DIGITAL RIGHTS MANAGEMENT SYSTEMS AND DIGITAL PIRACY – ARCHRIVALS OR UNINTENDED ALLIES?

by

ROBERT KUTIŠ*

Although Digital Rights Management systems were often triumphantly presented as a panacea for digital piracy they actually did not meet their objective. Moreover, number of products failed on the market because of the use of the DRM systems and various studies indicate that usage of such systems may indirectly act as a positive driver of digital piracy. With their further development DRM systems considerably evolved and became more sophisticated. Combating the piracy is no more their main aim and they became an important part of the competition strategies and business models of many companies. At the heart of this paper lies the question whether DRM technologies inherently include special characteristics which may cause that they act as a driver of digital piracy and whether were those characteristics identified by DRM system implementers and subsequently mirrored in further development of current DRM systems.

KEYWORDS

Digital piracy, Digital Rights Management, user´s privacy, interoperability, limitations of the copyright, characteristics and features of Digital Rights Management systems, potential ambiguous effect of Digital Rights Management systems, recent developments, triple protection

1. DIGITAL RIGHTS MANAGEMENT SYSTEMS – BY WAY OF INTRODUCTION

Digital Rights Management ("DRM") systems can be defined as a generic name for the range of architectural controls in software and hardware

* Mgr. Robert Kutiš, LL.M. , kutis.robert@gmail.com

which allow control of distribution and access to content, monitor its use and prevent unauthorised usage of this protected content or its usage on unauthorised devices.[1] However, DRM systems are often understood as technologies that only limit the use of digital content or devices. Such insight does not take into consideration the second aspect of the Digital Rights Management systems, that they also provide information to the users about permitted uses of the content and devices and also about ownership of the copyright, facilitating use and clearance of rights[2]. By recognition of those two aspects DRM systems can be divided into two general groups:

Rights management systems (or Rights management information), which serves to the mentioned second aspect of DRM and

Technological protection measures ("TPM"), the purpose of which is to provide means for the owners of the copyright and related rights to prevent unauthorised usage of protected content "by limiting access, copying or other unauthorised actions by end users conditional on compliance with licensing conditions applied by the owner of rights" [3].

DRM systems can be also recognized as:

- DRM in hardware - as a part of the equipment or hardware which is used to play digital content[4]. The region-coding technology for DVD's can serve as an example. Region code included in DVDs and also in DVD players is restricting the area of the world in which the DVDs can be played[5].

- DRM in software – as technologies whose purpose is to prevent copying of the content or to control or restrict certain use of protected digital media. DRM in software is used more often than DRM in hardware[6], mainly in connection with music and e-books.

In the following text, the terms Digital Rights Management systems and Digital Rights Management technologies will be used as terms for both DRM systems with management functions and Technological protection measures, as well as DRM in hardware and also DRM in software.

DRM systems were developed as the second modality of content protection after the first form, the law based copyright protection, failed to do it sufficiently. However, not even this technological protection was enough to bring success adequate to the amount of time and resources spent on development and introduction of it, mainly because no DRM system is unbreakable - no matter how robust the technological protection is. According to the available scorecard from 2007 every single existing DRM system had been cracked[7] and nothing changed in this respect until nowadays. Simple

DRM systems can be broken in seconds even by very primitive means, as holding the shift key while inserting the CD into the CD-ROM drive[8] and the more complex ones can be cracked in weeks or rarely in months[9]. Thus, without the legal protection against circumvention, technological protection represent only small, but costly speed bump on the digital highway leading to the protected content. Therefore, it was not surprising that members of the content industry lobbied for legal protection of DRM systems like they successfully did before in connection with the protection of the cable and satellite television broadcast scrambling technologies[10]. Although the issue of legal protection against DRM circumvention caused big hesitation and discrepancy between the delegates of the WIPO conference in Geneva, effort of the content industry was successful and it was finally agreed to add Articles 11 and 12 to the 1996 WIPO Copyright Treaty and Articles 18 and 19 to the 1996 WIPO Performances and Phonograms Treaty. [11] Those articles then stimulated national and regional legislation which implemented those treaties, among others Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the Harmonization of Certain Aspects of Copyright and Related Rights in the Information Society ("Copyright Directive") in the EU and national laws implementing it.

2. CHARACTERISTICS OF DRM SYSTEMS POTENTIALLY CONTRIBUTING TO DIGITAL PIRACY

However, neither introduction of such triple protection[12] solved all the problems. Quite the contrary - a number of products failed on the market because of the draconian DRM systems[13] and some studies indicate that robust DRM systems could indirectly act as a positive driver of digital piracy.

University of Cambridge researcher Patricia Akester noted in her report from 2009 that problems resulting from DRM protection of the content often drive individuals to obtain illegal copies, free of DRM[14]. As one of many examples, Akester cited a situation in which a blind person who bought a legal electronic copy of the Bible from Amazon could not utilize text-to-speech function. Since Amazon's policy is not to refund eBooks once they've been downloaded and the publisher also provided little help referring her back to Amazon, the individual in question ended up tracking down an illegal copy without the limitation of text-to-speech function[15].

Also OECD in its contribution "Piracy of Digital Content" noted that DRM may reduce the degree of technical availability and mobility of digital products and thus act as a positive driver of piracy[16]. Finally, the most recent study – research carried out by Rice and Duke University called "Music Downloads and the Flip Side of Digital Rights Management Protection" - used analytical modeling to examine how piracy is influenced by the presence or absence of DRM restrictions and showed that piracy actually decrease when a company allow DRM-free downloads[17].

Therefore, with regard to above findings, following two questions arise: What characteristics of DRM systems can make them to act as a positive driver of digital piracy? And are those findings mirrored in the recent developments in the field of DRM systems? The answers to both of these questions should be found in the following text.

2.1 THE EASE OF DRM SYSTEMS CIRCUMVENTION AND PERFORMANCE PENALTIES OF ROBUST DRM SYSTEMS

The first characteristic important from the point of the view of DRM systems and digital piracy interrelation is the above mentioned ease of their circumvention.

Vulnerability of the DRM systems lies in the basic structure of functioning of the DRM systems and the ease of the crack-solutions distribution. DRM systems provide their recipients with ciphertext, the cipher and the key, so in case, when the recipient is also an attacker "the secret isn't a secret anymore"[18]. Moreover, even if only a small group of users is able to circumvent the DRM system and to transform protected content to an unprotected form, this transformed content, and also the crack itself, can be easily distributed to the less skilled users[19]. Although implementation of the robust DRM systems may seem as unavailing, according to some authors it does not invalidate its use to protect the content[20]. The purpose of the DRM technologies can lie not in the effort to unbeatably secure the content, but in the endeavour to make circumvention harder for most of the users and together with the anti-circumvention provisions, make them aware that they will break the law if they would try to circumvent the DRM systems[21]. However, such purpose of DRM systems can be then interpreted as endeavour to keep the honest people honest, what is as Cory Doctorow aptly wrote - like keeping a tall user tall[22].

The fact that DRM systems are easy to circumvent may be linked to piracy in two ways. Firstly, volume of piracy and pirated works is not influenced by the use of DRM technologies so unprotected versions are still easily available and represent competition for legal, DRM protected versions.

Secondly, when DRM implementers try to enhance efficiency of the DRM systems (in other words to make the unauthorised use of the protected content as hardest as possible) it is always the legitimate user who suffer from the restrictions in the end. The obvious link can be seen between the demand for the pirated copies of the works and the robustness of DRM systems. Experience with some extremely robust DRM systems suggests that when the DRM systems turn up to be draconian also for the legitimate users demand for pirated copies increases rapidly. Examples may be seen mainly in the fields of the music or game industry. After the release of the game Spore protected with the revolutionary strict DRM system enabling only three activations, the game became the most pirated game in the year 2008 and very probably also in history[23]. The game also got the worst score ever in the customer reviews on Amazon.com and overwhelming majority of those "one star reviews" were because of the DRM[24]. As another example may serve the Coldplay CD "X&Y" protected by robust DRM system which among other restrictions made the CD unplayable in some CD players, DVD players, car CD players, game consoles and also did not enabled the conversion of the CD tracks to mp3 format or to copy the CD using Macintosh PCs. Immediately after the release users started to look for a ways how to circumvent the Macrovision DRM system, and in short time they succeeded[25]. The issues with robust DRM protection are intertwined with another problematic characteristic of the DRM systems and hence with the fact that DRM systems often do not enable the exercise of limitations of copyright. Simply put, by being algorithmic, DRM systems tend to be less flexible[26]what means that limitations are often overlooked[27]. The result of the disappointment or frustration[28] caused by the performance penalties connected with the robustness of DRM systems is often the consumer rejection of the legitimate content protected by DRM technologies. Such situation may subsequently lead to digital piracy, mainly if the only source of DRM-free content represents illegal copies of the works.

2.2 THE LACK OF INTEROPERABILITY

Interoperability means that "one system can receive, read, interpret, and act on the copy protection and rights management information that comes from the system of another vendor"[29]. Interoperability is connected with user-friendliness of the products[30] and among other things determines how much should a consumer worry that he would not be able to play his legally obtained DRM protected songs on his MP3 player, read the DRM protected book on his e-book reader or play purchased DRM protected music CD on his computer, or in his car. Consumers want to be able to use their legally purchased content wherever is needed, on any appropriate device and possibly to share this content with their friends and family[31], but early DRM technologies often stood in the way. For example Sony´s portable player – the Music Clip was not able to play even songs in MP3 format because of the draconian anti-copying technology used[32].

In fact, non-interoperability often leads directly to the circumvention of the DRM systems and also to piracy. Obvious example is Content Scramble System ("CSS") and the DeCSS computer program. CSS function was to limit the range of devices which are able to play DVD disks. User was not able to play DVD content unless he was using a device that could decode the CSS routines. The only operating systems which were able to play thus protected DVD discs were only Windows and Macintosh. Linux PCs operating system was somehow "forgotten" in this, so machines with this operating system were not able to play content of the DVD. This gave rise to the DeCSS program, which disabled the encryption system on a DVD disk by cracking the CSS system. DeCSS enabled to DVD content to be played on any machine[33].

Similar examples can be found in the field of the music industry, both involving Apple´s iTunes FairPlay DRM system. Firstly, there was a case that iTunes software was not available for Linux operating system, which led again to the circumvention of the Apple´s FairPlay DRM system[34]. Second example is connected with the company RealNetworks and their program called Harmony. This program was developed on the base of reversed-engineering of the FairPlay DRM system. Purpose of the Harmony was to enable users to buy music from Real´s Music Store and play it on the iPods. Without Harmony iPod owners could buy and play only the music bought through Apple´s iTunes service[35]. Harmony brought more interoperabil-

ity and freedom for the user, because it offered another source for the iPod owners.

As those examples suggest, non-interoperability frequently leads to circumvention of the DRM systems[36] and force users to seek help and solutions in the field of piracy. It is possible, that consumer´s dissatisfaction will foster standardisation and interoperability, but until that will happen, lack of interoperability of the DRM technologies will continue to steer consumers into the arms of piracy.

2.3 SOPHISTICATED DRM SYSTEMS AND THREATS FOR USERS´ PRIVACY

Naturally, the content industry recognised above mentioned problems and after some time abandoned the idea that massive DRM systems are the new panacea to the digital piracy and realised that not the development of the robust technological protection measures, but the creation of a business model competitive to the P2P file sharing networks did present the proper response. Thus, DRM systems implementers refocused from heavy technological protection to a more refined system of rights management and DRM systems became more sophisticated. That gave rise to the heyday of the online retailers like Amazon.com, Apple´s iTunes Store, Rhapsody, Napster, Movielink or CinemaNow. Although the new development in the design of the DRM systems brought some flexibility and enabled more relaxed usage of the content in many ways, it did not rid them of the pitfalls. Some problems which existed before continue to persist in bigger or smaller scale[37] and even some new arose. DRM system implementers still stick to the endeavour to keep honest users´ honest but combating piracy is no more the solely function of DRM systems and they became inherent part of the business models and distribution schemes. Interoperability issues and performance penalties caused by DRM systems were significantly suppressed by new DRM systems, however the interoperability between various DRM systems is sometimes still negligible; not because of rigidity and robustness of DRM technologies, but because a business decision behind. Example can be endeavour of Apple´s iTunes DRM technology, which dictated which portable players (Apple´s iPods) could be only used to play music files downloaded from iTunes.

Thanks to such refocus content industry identified novel content-control opportunities, methods of charging providing them with higher revenues or

data mining possibilities offered to them by the new design of the DRM systems integrated in the online services and without hesitation started their further development and massive exploitation[38].

Privacy is thus nowadays linked to the copyright enforcement as never before and privacy issues became the talk of the day with regard to sophisticated DRM systems which may, and also very often do, involve the collection and further processing of vast amount of personal data and enable implementers of DRM systems to closely monitor and track the use of digital content and increasingly also the behaviour of users. Various types of information are collected by means of current DRM systems. This information may relate to identification data often needed for purchase of the content, such as names, credit cards numbers, age, address, e-mail address, but also to user´s hardware, preferences, habits or access and usage patterns[39]. The peril of such data collection lies in the various consequences on privacy; DRM systems may present constant surveillance of what people view, listen or read, far beyond the extent what hitherto has been usual[40] and adversely affect privacy related interests as autonomy, integrity or human dignity[41]. Collected personal data are also often used or sold to the third parties for secondary purposes such as targeted advertising or profiling of users´ access and usage patterns or preferences[42]. Usage of this data also contributes to limiting access to content and price discrimination[43]. Moreover, it may also have serious implications on democratic society and expression of "non-conformist opinions and preferences"[44]. Content distributors claim that they need this data as the basis for their various operations –to enable online purchases of the content[45], offer "personalized services" in order to simplify the ordering or downloading of the content and therefore provide better services, improve models of traffic and infrastructure of the online services, to more effectively impose restrictions to the use according to the rules of content usage and finally, to combat piracy[46]. Sometimes, it is even proclaimed that without tracking of content, usage rights could not be managed[47]. Nevertheless, the main reason of interest lies in the economic value of the data and business opportunities offered to the content industry by collection and processing of this information. Collected data enable profiling of the users and providing targeted marketing on the base of the information about users´ individual preferences, new methods of charging providing higher sales and mainly facilitate price discrimination[48]. Information recorded by

the DRM systems offers better image of individuals´ willingness to pay for the content to the content industry and thus enable to charge every individual with different price set near to the maximum limit of his abilities and alacrity[49]. Collected data have also value as an economic asset.

Such development is confirmed by various studies and examples from practice. According to the study from the year 2003[50], carried out by Burstein, Han and Mulligan from University of California, each of the scrutinized services required installation of proxy software and service proxies read the index.dat files[51] persistently during every stage of use of the protected content what may suggest monitoring of users´ browsing habits[52]. It also states, that all examined DRM systems carried out surveillance of protected content usage, mainly in connection with type of the content and time, frequency and location of use[53]. Actions taken against Sony BMG for its use of the Extended Copy Protection ("XCP") and MediaMax DRM systems were mere confirmation of such practices. XCP system was used on some Sony-BMG music CDs which, after the CD was played in the computer, installed a root-kit[54]like program into the user´s computer hard drive[55]. This software, presenting a security risk for the computers without means to uninstall it, had been covertly gathering data and sending them "back home" to the company[56]. Moreover, everything was done without users´ knowledge; the end-user license agreement did not contain any provision entitling Sony to put software on the users´ computers[57]. However the whole revelation of XCP DRM system spying on users´ computers resulted in notable disapproval, Sony-BMG continued to use the even more hidden, but functionally very similar MediaMax[58] DRM system up to its detection[59]- causing, understandably, another scandal. Even those public relations hassles did not change content industry approach to the privacy issues associated with the use of sophisticated DRM systems. More recent Canadian assessment on use of the DRM systems and its implications for user´s privacy[60] came up with conclusions that "privacy-based criticisms of DRM are well-founded"[61] because during examination authors observed tracking of usage and surfing habits, generally without options to opt-out of unnecessary collection, use and distribution of data[62]. Moreover, assessment pointed out a growing trend in DRM systems that involved internet authentication, surveillance and tying of content to an online platform[63]. Surprisingly, examination did also uncover a number of third party communications which were not explained in corres-

ponding privacy policies[64]. These conclusions seems to be very close to the standard industry practice of nowadays, what can be affirmed by very recent cases of privacy threats connected with use of SecuROM Product Activation DRM system[65], Amazon´s Kindle devices[66] or new Ubisoft´s DRM systems[67].

Until consumers would be able to legally obtain copies of works without the similar interferences into their privacy, DRM systems remains to be felt as an intrusive surveillance of consumer´s lives and thus may lead to obtaining pirated content. However, at this point of the development I think that risks of current DRM systems for users´ privacy are far more serious than the risk that "privacy unfriendliness" will become the most significant characteristic making DRM systems to act as a positive driver of digital piracy.

3. CONCLUSION

The piracy of digitized content gave rise to the creation of the Digital Rights Management technologies which were supposed to be the decisive technological response to this undesirable phenomenon. However, their introduction to practice proved that DRM systems do not represent the panacea for digital piracy as was often triumphantly presented. DRM technologies actually failed in this main aim and transformed to something significantly different. Combating the piracy is not more the main aim of the DRM systems and these technologies themselves became an important part of the competition strategies and business models of many companies. Such shift in logic may be linked to the fact that DRM systems inherently include special characteristics which, as reasoning and the examples included in this paper confirms, can make them act as a positive driver of digital piracy. The ease of DRM systems circumvention and performance penalties of robust DRM systems often result to consumer rejection of the legitimate content protected by DRM technologies and subsequently to obtaining easily available pirated copies. Also lack of interoperability may force users of DRM protected content to seek help and solutions in the field of piracy. Acknowledging that and also the fact that DRM systems will never secure absolute protection of content, DRM system implementers started to use DRM systems more as a tools contributing to the functioning of new distribution channels created by them rather than just as a form of copyright protection. Although such further development of DRM systems enabled more relaxed use of

protected content, since DRM systems became more flexible and less restrictive, it may be compared to the stone dropped to the water – the ripples spread outward and bestirred waters far away from the immersion, including previously quiet waters of the users´ privacy. Amount of data processed by DRM systems increased rapidly what understandably raises concerns about users´ privacy. Thus, although adverse effects of above mentioned characteristics were partially reduced by introducing of more sophisticated DRM systems, privacy issues with regard to current DRM systems usage may act as even stronger incentive to obtain pirated copy of desired content. Such risk is even bigger taking into account increasing awareness of privacy and data protection importance in today´s information society among general public.

Nevertheless, consequences for digital piracy may be seen as a molehill rather than a threatening mountain when compared with dangers and consequences of current use of such privacy intruding DRM systems for individuals.

REFERENCES

[1]See: OECD Publishing, 2009 Piracy of Digital Content, Paris. p. 57 Westbrook, S (2009) "Composition and Copyright, Perspectives on Teaching, Text-making and Fair Use", State University of New York Press, Albany: NY. p. 57

See also: Becker, E., Buhse, W., Günnewig, D., Rump, N. (eds) (2003) "Digital Rights Management, Technological, Economic, Legal and Political Aspects" Springer – Verlag Berlin Heidelberg, Berlin. p. 4

[2] OECD Publishing, 2009, Piracy of Digital Content, Paris. p. 57

[3] OECD Publishing, 2009, Piracy of Digital Content, Paris. p. 57

[4] Hofman, J. 2009, Introducing Copyright, A plain language guide to copyright in the 21st century, Commonwealth of Learning, Vancouver. p. 112

[5] For more see: Doctorow, C. 2008, Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future, Tachyon Publications, San Francisco. p. 12

[6] Hofman, J. 2009, Introducing Copyright, A plain language guide to copyright in the 21st century", Commonwealth of Learning, Vancouver. p. 112

[7] Wolfe, A. 01.08.2007, DRM Scorecard: Hackers Batting 1000, Industry Zero, InformationWeek, http://www.informationweek.com/blog/main/archives/2007/08/drm_scorecard_h.html [Accessed: 03.09.2011]

[8] For more see Halderman, J. A. 2003, Analysis of the MediaMax CD3 Copy-Prevention System, Department of Computer Science, Princeton University. https://jhalderm.com/pub/cd3/ [Accessed 03.09.2011]

Or Deane, 08.10.2003, DRM defeated by exotic hack: The Shift key", Gadgetopia. http://gadgetopia.com/post/1233 [Accessed 15.4.2011]

[9] Doctorow, C. 2008, Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future ,Tachyon Publications, San Francisco. p.7

[10] Esler, B.W. 2002, Technological Self-Help: Its Status under European Law and Implications for U.K. Law. Proceedings of the 17th BILETA Conference, Free University, Amsterdam. p.5

[11] Esler, B.W. 2002 Technological Self-Help: Its Status under European Law and Implications for U.K. Law. Proceedings of the 17th BILETA Conference, Free University, Amsterdam. p.7

[12] As a three level protection of content encompassing copyright protection, technological protection in the form of DRM systems and legal protection of the technological protection by means of anticircumvention legislation.

[13] Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p. 213-214

[14] Akester, P. 2009, Technological accommodation of conflicts between freedom of expression and DRM: the first empirical assessment, Centre for Intellectual Property and Information Law, University of Cambridge, Cambridge, UK.

[15] Akester, P. 2009, Technological accommodation of conflicts between freedom of expression and DRM: the first empirical assessment, Centre for Intellectual Property and Information Law, University of Cambridge, Cambridge, UK. p. 47-49

[16] OECD Publishing, 2009, Piracy of Digital Content, Paris. p.58

[17] Vernik D.A., et al. 2011, Music Downloads and the Flip Side of Digital Rights Management Protection. Marketing Science mksc.1110.0668. Published online before print October 13, 2011, http://mktsci.journal.inform-

s.org/content/early/2011/10/13/mksc.1110.0668.full.pdf+html [Accessed 08.11.2011]

[18] Doctorow, C. 2008, Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future ,Tachyon Publications, San Francisco. p. 6-7

For more see also: Felten, E. 03.12.2002, Why Unbreakable Codes Don't Make Unbreakable DRM, Freedom to Tinker - Princeton's Center for Information Technology Policy. https://freedom-to-tinker.com/blog/felten/why-unbreakable-codes-dont-make-unbreakable-drm [Accessed 03.09.2011]

[19] Becker, E., Buhse, W., Günnewig, D., Rump, N. (eds) 2003, Digital Rights Management, Technological, Economic, Legal and Political Aspects, Springer – Verlag Berlin Heidelberg, Berlin. p. 224

[20]Hinduja, S. 2006, Music Piracy and Crime Theory, LFB Scholarly Publishing LLC. New York. p. 144

[21] Akester, P., Akester, R. 2006, Digital Rights Management in the 21st Century", European Intellectual. Property Review 28(3). p. 159-168. p. 8

[22]Doctorow, C. 2008, Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future, Tachyon Publications, San Francisco. p.8

[23] Greenberg, A., Irwin, M.J. 09.12.2008, Spore's Piracy Problem, Forbes. http://www.forbes.com/2008/09/12/spore-drm-piracy-tech-security-cx_ag_mji_0912spore.html [Accessed 27.03.2011]

Ernesto, 13.09.2008, Spore: Most Pirated Game Ever Thanks to DRM, TorrentFreak. http://torrentfreak.com/spore-most-pirated-game-ever-thanks-to-drm-080913/ [Accessed 27.03.2011]

Kingsley-Hughes, A. 15.09.2008, Spore DRM could kill PC gaming, ZD Net. http://www.zdnet.com/blog/hardware/spore-drm-could-kill-pc-gaming/2617 [Accessed 15.04.2011]

[24] Nyquist, G. E. 11.09.2008, I Really, Really want to love this game. Amazon.com, http://www.amazon.com/gp/cdp/member-reviews/A2K5RVNC6R93EA/ref=cm_pdp_rev_title_1?ie=UTF8&sort_by=MostRecentReview#R2MEOXG6BMBD02 [Accessed 15.04.2011]

[25] See: Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p.244

[26] Johns, A. 2009, Piracy, The Intellectual wars from Guttenberg to Gates, The University of Chicago Press, Chicago. p.506

[27]Or in many cases not recognized at all.

[28] For example 75 percent of calls to customer support phone service of the server Musicload.de in the 2007 were because of the frustration from the DRM.

Fisher, K.18.03.2007, Musicload: 75% of customer service problems caused by DRM. Ars Technica. http://arstechnica.com/tech-policy/news/2007/03/75-percent-customer-problems-caused-by-drm.ars [Accessed 27.03.2011]

[29] Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p.248

[30] Becker, E., Buhse, W., Günnewig, D., Rump, N. (eds) 2003, Digital Rights Management, Technological, Economic, Legal and Political Aspects Springer – Verlag Berlin Heidelberg, Berlin. p.13

[31] Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p.219-220

[32] See: Doctorow, C. 2008, Content, Selected Essays on Technology, Creativity, Copyright, and the Future of the Future, Tachyon Publications, San Francisco. p. 47

[33] Lessig, L. 2001, The future of ideas: the fate of the commons in a connected world, Random House Inc., New York. p.189

[34] Akester, P., Akester, R. 2006, Digital Rights Management in the 21st Century, European Intellectual. Property Review 28(3). p. 159-168. p.6

[35] Boyle, J. 2008, The Public Domain, Enclosing the Commons of the Mind. Yale University Press. New Haven, CT. p. 110-111

[36] Read also: Akester, P., Akester, R. 2006, Digital Rights Management in the 21st Century, European Intellectual. Property Review 28(3). p. 159-168. p. 7

[37] For example problems with carrying out the private use, or fair use, copyright exceptions.

[38] See also: Odlyzko, A. 2007, Digital rights management: Desirable, inevitable, and almost irrelevant. Digital Technology Center, University of Minnesota. http://www.dtc.umn.edu/~odlyzko/doc/drm2007.pdf [Accessed 12.09.2011]

[39] See also: Drossos, L., Papatheodorou, T., Sioutas, S., Tsolis, D. 2009, Digital Rights Management for E-Commerce Systems. Information Science Reference, Hershey, PA. p.351

[40] Bygrave, A.L. 2002,The Technologisation of Copyright: Implications for Privacy and Related Interests, Originally published in European Intellectual Property Review.vol. 24, no. 2. pp. 51–57. p.4

http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf[Accessed 02.10.2011]

See also: Cohen, J.E. 1996, A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, Originally published 28 Conn. L. Rev. 981. 1996. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990 [Accessed: 03.10.2011]

[41] See: Becker, E., Buhse, W., Günnewig, D., Rump, N. (eds) 2003, Digital Rights Management, Technological, Economic, Legal and Political Aspects, Springer – Verlag Berlin Heidelberg, Berlin. p.422

[42] Akester, P., Akester, R. 2006, Digital Rights Management in the 21st Century, European Intellectual. Property Review 28(3). p. 159-168. p.6

[43] Akester, P., Akester, R. 2006, Digital Rights Management in the 21st Century, European Intellectual. Property Review 28(3). p. 159-168. p.6

See also: Odlyzko, A. 2007, Digital rights management: Desirable, inevitable, and almost irrelevant. Digital Technology Center, University of Minnesota. http://www.dtc.umn.edu/~odlyzko/doc/drm2007.pdf [Accessed 12.09.2011]

[44] Bygrave, A.L. 2002, The Technologisation of Copyright: Implications for Privacy and Related Interests, Originally published in European Intellectual Property Review.vol. 24, no. 2. pp. 51–57. p.4-5

http://folk.uio.no/lee/publications/technologisation_copyright_eipr_final.pdf [Accessed 02.10.2011]

See also: Bygrave, L.A., Koelman, K. J. 1998, Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management Systems. Institute for Information Law, Amsterdam. June 1998. p.7 http://www.ivir.nl/publications/koelman/privreportdef.pdf [Accessed 05.10.2011]

[45] E.g. If content distributor offer streaming of content for fixed prices for certain amount of data streamed, he needs to know how much data were streamed to a particular user.

[46] See: Drossos, L., Papatheodorou, T., Sioutas, S., Tsolis, D. 2009, Digital Rights Management for E-Commerce Systems. Information Science Reference, Hershey, PA. p. 326-328

[47] However it is a debatable point.

Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p.245

See also: Drossos, L., Papatheodorou, T., Sioutas, S., Tsolis, D. 2009,Digital Rights Management for E-Commerce Systems. Information Science Reference, Hershey, PA. p.327

[48] Odlyzko, A. 2007, Digital rights management: Desirable, inevitable, and almost irrelevant. Digital Technology Center, University of Minnesota. http://www.dtc.umn.edu/~odlyzko/doc/drm2007.pdf [Accessed 12.09.2011]

[49] See: Odlyzko, A. 2003, Privacy, Economics, and Price Discrimination on the Internet, Digital Technology Center, University of Minnesota. p. 1-4 http://www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf [Accessed 10.09.2011]

[50] Study examined DRM-based services of music and movies delivery provided by iTunes, PressPlay, Rhapsody, MusicNet, MusicNow, Liquid Audio, MovieLink and CinemaNow.

[51] Index.dat files „act as a type of permanent record of the websites that users have browsed and of the files that they have download from the Internet".

Burstein, A. J.,Han, J., Mulligan, D. 2003, How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use", Proceedings of the 2003 ACM Workshop on Digital Rights Management. Washington, DC. p.7 http://www.law.berkeley.edu/files/DRM_personal_use.pdf [Accessed 18.10.2011]

[52] Burstein, A. J.,Han, J., Mulligan, D. 2003, How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use", Proceedings of the 2003 ACM Workshop on Digital Rights Management. Washington, DC. p.7 http://www.law.berkeley.edu/files/DRM_personal_use.pdf [Accessed 18.10.2011]

[53] Burstein, A. J.,Han, J., Mulligan, D. 2003, How DRM-Based Content Delivery Systems Disrupt Expectations of "Personal Use", Proceedings of the 2003 ACM Workshop on Digital Rights Management. Washington, DC. p.11 http://www.law.berkeley.edu/files/DRM_personal_use.pdf [Accessed 18.10.2011]

[54] Root kit is cloaking technology which hides system objects from the computer´s operating system, usually in order to cover viruses or malwares before detection by diagnostic and security software.

For more see: http://netsecurity.about.com/od/frequentlyaskedquestions/f/faq_rootkit.htm Retrieved: 06.10.2011

[55] Johns, A. 2009, Piracy, The Intellectual wars from Guttenberg to Gates, The University of Chicago Press, Chicago. p.507

[56] Russinovich, M. 31.10.2005, Sony, Rootkits and Digital Rights Management Gone Too Far, Sysinternals Blog. http://blogs.technet.com/b/mark-russinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx [Accessed 07.10.2011]

[57] Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content, Focal press, Burlington, MA. p.240

[58] MediaMax first automatically installed the program into the computer and then ask user to accept the licence agreement. However, MediaMax DRM system may become permanently activated even in the case when licence agreement was declined.

See: Halderman, A. 28.11.2005, MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA. Freedom to tinker Blog. https://freedom-to-tinker.com/blog/jhalderm/mediamax-permanently-installs-and-runs-unwanted-software-even-if-user-declines-eula [Accessed 09.10.2011]

[59] See: Halderman, A. 28.11.2005, MediaMax Permanently Installs and Runs Unwanted Software, Even If User Declines EULA. Freedom to tinker Blog. https://freedom-to-tinker.com/blog/jhalderm/mediamax-permanently-installs-and-runs-unwanted-software-even-if-user-declines-eula [Accessed 09.10.2011]

Van Tassel, J. 2006, Digital Rights Management, Protecting and Monetizing content", Focal press, Burlington, MA. p.240

[60] The Canadian Internet Policy and Public Interest Clinic examined DRM systems used in connection with various products and services like Apple iTunes Music Store, Apple iTunes Video Store, Microsoft Office Visio, Napster, Quick Tax, Pirates of the Caribbean DVD, OverDrive digital audio book, Norton SystemWorks 2006, Half-Life 2, The DaVinci Code e-book and others.

For more details see: The Canadian Internet Policy and Public Interest Clinic, 2007, Digital Rights Management and consumer privacy", An Assessment of DRM Applications Under Canadian Privacy Law. http://www.i-fap.ru/library/book217.pdf [Accessed 07.10.2011]

[61] The Canadian Internet Policy and Public Interest Clinic, 2007, Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. Executive summary. p. 2 http://www.cippic.ca/sites/default/files/CIPPIC_DRM_ExSum_EN.pdf [Accessed 07.10.2011]

[62] The Canadian Internet Policy and Public Interest Clinic, 2007, Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. Executive summary. p. 2-5 http://www.cippic.ca/sites/default/files/CIPPIC_DRM_ExSum_EN.pdf [Accessed 07.10.2011]

Available on: http://www.cippic.ca/sites/default/files/CIPPIC_DRM_ExSum_EN.pdf Retrieved: 07.10.2011

[63] The Canadian Internet Policy and Public Interest Clinic, 2007, Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. Executive summary. p. 3 http://www.cippic.ca/sites/default/files/CIPPIC_DRM_ExSum_EN.pdf [Accessed 07.10.2011]

[64] The Canadian Internet Policy and Public Interest Clinic, 2007, Digital Rights Management and consumer privacy, An Assessment of DRM Applications Under Canadian Privacy Law. Executive summary. p. 5 http://www.cippic.ca/sites/default/files/CIPPIC_DRM_ExSum_EN.pdf [Accessed 07.10.2011]

[65] SecuROM Product Activation is a DRM solution to authenticating legitimate use of content at online Product Activation Server. This DRM system was used in several computer games (most recently in Dragon Age 2 released in 2011) and required authentication of use in various intervals - from the need of a permanent connection to 10 days authentication interval.

See: SecuROM Product Activation Licence Information. https://support.securom.com/faq_pa.html#2.2 [Accessed 08.10.2011]

Pham, M. 16.03.2011, Connecting Dragon Age 2's "Release Control" To SecuROM" Reclaimyourgame.com. http://reclaimyourgame.com/content.php/774-RYG-News-Connecting-Dragon-Age-2-s-%93Release-Control %94-To-SecuROM [Accessed 08.10.2011]

Chalk, A. 07.05.2008, Mass Effect, Spore to use recurring validation, The Escapist Magazine. http://www.escapistmagazine.com/news/view/83689-Mass-Effect-Spore-To-Use-Recurring-Validation [Accessed 08.10.2011]

[66] See: Stone, B. 17.07.2009, Amazon Erases Orwell Books From Kindle Devices, The New York Times. http://www.nytimes.com/2009/07/18/technology/companies/18amazon.html [Accessed 09.10.2011].

Pogue, D. 17.07.2009, Some E-Books Are More Equal Than Others, The New York Times. http://pogue.blogs.nytimes.com/2009/07/17/some-e-books-are-more-equal-than-others/ [Accessed 09.10.2011]

[67] Kutchera, B. 18.02.2010, Official explanation of controversial Assassin's Creed 2 DRM, ArsTechnica

http://arstechnica.com/gaming/news/2010/02/ubisoft-details-drm.ars [Accessed 08.10.2011]