Human aspects of digital rights management: the perspective of content developers.

FAVALE, M., MCDONALD, N., FAILY, S. and GATZIDIS, C.

2016

scripted

Volume 13, Issue 3, December 2016

HUMAN ASPECTS IN DIGITAL RIGHTS MANAGEMENT: THE PERSPECTIVE OF CONTENT DEVELOPERS

Marcella Favale, Neil McDonald, Shamal Faily, Christos Gatzidis[*]

Abstract

Legal norms and social behaviours are some of the human aspects surrounding the effectiveness and future of DRM security. Further exploration of these aspects would help unravel the complexities of the interaction between rights protection security and law. Most importantly, understanding the perspectives behind the circumvention of content security may have a significant impact on DRM effectiveness and acceptance at the same time. While there has been valuable research on consumer acceptability, (The INDICARE project, Bohle 2008, Akester 2009) there is hardly any work on the human perspective of content creators. Taking video games as a case study, this paper employs qualitative socio-legal analysis and an interdisciplinary approach to explore this particular aspect of content protection.

DOI: 10.2966/scrip.130316.289

[*] Marcella Favale is Senior Research Fellow in Law at Bournemouth University, email: mfavale@bournemouth.ac.uk; Neil McDonald (Research Assistant) is undergraduate student in Law at Bournemouth University; Shamal Faily is Senior Lecturer in System Security Engineering, email: sfaily@bournemouth.ac.uk; Christos Gatzidis is Principal Academic in Creative Technologies at Bournemouth University, email: cgatzidis@bournemouth.ac.uk.

1. Introduction[1]

Copyright infringements and the evolution of digital rights management (DRM) have been among some of the most antagonistic points of the digital era. The debate surrounding the effectiveness and future of rights protection mechanisms has been closely aligned to the subjects of interoperability, user privacy, user acceptance, and maintenance of secure systems. While research from the content industry focused on the effectiveness of digital locks, most research from the users' side examined legal and social impact of content protection. The human aspects of DRM technologies, however, have been one of the lesser explored areas.[2] Moreover, when human aspects were considered by the relevant literature, they mostly investigated the user perspective. Legal compliance and acceptability of protecting technologies has rarely been analysed from the viewpoint of the other players at stake: the content creator and the content distributor.

It is questionable whether a flawless rights protection system can ever be accomplished when it is based on a technology incapable of distinguishing between an attacker and an authorised user; and it is even more questionable whether copyright issues should be entirely entrusted to technology. On the other hand, it has been argued successfully that that self-enforcement of copyright lowers transaction costs and it is therefore considered economically optimal.[3] However, it is submitted that this "computational copyright"[4] can only be considered to be truly successful if it takes into account all perspectives involved. In other words, DRM should not ignore the human component in security strategies.

This paper seeks to explore human aspects of DRM protection from the perspective of content developers. To this end it will review the available research and fill the gaps by providing original empirical data. We have chosen to focus on the game industry as a case study, because of its economic relevance compared to other creative industries. In 2014, for example, the UK computer video games market grew by 7.5% (to reach £2.5bn), while the market for videos decreased by 1.4% (to reach £2.2bn) and the market for music fell by 1.6% (to reach £1billion).[5]

While this has obvious positive consequences for growth and innovation, such an expansion should be matched by an extended attention to the fundamental values, the

---

[1] This paper is the main deliverable of a research project funded by the Fusion Investment Fund of Bournemouth University. The fund was awarded to Dr. Marcella Favale, Senior Research Fellow at Bournemouth University and member of the Centre for Intellectual Property Policy and Management (CIPPM) mfavale@bournemouth.ac.uk.

[2] R Anderson, *Security Engineering* 2nd ed. (Hoboken: Wiley, 2008) at 679-725, at 679.

[3] W Gordon, "Fair Use as Market Failure: a Structural and Economic Analysis of the Betamax case and its Predecessors" (1982) 82 *Col L. R*. 1600-1657, at 1654.

[4] O Conetta and B Schafer, "Self-enforcing or self-executing? What Computational Copyright can learn from LKIF Transaction Configurations for Eurobonds", CREATe Working Paper 2014/12 (October 2014), available at https://zenodo.org/record/12432/files/CREATe-Working-Paper-2014-12.pdf (accessed 16 Oct 15).

[5] See generally L Butler, "ERA UK Market Statistics" (2014) available at http://www.gera-europe.org/info-stats/overview.aspx (accessed 16/04/2015).

norms, and the social interactions impacted by these technologies. The perspectives in this work are limited to games, but the questions raised could be applied to any type of rights protected digital content.

This paper aims to understand the extent to which the human aspects surrounding DRM technology and circumvention[6] are perceived, identified and understood by videogame developers. To this end, the paper consists of two parts. In the first part a systematic analysis of the relevant literature will help identify the key human aspects revolving around content protection. The discussion surrounding fairness and DRM will be explored from the point of view of the content developers, content distributors, and content users. This part benefits from the contribution of academics from various disciplines (law, cyber security, game development) in order to give a multi-dimensional picture of the issues surrounding DRM. A number of key questions shall be identified by the analysis of these opposing perspectives, which will be proposed, in the second part of the paper, to a sample of developers from the videogame industry.

2. The evolution of digital locks[7]

Before DRM is discussed is more in detail, it would be useful to briefly examine its evolution, particularly in terms of some approaches that have been followed throughout the history of computer/video games development. Very early attempts at games development did not concern themselves overtly with DRM, as the market was not mainstream or large enough to warrant this. With the advent of home computers, there emerged a need for developers to protect gaming software from piracy in order to safeguard revenues. For earlier cartridge-based consoles - at least until the advent of the generation of consoles with a CD drive in the mid-1990s, for example Sony's original PlayStation - there was no significant need for DRM. For home computer games software protection originally focused on ensuring that any game could only be used by the user who purchased it, via targeted checks. This usually manifested in the form of a manual/physical approach. The diversity and ingenuity of methods employed remain fascinating to games audiences and relevant historians alike to this day, sometimes for the sheer imagination behind them, and sometimes because of the incredible ease with which these could be bypassed today.

This manual/physical approach, in pre-Internet days, was normally reliant on inputting data from physical documentation provided alongside the game when purchased (i.e. included in its box). This could either be in the user manual itself, or something more elaborate included within the box of the game. A genre of games

---

[6] Data has been retrieved from Scopus, IEEE'sXplore, book chapters, journal articles and the conference proceedings of the ACM Digital Library. The literature selection utilised Google Scholar and Scopus to identify the most frequently cited material. The analysis is supported by NVivo qualitative analysis software using an open coding technique with a hierarchal structure with four master codes of Developer view, Distributor view, User view and Legal view. The sub-code structure was broken down into: a) Constraints of DRM, b) interoperability of DRM, c) opinions on DRM, and, finally, d) reasons for DRM. The socio–legal approach identifies and explores the elements of law and the human behavioural aspects in rights protection security by focussing on the perspectives and opinions of the stakeholder groups.

[7] This section is authored by Dr Christos Gatzidis, Principal Academic in Creative Technology at Bournemouth University, cgatzidis@bournemouth.ac.uk.

which explored more imaginative approaches linking DRM with materials and documents (plus on occasion the game itself) was adventure games; a very popular, story-driven and puzzle-based genre which was part of the gaming mainstream from the mid-1980s and during a large part of the 1990s. It is also notable that this form of DRM protection would not always come at the beginning of the game, but only once the player had made some progress (and could not progress further without passing the aforementioned targeted check with the correct user input, or worse yet, would be killed off as punishment for incorrect entries).

Two developers of the era, who both had a number of impactful and successful games in this genre and employed DRM (in different ways yet based on the above principle), were Sierra On-Line and LucasFilm Games (later LucasArts), both now defunct. Sierra On-Line used DRM in many of their titles, amongst which was King's Quest III (1986), where the manual contained the different steps for the user to follow, and also components needed for different magic spells, all at the core of the gameplay. Leisure Suit Larry 5 (1991) featured another typical approach of the era towards DRM; codes provided in the documentation. These codes were to be used when the player needed to fly to different locations in order for the game to progress. However, the codes were printed in black font against a red back background in order to make it difficult to photocopy and pass on to another player who had not purchased the game (and was not in possession of the documentation). LucasArts took this method a step further, with more complex approaches such as the one exhibited on the Secret of the Monkey Island game (1990). The box of the game included a physical, rotatable contraption that resembled a wheel (with two different parts), which the player would use for the check (faces, years and locations were used on this particular game's DRM). This approach was used again in the game's 1991 sequel, although this time the theme was not pirate faces as before (revolving around the theme of the series), but recipe parts and dosages. It is difficult to estimate how effective these approaches were and how much, if indeed at all, they deterred piracy. However, the intricacy/complexity of some of these approaches reveals how seriously protecting DRM was taken, already, during the 1980s and 1990s in home computer gaming software.

Today there is no need for the above DRM approaches for games. These can alienate customers, not only because they are cumbersome and obstructive, but also expensive and obsolete (as games have moved from the physical retail approach to digital downloads and boxes full of material are of the past) and would, in any case, be very easy to bypass. A very commonplace, modern approach to DRM is ensuring that the user and game remain online at all times for a continuous check of any possible breach. This approach has evolved, and while it is more streamlined in 2016 from a technical point of view, there remain problems with it (albeit of a different nature to the ones observed with the earlier games discussed). An interesting case study for this is Blizzard's Diablo 3(2012) for the PC platform (and later on for consoles as well). Whilst this DRM approach is effective, this specific game garnered a significant amount of attention, as early issues with servers on the developer side effectively made it impossible for many users to play the game. This attracted a significant amount of controversy because of the immense popularity of the game and, inevitably, a lot of negative publicity, not just for the game itself (which still performed well commercially and critically) but also, and predominantly, for this specific approach to enforcing DRM. Regardless of the problems such approaches to DRM can cause, it is envisaged that some games developers will continue to use them

as they can offer advantages above DRM, such as collecting player data that can then be analysed (for the developers' and even players' benefit), as we will see further below in this paper.

3. The "Unfairness" of DRM

Piracy is the use of a copyrighted material without paying for it.[8] Digital piracy occurs regardless of what type of media is being developed or for what distribution platform it is intended for. The factors influencing the user's desire to circumvent DRM in acts of piracy can be construed as a social problem driven by human aspects such as intent, motive, moral judgement, and social consensus.

Possible reasons behind the circumvention of DRM go beyond any technological weaknesses of the security into the human aspects of security. The growth of online gaming, and the uptake of faster internet connections along with the rise of initiatives such as the 'Occupy Movement' against corporatism and economic inequality[9] have provided opponents to DRM with more ways to justify the circumventing actions. Arguably, video games manufacturers view DRM as a necessary instrument in the fight against copyright violation. However, the critics of DRM allege that it stifles innovation and fair competition by quashing lawful uses of digital content. As such, it is creating economic and social inequality regardless of the context of the intended use.[10]

Because of this perceived economic and social inequality between rights holders and users of games, it becomes imperative for the legal system to ensure that there is fairness for all in the event of a legal dispute. Fairness is achieved when people restrain their liberty in ways necessary to yield advantages for all.[11] Fairness in the English legal system is underpinned by the principle of Equity. This is described as "the means by which a system of law balances the need for sufficient judicial discretion to achieve fairness in individual factual circumstances".[12] Because of the perceived bias towards the rights holders, it is essential that "justice should be seen to involve procedural fairness and a fair decisions being reached by an objective decision-maker, whilst protecting the rights of individuals and promoting public confidence in the legal process".[13]

---

[8] G Nagesh, "24% of Web Traffic Involves Piracy" Hillicon Valley Blog, the Hill (2011) available at http://thehill.com/policy/technology/141509-study-24-percent-of-web-traffic-involves-piracy (accessed 10 Apr 15).

[9] M Townsend, "Parliament Square fence crushes protest rights, says Occupy Democracy" (2015) available at: http://www.theguardian.com/uk-news/2015/jan/03/boris-johnson-occupy-democracy-london-protest-fence (accessed 15 Apr 2015).

[10] B Litlow, "DRM's Rights Protection Capability: a review" (2012) Volume 1 *The First International Conference on Computational Science and Information Management* 12-17, at 12.

[11] H Hart, "Are there any natural rights?" (1955) 64(2) *The Philosophical Review* 175 -191, at 17.

[12] A Hudson, (2012) *Equity and Trusts* 7th ed. (Oxford: Routledge, 2012) at 5-6, at 5.

[13] Y-L Chang, "Who should own access rights? A game-theoretical approach to striking the optimal balance in the debate over Digital Rights Management" (2007) 15(4) *Artificial Intelligence and Law* 323-356, at 323.

Perhaps the most serious drawback to the debate surrounding the effectiveness and future of DRM is that fairness for all, as defined by Hart, may never be achievable across groups serving such different interests. Consequently, the usage restrictions implemented by content distributors extends beyond intellectual property monopoly and it often raises issues of consumer acceptance.[14] Because of these restrictions, DRM can seem inequitable and unfair when applying Hart's principle of fairness. This apparent lack of fairness and bias in the direction of rights-holding organisations results in DRM getting a lot of attention by copyright academic, content industry and media.[15]

4. Why designing DRM is hard[16]

DRM is a suite of technologies that protect the rights of various stakeholders associated with digital content. Typically, these stakeholders are content producers, consumers, and publishers. Although there is no standard model for DRM architecture, DRM solutions typically include components for:

* managing content to be protected;

* creating and managing licenses that specify the rules for consumption of content;

* tracking usage of content, to ensure this is in line with license rules; and

* submitting packaged content for management by the DRM architecture.

These components are also supported by a number of security services. The expectations on these services are myriad and included guaranteeing the integrity of licenses, protecting content against tampering, authenticating consumers before protected content can be accessed, and safeguarding sensitive data at rest and in transit.[17] These services are implemented to defend against attacks to DRM protocols, attacks against DRM client software, and the software and hardware used to store and render the protected content.[18]

Designing any software system to meet the security expectations of different stakeholders is hard because product innovation is the main goal for building software rather than security. As a result, the time-consuming user research activities necessary for modelling these expectations is de-emphasised, and difficult to sustain throughout long projects.[19] DRM is unusual in that securing content is one of the key

---

[14] C Darroch, "Problems and Progress in the Protection of Videogames: A Legal and Sociological Perspective" (2012) 1(1) *The Manchester Review of Law, Crime and Ethics* 136-172, at 136.

[15] E Diehl, *Securing Digital Video: Techniques for DRM and Content Protection* (New York: Springer, 2012) 4-5, at 4.

[16] This section is authored by Dr Shamal Faily, Senior Lecturer in Systems Security Engineering within the Department of Computing and Informatics, Bournemouth University, sfaily@bournemouth.ac.uk.

[17] S Michiels et al. "Towards a software architecture for DRM" (2005) *Proceedings of the 5th ACM Workshop on Digital Rights Management* (DRM '05) 65–74.

[18] G Taban, A Cárdenas, and V D Gligor, "Towards a secure and interoperable drm architecture" Proceedings of the ACM Workshop on Digital Rights Management (DRM '06) at 69–78 (New York, NY, USA: ACM, 2006).

[19] S Faily et al, "Usability and Security by Design: A Case Study in Research and Development" in *Proceedings of the NDSS Workshop on Usable Security,* Internet Society, 8 Feb 2015 San Diego CA.

goals of any DRM system, but these challenges still remain because designers must be mindful of the impact of DRM on consumer rights.[20] Unfortunately, designing for DRM also introduces several particular challenges.

First, as difficult as designing security is, designing DRM is even harder because it entails integrating security mechanisms such cryptographic libraries, access control systems, and secure storage solutions into a coherent whole. Moreover, as Michiels indicates,[21] there are many candidate architectures for satisfying the requirements of different stakeholders. Each configuration might be associated with different threat and trust models, and have a different 'attack surface'. Moreover, despite the pervasiveness of DRM technology in practice, there are no case studies in the literature reporting on the design, evolution, and lessons learned implementing DRM software architectures 'in the wild'. Without such studies, there is little support for designers on encapsulating the expectations of different DRM stakeholders in DRM architectures.

Second, the trust and threat models associated with DRM are byzantine. From a traditional security perspective, one might assume that both the content owner and content user are trustworthy, and any malicious agents may be trying to spoof communication traffic, or intercept and tamper with it. However, when we think about DRM, these models start to break down. For example, content users may accept distributors knowing about purchase details, but may not be happy about distributing misusing this data by sharing it with 3rd parties. Theoretical security models assume that legitimate use and misuse are well-defined, but this is not the case with DRM.[22] Moreover, as Diehl notes,[23] not only does the content owner not trust the content user, there is no easy way for a content owner to distinguish between honest and dishonest users. Moreover, even if the content user could be trusted, this trust might not be warranted if another user controls the content user's machine through malware.

Finally, the business models upon which DRM are based are dynamic, and it is uncertain how suitable DRM designs in the literature are given the current socio-legal and socio-economic climate where DRM is now pervasive. Although interoperability has long been cited as a 'grand challenge' for ecosystems where heterogeneous DRM solutions are pervasive,[24] there has been little progress implementing interoperability in practice. This is due in part to new classes of DRM attacks resulting from the need for device cross-compliancy and data leakage associated with the migrating content

---

[20] A Kubesch and S Wicker, "Digital Rights Management: The Cost to Consumers [Point of View]" (2015) 103(5) *Proceedings of the IEEE* 726-733.

[21] S Michiels et al. "Towards a software architecture for DRM" (2005) *Proceedings of the 5th ACM Workshop on Digital Rights Management* (DRM '05) 65–74.

[22] J Feigenbaum et al, "Privacy Engineering for Digital Rights Management Systems" in T Sander ed. *Security and Privacy in Digital Rights Management* volume 2320 of *Lecture Notes in Computer Science*, 76-105 (Berlin Heidelberg: Springer, 2002).

[23] E Diehl, *Securing Digital Video: Techniques for DRM and Content Protection* (New York: Springer, 2012) 4-5.

[24] R Koenen et al "The Long March to Interoperable Digital Rights Management" (2004) 92(6) *Proceedings of the IEEE* 883-897.

for interoperability.[25] However, it has also been suggested that interoperability requires DRM designers to publish more details of their design and implementation than they might feel comfortable doing.[26]

5. The Players in the DRM Game

DRM systems are in essence technical locks designed to self-enforce copyright protection in the digital world. Traditionally, the golden triangle of the copyright stakeholders is formed by: a) the creator; b) the user; and c) the distributor.[27] In what follows we will examine their different perspectives.

5.1 Content Developers

DRM impacts on a complex range of interests.[28] Content developers are obviously one of the most relevant stakeholders, although they might not necessarily rely on legislation to enforce their policies.[29] Self-enforcement of digital rights might be more effectively entrusted to cyber-protection technologies, especially given the practical difficulty to pursue millions of infringers.

It has been argued that some users will inevitably try to use digital content without paying the appropriate fee, unless they are prevented from doing so by societal rules and social consensus.[30] However, there is very little work on precisely which societal rules might be used to prevent the social perception that circumvention of DRM security in acts of piracy is a fair or a victimless act. Part of the ant-circumvention strategy of content developers relies on these rules.[31]

For some content developers, moreover, the perception of DRM is arguably influenced by their business model, despite there is little literature dedicated to the relationship between business model choice and DRM deployment. For the case of videogame developers, for example, it is different whether they expect their product to generate a steady income stream or whether the product will be offered at a one-off price to a distributor, who will then take ownership of the rights and financial revenues. Many developers are start-ups, often backed by external investors who have

---

[25] G Taban, A Cárdenas, and V D Gligor, "Towards a secure and interoperable drm architecture" Proceedings of the ACM Workshop on Digital Rights Management (DRM '06) at 69–78 (New York, NY, USA: ACM, 2006).

[26] E Diehl, *Securing Digital Video: Techniques for DRM and Content Protection* (New York: Springer, 2012) 4-5.

[27] W Grosheide, "Copyright Law from a User's Perspective: Access Rights for Users" (2001) 23(7) *E.I.P.R.* 321-325.

[28] It has been argued that "DRM requires a complex system of technical, organisational and social elements" See V Mayer-Schonberger, Beyond Copyright: Managing Information Rights with DRM. (2006) 84(1) *Denver University Law Review* 181, at 181.

[29] Digital content developers only accounted in total for "6.7% of lobby meeting requests with the evaluation rapporteur of the EU Parliament Copyright Directive 2001/29/EC". See J Reda "EU copyright evaluation report – explained" (2015) available at https://juliareda.eu/2015/01/report-eu-copyright-rules-maladapted-to-the-web/ (accessed 09 Apr 15).

[30] V Mayer-Schonberger, Beyond Copyright: Managing Information Rights with DRM. (2006) 84(1) *Denver University Law Review* 181.

[31] M Yar, "The rhetoric and myths of anti-piracy campaigns: criminalization, moral pedagogy and capitalist property relations in the classroom" 2008 10(4) *New Media & Society* 605-623.

a financial interest in DRM deployment in order to maximise the return of their investment. In addition, changes in business models need to be considered in the wider DRM debate centred on the effectiveness and future of game security. Digital content production takes place in a very fast-moving environment,[32] and while a business model can befit or indeed need DRM implementation, changes or modifications of the same business model can have entirely different requirements in terms of security policy, especially if the user acceptance enters the equation.

It is questionable whether game developers should be leaving DRM for the publisher to deploy. After all, they are the original owner of the copyright arising from the creation of the product. They might be entitled to decide what usage restrictions are implemented on their creation. However, for a number of reasons that will be clearer in the last section of this paper, in practice (at least in the sector of game development) they prefer to leave content protection to the other side of the golden triangle: the distributor.

5.2 Content Distributors

The examined literature shows that the distributors have the strongest interest in DRM deployment. Developers are surrendering unprecedented control over their products to distributors.[33] For developers to continuously improve the gameplay experience, they need a recurrent income stream or a large preliminary investment from a content distributor with a large market reach.

Consumers now have a greater than ever choice of content through multiple merchants such as Google Play, iTunes, Xbox Live etc. As a consequence, one of the emerging business models for games is the 'freemium model' where the core game content is offered for free but value is added by optional in-game purchases such as in-game characters, extra content, cheats or game customisations.

Because of the increasing implementation of this model, consumers of games are no longer considered a mere submissive receiver of products through an initial one-time purchase. The freemium model appears to eliminate the need for DRM in the traditional sense, as wider distribution of the core free game content targets a wider market share for in-game purchasing resulting in the higher probability of in-game purchases. However, even in freemium models DRM is implemented on additional purchases. While under the traditional one-off purchase business model the distributor appears to be shouldering the entire burden of rights protection and security, in the freemium model content protection is implemented by the developer, according to the requirement of digital distributors.

While the costs of DRM implementation have been object of analysis,[34] little attention has been paid to the legal implication of the fact that distributors are shouldering the

---

[32] During the last two decades, for example, the digital content industry has undergone a period of significant change in both social and business strategy, *ibid*.

[33] C Darroch, "Problems and Progress in the Protection of Videogames: A Legal and Sociological Perspective" (2012) 1(1) *The Manchester Review of Law, Crime and Ethics* 136-172, at 136.

[34] P Petrick, Why DRM Should Be Cause for Concern: An Economic and Legal Analysis of the Effect of Digital Technology on the Music Industry. The Berkman Center for Internet and Society, Research publication n. 2004-09 (November 2004), available at http://cyber.law.harvard.edu/home/uploads/408/DRMPetrick.pdf, (accessed 12 Oct 15), at 27)

entire rights protections and security burden. If DRM is a complex of security mechanisms designed to protect the game assets, the distributor ends up taking full responsibility and, as a consequence, liability, for the security of the game. If this is the case, distributors are seemingly accepting responsibility for any possible security vulnerability associated with the development code, the game engine, or indeed any aspect of the game. This might have important legal consequences, for example in terms of vicarious liability.[35]

5.3 Content Users

DRM consists of a variety of security mechanisms designed to prevent users from carrying out actions that may breach rights protected by copyright and IP law.[36] However, this system of restrictions often fails to account for the permitted copyright exceptions granted to users in the EU or the fair use allowances granted in users in the USA.[37] Both of these allowances permit backup copies for personal use, or for the purposes of educational use. Users of rights-protected content account for only 20% of the total lobby meeting requests with the evaluating rapporteur of the EU European Parliament Copyright Directive 2001/29/EC.[38] Regardless of the size of the stakeholder's interest in DRM there is an underlying sense of an imbalance of power with the bias falling in the direction of rightholders. The rights holders appear to be free to undermine a number of lawful copyright limits granted by law to the users.[39]

In addition, literature suggests that overly restrictive DRM systems are likely be counter-productive as they provide little in the way of an incentive for users to purchase legitimate, paid-for content.[40] It can be argued that the financial motives for user piracy, or circumvention of DRM, would be less prominent if the pricing policies set by distributors were more aligned with current economic times.[41] Unfair DRM in sum is not only against the law, but also against a sensible marketing policy. At present, distributors have unprecedented levels of power overprice determination and

---

[35] Vicarious Liability in essence is the responsibility of any third party that has the "right, ability or duty" to control infringing acts. In this case the distributor will be the third party between the rightholder and the user.

[36] G Qun, Digital Contents Interoperability between Diverse DRM Systems (2010) *Shandong, Intelligent Computing and Intelligent Systems* (ICIS)(2) at 170-173.

[37] M Favale, "Fine-Tuning European Copyright Law to Strike A Balance Between the Rights of Owners and Users", (2008) 33(5) *European Law Review* 687-708, at 306)

[38] J Reda "EU copyright evaluation report – explained" (2015) available at https://juliareda.eu/2015/01/report-eu-copyright-rules-maladapted-to-the-web/ (accessed 09 Apr 15).

[39] For example, the game World of Warcraft (prior to the freemium model version) could not be successfully bought used, because of a DRM-based one-time installation key policy. See S Dusollier, "Tipping the Scale in Favour of the Right Holders: The European Anti- Circumvention Provisions" in *Digital Rights Management - Technological, Economic, Legal and Political Aspects in the European Union* (Berlin: Springer-Verlag, 2003) 462-478, at 462.

[40] C Darroch, "Problems and Progress in the Protection of Videogames: A Legal and Sociological Perspective" (2012) 1(1) *The Manchester Review of Law, Crime and Ethics* 136-172.

[41] In fact, arbitrary price determination by distributors of online products has been object of attention by Courts. See http://www.cnet.com/news/new-york-focuses-antitrust-probe-of-record-labels/ (accessed 5-Oct 15).

differentiation. This, in turn, has had a negative impact on the user's attitude towards - and acceptance of - DRM technologies.[42]

Another problem faced by users when interacting with the other stakeholders are language difficulties. For example, End User Licence Agreements (EULA), which include the Terms and Conditions of Use for rights-protected content, are often written using legalistic language and there is an apparent disengagement by content users of anything that appears written in that manner.[43] In many cases the contractual relationship and legal terms that the user enters into with the rights holder are not given a second glance.

Another example is the use of abbreviations in language used by different stakeholders, such as developers or distributors. In the online contracts the abbreviation TPM stands for Technological Protective Measure, but in the field of software development TPM is the abbreviation for Trusted Platform Module.[44] These are only examples of the problems that can be caused by language difficulties across different stakeholder with mostly entirely different backgrounds and interests.

6. The Need for Balance

If the acceptance levels of DRM are to be improved, it is vital that a greater degree of balance is struck between the stakeholders.[45] As can be seen from the discussion in this paper, rights protection within cyber-security is a complex issue with multiple viewpoints and social arguments for and against its implementation, where a focus on fairness is seldom present. In the Courts of Law, however certain attention for balance and fairness is sometimes visible. For example, the issue of DRM has been examined at the highest European level with regard to circumvention on games consoles. This circumvention is sometimes achieved through the commercialization of modified chips ('mod chips') which allow the user to play unauthorised games.

The European Court[46] held that the protection of 'effective' Technological Protective Measures (TPMs) can be extended to external hardware devices such as mod chips because there is nothing in the Information Society Directive 2001/29/EC of the European Parliament that forbids it, especially when considering the broad definition of TPMs provided by the directive. The Court however specified that a number of conditions need to be satisfied in order to allow the protection of TPMs. In particular, a) the aim pursued by the manufacturer implementing TPMs must be legitimate (e.g. it must seek copyright protection and not competition hindrance); b) TPMs must be suitable for the task (e.g. 'effective'); and c) certain proportionality criteria must be met, which includes a number of considerations: the volume of infringing behaviours

---

[42] C Darroch, "Problems and Progress in the Protection of Videogames: A Legal and Sociological Perspective" (2012) 1(1) *The Manchester Review of Law, Crime and Ethics* 136-172.

[43] M A Lemley, "Terms of Use" (2006) 91 Minn. L. Rev. 459-461 n.5.

[44]This "is a crypto-graphic coprocessor chip that has been included on most enterprise-class PC and laptop motherboards produced in the past decade", see J Challener, "Trusted Platform Module Evolution" (2013) 32(2) *John Hopkins APL Technical Digest* 1.

[45] S Dusollier, (2003) Tipping the Scale in Favour of the Right Holders: The European Anti-Circumvention Provisions, in *Digital Rights Management - Technological, Economic, Legal and Political Aspects in the European Union* (Berlin: Springer-Verlag, 2003) 462-478.

[46] Case C-355/12 *Nintendo of Europe GmbH. v. PC Box Srl, 9Net Sr,* ECLI:EU:C:2014:25.

compared to legitimate behaviours, and whether a different protection technology 'could cause less interference' with legitimate uses.

The above ruling clearly shows the highest European Court's struggle regarding 'fairness'. The "fair balance of interests", provided in the recitals (albeit not in the text) of the EU Copyright Directive,[47] seems to be seriously considered by the judiciary invested with copyright matters.

However, it is unlikely that DRM systems will ever be able to accurately predict or read human intent and, as such, there is a very fine line between legitimate fair use actions (i.e. hardware modifications to allow bespoke home-brewed content to run or be used for backup purposes) and those actions that have a secondary purpose that can carry out unlawful circumvention of DRM and breach TPMs. Ultimately, the DRM system cannot know enough about the circumstances outside of the computer.[48]

Moreover, human intent is only one part of the problem. Copyright infringement can be determined objectively, irrespective of the human intent, when the unlawful acts (unauthorised reproduction, communication, and distribution) are clarified by law. As this is not the case currently it can be suggested that legislative reform in this area is urgently needed.

7. The need for Clarity and Legal Certainty

From a legal perspective, DRM can create a variety of different disputes in the legal areas of copyright, privacy, competition, contract, and other branches of law.

The complexity of the legislation regulating anti-circumvention measures, which are the provisions impacting on DRM, does not help legal certainty. For example, in Europe Technological Protection Measures have to comply with copyright exceptions, according to the Copyright Directive. But each EU country has implemented the directive with a different selection of exceptions with which TPMs have to comply, and it applied different civil or criminal charges against DRM circumvention.[49]

In the US, the lack of a clear definition between fair uses from acts that would constitute copyright infringements does not help the status of DRM security. Although some uses are clearly fair and others clearly not fair, there is essentially a large grey area of uses that may or may not be conceived as fair and could only ever be settled with the assistance of a court ruling. Even a well-accomplished copyright lawyer cannot say with absolute certainty where the line between fair and unfair use is really found.[50]

Moreover, although DRM legal protection originates and is defined within copyright protection, it is in practice implemented to achieve anti-competitive practices. For

---

[47] Council Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society *Official Journal L 167, 22/06/2001 P. 0010 – 0019,* Recital 31.

[48] E Felten, "A sceptical view of DRM and fair use" (2003) 46 (4) *Communications of the ACM* 56-59.

[49] M Favale, "Fine-Tuning European Copyright Law to Strike A Balance Between the Rights of Owners and Users", (2008) 33(5) *European Law Review* 687-708, at 688.

[50] E Felten, "A sceptical view of DRM and fair use" (2003) 46 (4) *Communications of the ACM* 56-59, at 56.

example, interoperability requirements provided by the software directive[51] prompt essentially competition issues;[52] whereas on the side of the user, there are substantive privacy issues to be considered, as DRM can and is often used to track user behaviour.[53]

Advances towards a balanced DRM will be determined not only by technology modifications, but also by current and emerging economic and legal developments.[54] However, when markets go through rapid change like the gaming sector has, it takes time for legislation to catch up.[55] A fragmentary and out-dated legal framework increases the risk of litigation, which in turn increases variable costs to an unbearable extent for smaller players.

Additionally, changes in the game development market, such as the development of new hardware platforms, different distribution methods, and new payment technologies, all carry risks and legal challenges that require access to legal professionals for those involved in disputes. These market factors aid the need for legal professionals specialising in the DRM sector, who are often at a loss trying to apply out-dated or excessively complex legislation to new scenarios.

Additionally, the business models of the stakeholders involved in disputes around rights protection will also have an influence on the access to justice and legal outcome. The complexity of disputes in copyright law along with the nebulousness of the fair use exceptions, combined with the struggle of negotiating licensing agreements, mean that non-experts such as fledgling game developers are often at an informational disadvantage when they face a dispute involving DRM. In any legal dispute access to high quality legal advice is vital, but also dependent on having the financial means to defend one's position and seek the necessary guidance prior to litigation. Financial health and the ability to seek high quality legal advice are more commonly found in larger more established organisations than smaller nascent organisations.[56]

In sum, the ever-changing nature of content security and the complex legal issues DRM can create impact of the performance and commercial viability of small content producers. These problems can only be counteracted by a simplification of DRM regulations and the easy accessibility of alternative dispute resolution systems.

---

[51] Council Directive 91/250/EEC, *Official Journal L 122, 17/05/1991 P. 0042 - 0046*, Article 6.2 .

[52] U Gasser and J Palfrey, "When and How ICT Interoperability Drives Innovation", *Berkman Publication Series*, November 2007, available at https://cyber.law.harvard.edu/interop/pdfs/interop-breaking-barriers.pdf (accessed 12 Oct 15).

[53] D Burk and J Cohen, "Fair use infrastructure for rights management systems" (2001) 41 *Harvard Journal of Law and Technology* 48–82; J Feigenbaum et al, "Privacy Engineering for Digital Rights Management Systems" in T Sander ed. *Security and Privacy in Digital Rights Management* volume 2320 of *Lecture Notes in Computer Science*, 76-105 (Berlin Heidelberg: Springer, 2002); J Cohen, 'DRM and privacy', (2003) 18 *Berkeley Technology Law Journal* 575–616).

[54] G Heileman and P Jamkhedkar, "DRM interoperability analysis from the perspective of a layered framework" (2005) *Proceedings of the 5th ACM workshop on Digital rights management* (DRM '05 -1) at 17-26.

[55] P Samuelson, "DRM {and, or, vs.} the law" (2003) 46(4) Communications of the ACM 41-45, at 41.

[56] W Davies and K Withers, "Public Innovation, Intellectual Property in a Digital Age" (2006) *Institute for Policy Research* 48, at 48.

8. The Perspective of the Developers

The analysis carried out in the first part of this paper has produced a number of questions, which we have summarised in the following:

- What are the motives and incentives of DRM circumvention?
- Are cultural, legal, and/or commercial strategies effective against circumvention? Is DRM adding value? Or is value best reached through other measures?
- On DRM and Contract (EULA), are DRM developers aware of the legal issues?
- Are Developers aware of DRM limits (e.g. copyright limits and exceptions)?
- Overall is DRM a human (social, legal) problem or a technical one? What is the solution?

These questions formed the core of a semi-structured questionnaire that was submitted to a selection of UK based game developers. The responses to the questionnaire have been object of qualitative analysis.

Our case studies implemented different business models: the Premium model online (one-off fee per game), the Freemium model online (game available for free and extras available for a fee), and the sale of game consoles. Interestingly, none of them reported to have given any consideration to content protection upfront, when choosing their business model. However, it was acknowledged that the need for DRM implementation varies among business models because the very need for protection and the concrete possibilities of protection are different. For example while the Freemium model has no need for protection at release stage, it needs DRM when additional features of the game are purchased. Conversely, game consoles and CD-based Premium models need to implement DRM upfront if they want to avoid infringement. Moreover, server-based products offer more possibilities for controlling usage restrictions compared to client-based games.

In order to identify the source of content restrictions within each model, we have asked whether the platforms have imposed DRM on developers, contractually or otherwise (e.g. more or less binding business practices). The developers' responses suggest that all market leaders impose DRM implementation for the products they commercialise, whereas some minor player do not require content restrictions.

Developers' opinion on possible incentives for circumventing DRM mentioned the technical challenge for those that crack the game, and make it available on peer-to-peer file sharing. Unskilled game downloaders from P2P platforms, conversely, according to the project participants were possibly incentivised by: a) getting the game without paying the price, b) trying the game before buying it (trial versions are no longer available), and c) freedom of using a lawfully purchased product.

On the other side of the spectrum, developers' incentives for the implementation of DRM were rather low. Developers know that DRM has a low consumer acceptance, and they fear that the market penetration of their products can be seriously impaired by content protection. However, they do implement content protection because this is required by the platform, especially those able to guarantee wider market distribution. Overall DRM is considered valuable, as it adds value to the product, but at the same

time it is described as a necessary evil. In short, the general feeling of the interviewees was that they would rather not to have to worry about DRM. They would happily leave the whole task to the distributing platforms.

Interestingly, the main incentive arising from content protection, and directly impacting on the interests of developers, are the data monitoring possibilities offered by DRM. In short, product protection technologies allow studying users' behaviour. This information is valuable to determine future product modifications and in general future market policies.

Costs of DRM implementation were not perceived as relevant by game developers as mostly shifted on the distributor (the platform); and costs of DRM circumvention (piracy) vary among business models. While game console developers showed a fair confidence in the effectiveness of their DRM, the others found that the costs of breaches in content protection were offset by the advantages of broader circulation of the product in the market.

All the interviewees seem to be aware of a certain amount of DRM circumvention on their products, however they declared that they rarely action against it. In more detail, reported actions against DRM circumvention include: a) do nothing ("move on"), b) changing the code, and c) complain with the platform. The latter action seems to be effective due to corporate IP policies of large platforms, which handle the "notice and take down" process rather swiftly (and, it appears, without judicial scrutiny).

Taking legal action seems to be considered the last resort from the interviewed developers, mainly because of cost/benefit considerations. In short, broad circulation of the product on the market is perceived as creating more advantages than losses. However, legal action is contemplated in the case of professional infringement, as in cases in which somebody cracks the digital lock in order to commercialize the game in competition with the right holder.

The End User Licence Agreements (EULA) which is the contract between the user of the game and the rightholder (including the distributor) is either entirely handled by the platform or "borrowed" from competitors or other sources. Developers seem to have given no consideration to the legal aspects and implications of this document in terms of legislation they need to comply with (copyright, data protection, consumer protection).

Some of the developers have encountered data protection issues in their day-to-day activity, in particular when collecting behavioural data on users. They refer to have addressed this by screening identity information (e.g. the name of the user or the credit card details) and by providing privacy policies for each product, explaining what type of data is collected, and which are accessible online. No tailored legal advice was sought or provided, unless presented with a specific problem, however general guidance seems to be available from industry trade bodies.

Overall, the main problem with DRM technologies, according to game developers, is human/social, in the sense that DRM circumvention is not seriously perceived as "wrong". They find that the attempts to develop a social conscience about it, such as equalling infringement to stealing, are ineffective and deceptive for the public. The issue of fairness is also perceived as tipping the balance against users, who cannot try the product before buying it, and cannot do what they want with things that they own. Legal sanctions against circumventions are also considered to be "unfair," as they are way too severe. However, they all concur that although DRM circumvention is

basically a "human" issue, any viable solution can only be "technical". Social and legal solutions are in fact perceived as highly ineffective.

Finally, we asked our project participants what their dream scenario would be on DRM. While the short impulsive answer was "a world without it", more serious reflections included the acknowledgement that a digital world without content protection would be neither reasonable nor viable. A more realistic dream scenario involves a flexible DRM that allows users more freedom, while protecting the rights of the owner at the same time. Moreover, they would like a seamless DRM that is easy to implement, as they would prefer to focus on the creative process. They believe that creating a very good product is more important than defending mediocre products from infringement. If the product is very good, some argued, consumer acceptance of DRM may increase, as the pleasure to play the game will overcome the annoyance of having usage restrictions.

9. Conclusions

There are multiple stakeholder views associated with DRM security. This paper searched the literature to provide some of them, and it gathered original data to complete the picture. Current research on DRM shows the human (social and legal) implication of DRM only in relation to the final user of the digital product. The perspectives of the games industry, content developers, and distributors have instead been examined from a technical point of view (e.g. DRM effectiveness). We submit that in the complex picture surrounding DRM there are also human (social/legal) aspects that need to be explored elsewhere, on the side of content producers, whereas some other human (e.g. legal/economic) issues should be pursued among the content distributors and the policy makers.

The data we analysed in this paper suggests that while DRM circumvention is an essentially "human" problem, as it raises socio-cultural and legal issues, the only available solutions are "technical". In practice, industry-led research only aims at an increasingly effective DRM to address the issue of circumvention. However, as DRM advances, so does DRM circumvention, as technology can be defeated by another technology. Focusing on the human aspects surrounding this technology, on the side of all players of the DRM game, can provide new and more effective tools to appease this contentious issue.