TACD

TRANS ATLANTIC CONSUMER DIALOGUE
DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. IP-01-05 DATE ISSUED: APRIL, 2005

Resolution on Digital Rights Management

Introduction

Digital Rights Management systems are removing traditional rights from consumers, and the costs associated with them outweigh the benefits. TACD is calling attention to the problems produced by DRMs, and is calling on the EU and US Governments to establish certain preconditions complementary to the legal protection granted to these new technologies.

The Issue

Much of the discussion on the digital environment has focused on the perspective of rights holders, fighting copyright infringement and respecting copyright laws. Strong copyright laws in the US and EU[i] give copyright holders monopoly rights, not just on content, but also on the means to protect it. One of the tools deployed in the name of preventing copyright infringement are digital rights management systems (DRM), which can take the form of technological locks, unique identifiers like watermarks and technical implementations to monitor and control use of the product. A wide variety of technologies are involved in DRMs and they are increasingly embedded in consumer goods, such as music players, CDs and Ebooks. There are also proposals to embed DRMs in all digital TV's. These technologies have failed at every turn in the field: every work ever "protected" by DRM is currently available for download from P2P networks on the Internet, and there is no indication that these systems will ever work at their stated objective of stopping indiscriminate redistribution. However they impose costs on consumers by restricting use and curtailing competition.

Current technological measures designed to enforce copyright in the digital environment threaten core exemptions in copyright laws for disabled persons, libraries, educators, authors as well as consumers and undermine privacy and freedom. DRMs enable their controllers to make their own private rules and in so doing can override electronically not only the legislation of their own countries, but also that of other countries in relation to consumer protection and copyright exemptions.

A consumer who seeks to secure his interests and rights is restricted by technological and legal barriers that further curtail users' rights provided under the law.[ii] Consumers are faced with a triple lock between them and the exercise of their rights: copyright protection, technological restriction (by using DRMs) and legal

protection of the technological restriction (anti-circumvention provisions). This puts consumers in an impossible position. They are locked out of the exercise of their rights but cannot break the lock in order to do so. Even if a consumer is aware that their rights are being wrongly limited there is no consumer-friendly and workable means for them to exercise their rights. This is a matter of concern for TACD as US and EU consumers are amongst the first to face DRMs. Current DRMs have failed to stop professional infringements as every DRM 'lock' has been broken, but they have successfully limited the rights of ordinary consumers. They have created a mindset whereby rights holders impose stronger and stronger control to limit use rather than innovating to meet consumer demand. In fact, DRM may be part of the problem, pushing frustrated consumers into the arms of unauthorized channels like music download sites.

We believe that policymakers have failed to properly view the purpose and benefit of DRMs from the consumer perspective, and that current laws provide little effective consumer protection. Policymakers are allowing DRMs to set the law not just in relation to copyright but also general consumer and competition law. Instead, they should require them to be developed, implemented and run according to well-established principles of balance, fair description and consumer choice.

Risks for Consumers

Access to and use of content

DRMs are not just used to limit access to content. They are also used to prevent ways of using the product that consumers expect or are given by copyright law such as private copying (including to make private back up copies) lending, excerpting, sampling or other content modification, and resale and donation. In order for consumers to benefit from the digitalisation of content and the many and varied types of different digital equipment available, they expect to 'format-shift' (transfer content onto other devices), 'space-shift' (view content at a location remote from the place where it is stored), and 'time shift', (record for use at a later time, such as recording a TV programme). Restrictions on usage affect not just individual purchasers but also libraries and educators and prohibit access to knowledge. Many DRMs on the market now prevent these uses, such as copy-protected CDs that won't play on computers and DVDs that are encoded to only play in certain regions of the world.

DRM systems also define social entities such as 'household' and 'families', but these definitions are often narrow or restrictive. Such systems contain upper limits on the size of 'families', the number of physical locations that can be considered part of the 'household', and even on the number of times that a device can leave a single household - in effect a technological limit on custody arrangements, divorce and property ownership. TACD is concerned that, in Europe, the DVB standard is developing the concept of an 'authorised domain' which will define when, where and who can use a piece of content. It is unacceptable for an unaccountable industry group to seek to mandate definitions of such social and cultural importance. Such unprecedented interference into personal life goes way beyond the justification for the protection of copyright.

Consumers with disabilities: digital technologies have the potential to offer many benefits for people with sensory or mobility impairments. However, DRMs can prevent those benefits from being realised. DRMs can block the use of assistive technologies[iii] employed by people with disabilities including blind and deaf people. For example, they can make conversion into other formats such as Braille either impossible or expensive and difficult.

Privacy
DRMs incorporate mostly the collection and processing of personal data with the tendency to render anonymous or pseudonymous transaction in the digital environment impossible.

DRMs that are designed to generate and transmit huge quantities of data about the personal use of a product or service carry out an unprecedented level of monitoring. It's a little like having an irremovable camera owned and operated by the publisher attached to every book to monitor and record how its used and by whom. The consumer will often not be aware of these monitoring devices or the information they collect and will have no control over its use by the DRM controller

Moreover, DRMs that are entangled with intellectual consumption and do monitor user behaviour invade a sphere with sensitive personal data potentially revealing political convictions, religious or philosophical beliefs or sexual orientation.

Under the umbrella of copyright enforcement DRMs can be abused to profile consumers by collecting and reporting back personal data or data that can be linked to an individual. DRMs can therefore operate as 'spyware' which serves purposes that are different to DRMs original purpose and are harmful for consumers.

Interoperability
The ability for consumers to use DRM-locked products on different devices and in different ways crucially depends on the ability of these products to work on all these different devices. Many DRMS on the market lock consumers into using a particular provider or piece of equipment, such as Apple iTunes, as they will not play (interoperate) on other devices. Others prevent use at all. Many DRMs require specific software platforms to work, which means that certain users are excluded from using the product - no DRM systems work on Linux or other open or free software platforms. Indeed, the purpose of DRM is to block interoperability: that is, to stop manufacturers from interfacing their equipment with existing equipment, except on terms set out by rights holder companies.

Transparency and Contract terms
All consumer experience of DRMs has been negative, because of unexpected and unwanted usage restrictions, and has been fuelled by a lack of transparency about the effect of the DRMs. Such secrecy is counterproductive if DRMs are seeking to gain wider acceptance and it has lead to growing consumer resistance. Protection of copyright should not be allowed as an excuse to undermine the principle applied to other consumer products - that a product's function, including any limitations, should be clearly stated before a consumer buys it. Information about limitations, however, is a necessary but insufficient condition. Any limitations must respect consumer usage expectations and copyright exemptions.

The terms of a DRM system can be altered after the purchase, often without the knowledge or express consent of the consumer. For example, what a consumer can record or the number of copies they can make can be changed by a software download from the DRM controller, or by the expression of hidden "flags" in content -- a consumer has no way of telling in the shop which restrictions can be applied to the content on the device they are paying for, no way to know if, for example, a music label can flag a particular piece of music for "no backup" or whether a movie company can flag a particular show for "no record."

In addition, a provider may use contract terms under which a consumer signs away copyright exemptions such as private use. These contractual terms can be written in such an unintelligible form that the consumer may not be aware of their actions. Alternatively, the consumer may have no option but to agree because there is no other means of accessing that content and the contracts are non negotiable.

Security issues
Some DRM systems can impair or limit the use of other security measures in a consumer's equipment, such as security settings on a computer. They can also require an internet connection for registration that could leave a computer open to external attack. In neither of these cases is the consumer, if they are even aware of it, able to control these risks.

Anti-competitive behaviour
Supporters of DRMs claim that they will bring a wider choice for consumers to access and use digital products. The reality for consumers using many current DRMs is the opposite. DRMs are used to split current consumer usage rights so they can be exploited based on different pricing models. This will have the result of consumers having to pay more to do things that they currently expect to be a normal function of the product. DRMs may be used for price discrimination and market segmentation, such as the regional encoding used on DVD, and iTunes' higher prices for downloading in the UK. DRMs can restrict the creation of a single market within the EU and undermine the goals of a global trading market. DRMs can be used anti-competitively to lock out competitors or to shut out or control complementary products. For example, other content producers, like games manufacturers or makers of digital television, will have to contract with DRM controllers in order to access their content. Restrictions on competition threaten product diversity and choice for consumers.

Moreover, DRM licensing cartels, such as those governing the licensing of DVDs, and interfaces like HDMI and DTLA, and recording technologies like DVHS, are controlled by incumbent technology and entertainment companies. New market entrants who wish to add functionality to a media device -- say, by building a hard-drive-based DVD "jukebox" -- are inevitably stymied in their efforts because the licensing cartels will not allow them to lawfully produce such a device. In general, licenses that extend the functionality of cartel-licensed technologies, like DVD, are only approved if they are proposed by companies or consortia that are represented in the cartel: the DVD licensing body only gives licenses to innovate to companies that are members of the DVD licensing body.

Redress
DRM systems shift the burden of proof onto consumers who are the weaker party in any litigation and, as is well known, are often reluctant to litigate due to concerns over costs. Previously the burden was on the rights holder to enforce its rights against infringers, which required them to establish proof of infringement and also provided defences to consumers. Under the anti-circumvention provisions in US and EU legislation the burden is now on consumers to enforce their rights if a DRM scheme infringes them, through procedure that is so costly that is has never successfully been managed.

TACD endorses the comment in the Commission funded Indicare report[iv] on digital rights management and consumer acceptability that 'currently costs seem to outweigh the benefits of DRM from a consumer point of view. Many arguments in favour of DRM either do not bear a closer examination or need time and further development until they become valid.'

Recommendations

TACD urges the governments of the United States and the European Union to set certain preconditions that DRMs have to meet in order to qualify for legal protection. The preconditions recommended by TACD are set out below:

Access to and use of content
DRM systems that are capable of being used in excess of what is necessary to protect copyright will not receive the privilege of anti-circumvention protection.

DRM systems that define social entities such as 'household' and 'families' in their technology, and that define these entities more narrowly or restrictively than have been defined in local law or custom will not receive the privilege of anti-circumvention protection.

DRM systems that block the use of assistive technologies employed by disabled people will not receive the privilege of anti-circumvention protection.

Privacy
DRMs should be certified as compliant with data protection rules or privacy rights by the Data Protection Registrar or privacy enforcement agency before they are introduced onto the market. By building privacy interests into the design of the DRM, privacy rights may be enforced more effectively.

In particular, DRM systems should not use registration, use data, or other personal information for secondary purposes without first obtaining the individuals' informed and voluntary consent. That is, the individual should be able to use the media without consenting to marketing or other secondary uses of their personal information.

Interoperability
DRMs that restrict the normal expected usage of that product, such as space and time shifting, should not receive the privilege of anti-circumvention protection.

DRMs whose licensing and implementation terms preclude the use of Free and Open Source Software (FOSS) will not receive the privilege of anti-circumvention protection.

Transparency
DRM systems that are 'updated' without a user's consent will not receive the privilege of anti-circumvention protection.

All equipment containing DRMs must be clearly labelled showing what uses are allowed and what equipment it will or will not work on. DRM systems that are marketed without adequate disclosure of restrictions will not receive the privilege of anti circumvention protection.

Security
DRM software should not hamper or limit the use of software protection software on consumer computers. DRMs should not bring new vulnerabilities into consumers computing equipment and such systems must not interfere with consumers' ability to set and retain their own polices and levels of security for their own machines.

Anti-competitive behaviour
The potential anti-competitive effects of DRMs should be reviewed. In particular, a competition investigation should be undertaken into the licensing terms for DRM technology and the effect on competitors and complementary producers.

Redress
Consumers must have clearly defined and enforceable consumer rights that cannot be overridden by contract terms, DRM systems or other technological measures. They should not have to rely, as now, on the restraint or goodwill of the rights holders or, as in Europe, on the whims of each Member State as to which consumer exemption they will allow.

Among the consumer rights that should be clearly expressed:
right to private copy
right to fair commercial practices
right to be informed and refunded for faulty products
right to privacy and data protection.
right to free speech

A simple and speedy alternative dispute resolution system should be established for cross border DRM disputes so consumers do not have to rely on costly litigation for low value disputes, whilst retaining the right to use court action as a last resort.

Associated Files: see the end of this document

---

[i] US: Digital Millennium Copyright Act. EU: Directive 2004/48/EC 'the Copyright Directive'
[ii] 'Digital rights Management and Consumer Acceptability' State of the Art report December 2004-Indicare – 'The Indicare report'. (http://www.indicare.org.) The publication is a deliverable of the INDICARE Project that is financially supported by the European Commission, DG Information Society, as an Accompanying Measure under the econtent Programme (ref. EDC-53042 INDICARE/28609). INDICARE - The informed dialogue about Consumer Acceptability of Digital Rights Management Solutions.
[iii] Assistive technology is any device or piece of equipment that is used to maintain or improve the functional capabilities of a person with a disability
[iv] The Indicare report. Ibid