufficient incen-

tive to keep on creating. Developments in law as well as technology constantly threaten this balance, so it is hard to evaluate the effect of DRM in a vacuum, particularly since DRM currently applies to only a narrow slice of content distribution.

The most straightforward way of assessing DRM's effect on the copyright balance is to look at DRM systems and compare the rights they confer on users to those that one would expect to get in a typical copyright system. However, there are three limitations to this approach.

First, most DRM systems are not fixed with respect to the rights they confer; they can be configured by the content owner or distributor (a notable exception to this, admittedly, is Apple's FairPlay DRM for iTunes). Therefore, the rights that a given DRM confers on the public are primarily a function of market forces (iTunes is very popular and the subject of relatively few complaints about its DRM).

Second, DRMs are used in content licensing arrangements, which by definition are not sales of copyright (see the section on copyright law above). They can involve grants of rights that aren't typically considered in copyright systems (e.g., limited duration access, such as by number of plays or calendar time), which makes comparing them to the "copyright bundle" a bit like apples and oranges.

Finally, copyright systems vary from one country to another. As mentioned earlier in this article, there are differences between US/UK and EU copyright laws that acutely affect how DRMs might measure up to them.

Another way to look at how DRM affects the copyright balance is through incentives to content creators. It can be said that media companies use DRM to preserve their role in the content value chain. The media industry argues that this is synonymous with preserving incentives for content creators, though that is a matter for debate. Yet it is certain that if DRM did not exist, and content could be freely distributed without compensation, the structure of the content industry would change dramatically.

In particular, the industry's "scalability" would suffer beyond recovery. The media industry is currently structured around the concept of blockbuster films, songs, books, etc., which garner direct revenue that is directly

proportional to the number of copies sold. Without DRM, this component of media industry revenue would collapse. Distribution of content without the direct stream of revenue would become a means to an end rather than an end itself – a way for artists to get exposure so that they could make money on other things, such as performances and ancillary physical merchandise.

One way of using this observation to derive an assessment of DRM's impact on incentives is to look at small content producers, such as independent record labels. Most "indies" eschew DRM (e.g., they do not release copy-protected CDs, and they distribute unencrypted MP3s on sites like eMusic.com); they seek to maximize exposure for their artists. Indie artists get a smaller proportion of their revenue from direct content sales than big-name artists do. Would an "indie" artist who became famous suddenly embrace DRM? If so, at what point in the artist's popularity (e.g., after how many album sales)? Once the artist uses DRM, how much benefit redounds to the artist, as opposed to the record company? Following some artists over time and comparing the outcomes might provide some insight into how DRM preserves the balance of incentives in the copyright system.

2.2 Assessing DRM from the Consumer Perspective

Organizations such as the Electronic Frontier Foundation and UFC-Que Choisir (in France) have begun to assess DRMs from the consumer's perspective. Beyond issues of content rights that DRMs convey to users, these organizations have started to assess them with respect to users' privacy and security, which one might call environmental factors.

Many of the concerns that have been raised about DRM privacy and security relate to the PC platform, which was definitely not designed with DRM in mind. The recent furore over CD copy protection technology implemented by SonyBMG Music is a good example (Rosenblatt 2005). The technology, developed by the British firm First4Internet, transmitted information related to consumers' usage of content over the Internet, and it installed itself in a way that acted as a haven for viruses. CD copy protection in general is essentially a clumsy retrofit to the PC

platform; there are bound to be incompatibilities. DRM technologies that are incorporated into the designs of other devices (e.g., mobile phones) may not corrupt those devices' security, although they may still raise privacy concerns.

From the content owner's point of view, DRM technology is superior if it provides accurate information about content usage, in order to properly compensate rights holders, and if it is impossible to install, so that it cannot be circumvented. Those goals can be at odds with those of the consumer.

It should be possible for a consumer watchdog organization to develop criteria for testing security and privacy of DRMs, just as they could for other e-commerce technologies. A model for this may be the TRUSTe privacy certification for e-commerce websites, which signifies respect for users' privacy.

2.3 Assessing the Overall Economic Value of DRM

The final assessment criterion that we mention here is probably the most elusive one to measure: the overall economic value of DRM (Rosenblatt 2003). Perhaps the main reason why DRM has been slow to take off in the market is because no one wants to pay for it. In particular, the media industry – which, as implied above, has the most incentive for DRM – has been unwilling to pay for DRM technology.⁵

The media industry claims losses from media piracy in the billions of dollars each year. In 2005, the US motion picture industry claims USD 2.3 Billion in losses due to Internet piracy (out of USD 6.1 Billion, which also includes unauthorized reproduction of physical goods, such as VHS tapes and DVDs) (MPAA 2005). The music industry tracks physical but not Internet piracy (IFPI 2005). No media industry segment has attempted to determine how much file-sharing contributes to incremental sales through viral marketing, nor have they attempted to determine how much DRM-enabled services enhance revenue by implementing new business models for content (e.g., music subscription services).

Decent estimates of the above would go a long way towards establishing the economic value of DRM. The next step would then be to calculate the effect that certain DRMs have on

those figures; this would provide an upper bound on the economic value of DRM. To put this in some perspective: let's say that a DRM technology could cut the USD 2.3 Billion by 25 percent and add half a billion dollars in revenue from new business models – both reasonable numbers. That puts the maximum value of DRM at over a billion dollars, which buys quite a lot of DRM.

A few studies have been done that provide some data points (Jupiter 2003, INDICARE 2005, Fetscherin 2005), but much more work could be done. The benefit of such analysis would be better cooperation from consumer electronics vendors and more of a rifle-shot approach to DRM design that focuses on where it is most effective for content owners and consumers alike.

Notes

- 1) Even if those media companies are headquartered outside of the US, such as Bertelsmann and Sony.
- 2) The Audio Home Recording Act of 1992 (USC 17, §1001-10) includes some limited private copying rights for audio material.
- 3) The anticircumvention provision is also derived from the WIPO Treaties, and there are now anti-circumvention laws in most EU countries as well.
- 4) End User License Agreements, so called EULAs, or “clickwrap” agreements.
- 5) This is not entirely the fault of media companies: much DRM technology, especially in the early days, suffered from the twin problems of poor ease of use and being produced by venture-backed startup companies with unrealistic revenue expectations.

Literature

Analog Hole, 2005: Digital Transition Content Security Act of 2005; available at: <http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.4569> [last visit 23.06.2006]

California, 2004: California state statute on electronic transmission of copies of digital works; available at: http://www.leginfo.ca.gov/pub/03-04/bill/sen/sb_1501-1550/sb_1506_bill_20040921_chaptered.html [last visit 23.06.2006]

DMCA, 1998: Digital Millennium Copyright Act of 28 October 1998; available at: http://www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html [last visit 23.06.2006]

DMCRA, 2003: Digital Media Consumer Rights Act of 2003; available at: <http://thomas.loc.gov/cgi-bin/query/z?c108:H.R.107:IH> [last visit 23.06.2006]

EUCD, 2001: Directive 2001/29/EC of the European Parliament and of the Council on the harmonisation of certain aspects of copyright and related rights in the information society; available at: http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=32001L0029&model=guichett [last visit 30.06.2006]

FCC, 2003: FCC Broadcast Flag regulation; available at: http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-03-273A1.pdf?date=031104 [last visit 23.06.2006]

Fetscherin, M., 2005: Implications of Digital Rights Management on the Demand for Digital Content. PhD Dissertation. Bern: University of Bern

Grokster, 2005: Supreme Court decision in MGM vs. Grokster; available at: <http://www.supremecourtus.gov/opinions/04pdf/04-480.pdf> [last visit 23.06.2006]

Hollings, E., 2002: The Consumer Broadband and Digital Television Promotion Act of 2002; available at: <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:s.02048>: [last visit 23.06.2006]

IFPI, 2005: International Federation for the Phonographic Industry: The Recording Industry 2005 Commercial Piracy Report; available at: <http://www.ifpi.org/site-content/library/piracy2005.pdf>

INDICARE, 2005: Digital Music Usage and DRM, verfasst von Nicole Dufft, Andreas Stiehler, Danny Vogeley und Thorsten Wichmann, Mai 2005, online verfügbar unter http://www.indicare.org/tiki-download_file.php?fileId=110 [last visit 23.06.2006]

Induce, 2004: Inducing Infringement of Copyright Act of 2004; available at: <http://thomas.loc.gov/cgi-bin/query/z?c108:S.2560>: [last visit 23.06.2006]

Jupiter, 2003: Consumer Attitudes Toward Digital Rights & Content Ownership. Jupiter Research Report. New York: Jupitermedia Corporation

Lessig, L., 2004: Free Culture. New York: Penguin Press

MPIAA, 2005: Motion Picture Association of America Research Report: Worldwide Study of Losses to the Film Industry & International Economies Due to Piracy; available at: <http://www.mpa.org/research/Statistics.asp>. [last visit 23.06.2006]

Napster, 2001: Ninth federal circuit Court of Appeals decision in A&M Records vs. Napster; available at: <http://cyber.law.harvard.edu/~weltsel/napster.html> [last visit 23.06.2006]

Rosenblatt, B., 2003: Paying for DRM. In: Proceedings of BUMA/IViR Symposium: Copyright and the Music Industry: Digital Dilemmas, Amsterdam, Netherlands, July 2003; available at: <http://www>.

ivirbumaconference.org/docs/thefutureofdigitalrightsmanagementformusic1.doc [last visit 23.06.2006]

Rosenblatt, B., 2005: Meltdown Continues over First4Internet's CD Copy Protection. In: DRM Watch, November 17, 2005; available at: <http://www.drmwatch.com/drmtech/article.php/3565106> [last visit 23.06.2006]

Sony, 1984: Supreme Court decision in Sony vs. Universal; available at: <http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=464&invol=417> [last visit 23.06.2006]

USC 17: United States copyright law; available at: <http://www.law.cornell.edu/uscode/17/> [last visit 23.06.2006]

USC 35: United States patent law; available at: http://www.law.cornell.edu/uscode/html/uscode35/usc_sup_01_35.html [last visit 23.06.2006]

USCA, 2005: DC circuit Court of Appeals decision to strike down Broadcast Flag regulation; available at: <http://pacer.cadc.uscourts.gov/docs/common/opinion/s/200505/04-1037b.pdf> [last visit 23.06.2006]

WIPO, 1996: WIPO international copyright treaty; available at: http://www.wipo.int/treaties/en/ip/wct/trtdocs_wo033.html [last visit 23.06.2006]

Contact

Bill Rosenblatt
President
GiantSteps Media Technology Strategies
1841 Broadway, Suite 200, New York, NY 10023,
USA
Tel.: +1 - 212 - 956 10 45
Fax: +1 - 212 - 258 32 86

»

Privacy4DRM: Nutzer- und datenschutzfreundliches Digital Rights Management

von Jan Möller, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, und Stefan Puchta, Fraunhofer-Institut für Digitale Medientechnologie

Ziel dieses Artikels ist es, einen Überblick über Inhalt und Ergebnisse der Studie „Privacy4DRM“ zu geben, die vom Bundesministerium für Bildung und Forschung (BMBF) gefördert wurde. Dabei werden zunächst Eigenschaften und Einsatzumfeld von klassischen Systemen des Digital Rights Managements (DRM) näher beleuchtet; anschließend wird die datenschutzrechtlich geprägte Untersuchungsmethode erläutert, gefolgt von der Darstellung der konkreten rechtlichen Anforderungen an DRM-Systeme. Abschließend werden Handlungsempfehlungen und Forschungsbedarf in diesem Zusammenhang vorgestellt.

1 Einleitung

Virtuelle Güter in digitaler Form (kurz: digitale Inhalte) spielen eine zentrale Rolle in der Informationsgesellschaft. Dabei kommt dem Schutz und dem Management der Urheber- und Verwertungsrechte einerseits und der Wahrung von Kunden- und Nutzerrechten andererseits eine wichtige Bedeutung zu. Die seit einiger Zeit geführten Debatten zielen dabei besonders auf den Sinn und die Einsatzmöglichkeiten so genannter digitaler Rechtemanagement-Systeme (DRM-Systeme) ab. Dabei zeigt sich, dass die Verwendung von DRM-Technik in aktuellen eCommerce-Anwendungen nicht nur technische sondern auch vielfältige rechtliche Probleme aufwirft – insbesondere, wenn es um den Schutz der Privatsphäre des einzelnen Nutzers geht. Eine datenschutzkonforme, das informationelle Selbstbestimmungsrecht des Kunden respektierende Gestaltung von DRM-Systemen ist aber nicht nur unter Compliance-Gesichtspunkten¹ geboten, sondern ist für das einsetzende Unternehmen auch eine Frage der Beziehung zum und des Umgangs mit dem Kunden.

In der Studie „Privacy4DRM“, die das Fraunhofer Institut für digitale Medientechnologie (IDMT) Ilmenau zusammen mit dem Unab-