OPEN
RIGHTS
GROUP

Digital Handcuffs

How DRM disempowers consumers

Digital Rights Management and the battle for ownership of your digital life

September 2018

Written by Slavka Bielikova and Javier Ruiz Diaz

Table of Contents

This is an Open Rights Group report written by Javier Ruiz Diaz and Slavka Bielikova.

Open Rights Group would like to thank the following people for their contributions.

James Allen-Robertson
Ray Corrigan
Francis Davey
Andrew Katz
Peter Vass

Introduction

About this report

This report examines issues arising from Digital Rights Management (DRM) technologies and the legislation protecting these technologies. The report looks at how the use of DRM can impact on users' security, privacy and right of access, while also exploring how DRM stifles innovation and competition. Furthermore, the report looks into the phenomena of obsolescence and vendor lock-in facilitated by DRM.

We have looked at various industries where DRM technologies have been employed and examined flaws introduced by their use. While companies increasingly use DRM technologies to further their profits and not merely just to protect intellectual property, it is the legal framework that enables companies to do so. This report also examines legal regimes in the United Kingdom, the European Union and the United States that protect anti-circumvention provisions prohibiting removal of DRM technologies.

What is DRM?

With the continuous development of digital content and media, copyright industries started to develop technologies to prevent copyright infringement. These technologies are collectively named Digital Rights Management (DRM). While the industries using DRM insist it is about "copying" and "consumer behaviour", the main benefit they accrue is control of the technology, or distribution of products, and therefore control of pricing and products. This is inherently anti-consumer and pro-monopoly, and we can observe these effects in practice.

Copyright industries successfully lobbied governments and international bodies that took the initiative to include provisions on DRM in international treaties. The treaties delivered international standards for digital rights management and bound their signatories to uphold the “rights” of copyright holders. Legislation from the EU, UK and US all contain clauses and articles that reflect requirements from the international treaties.

The term “digital rights management" is currently used to cover two related aspects that have become indistinguishable. DRM proper refers to “rights management information” — systems and tools to enable rights-holders to identify works and establish authorship (e.g. watermarking), as well as managing terms and conditions.

The other term that is often used interchangeably is “Technological Protection Measure" (TPM). TPMs are devices or software designed to enable rights-holders to control the uses of copyrighted materials after purchase. In this section of the report we will use the precise terms, but elsewhere in this paper, DRM will be used to encompass all forms of technical controls.

TPM mainly covers anti-copying and access control mechanisms. For example, the game Microsoft Adventure from 1981 was sold on floppy disks with so-called “bad sectors” that could not be copied under normal circumstances, so only original disks would be played.[1] But the development of access controls has created significant controversy because they affect how legitimate users can enjoy their purchases. Many computer games now require users to be connected to the company’s platform all the time. Ebooks can have all forms of restrictions on copying

[1] http://www.gamepressure.com/e.asp?ID=131

text — making quotations and studying more difficult — and Amazon has even deleted purchased ebooks due to changes in licensing.

DRM and TPM are in general seen by industries as providers of security for their products. Often the reason the manufacturers use protective measures is because they feel threatened by their customers. In their view, customers' behaviour can pose a threat if they decide to copy or alter products and services they purchased.

Changes to ownership

The perceived threat posed by customers' conduct has led to a change in ownership. DRM technologies treat access to the lawfully-acquired products as temporary — users do not have control over their products and have to abide by the rules established by an external authority.

The rules created by an external authority are not the product of a legislative process. They generally go beyond the restrictions defined by copyright to extend control into new areas and business models. Rather they are an agreement between a retailer and a publisher or a manufacturer that is then imposed on the public. Leaving out the legislative process results in contractual licence terms enforced by unchallengeable technical measures being used as a replacement for due process.

Partially due to DRM, ownership can now be divided into two categories: analogue and digital. Analogue ownership corresponds to physical ownership of products. Demands of copyright law prevent users from making copies of products but otherwise, if consumers own an analogue product, it is theirs to do with as they please.

However, ownership within the digital sphere is marked by an impermanent access to products. The lack of legislative process and the rise of licence terms in its stead has led to a loss of certain rights with undue restrictions on how or when media can be consumed, in a way that would be unacceptable when applied to analogue copyrighted works. The terms can vary widely, and it becomes unclear what rights consumers actually acquire. As such, it would not be appropriate to talk about "digital ownership" but rather a "digital rental" status.

Years of ownership practice reinforced by legal rules created certainty for consumers who know what rights they acquire when they purchase an analogue product. The certainty in purchasing digital products is lost when ownership rights are defined by the variable and illegible text of licence agreements.

At the same time, DRM allows for automatic enforcement of licence terms. DRM technology has shifted from a largely placid form of authentication of legitimate purchases to a technologically-embodied philosophy that views all users as threats whose actions need to be monitored and must have limits enforced on their use of products they purchase.[2]

Unlocked by DRM, the possibilities to control consumer behaviour have also pushed the market toward the further use of protective technologies as a way to fight competition, even where there is no fear of infringement

[2] Aaron Perzanowski. "The End of Ownership: Personal Property in the Digital Economy (The Information Society Series)."

Issues with DRM

A closer look into the implications of using DRM shows that users' needs are constantly overlooked. DRM technologies are inherently anti-consumer.

Laws provide limited consumer protections through exceptions that allow copying in the EU, UK and US. These exceptions do not function in a satisfactory manner to create parity between the use of a product without a digital component and a digital product. Having to contact the rights-holder or the rights distributor to make private copies and copies to create disability-accessible versions of products are still common problems today. So are the issues around research into the copyrighted products that lead to declining opportunities for innovation and for the establishment of competing businesses.

Placing restrictions on consumers' use of digital products or products with digital components goes inherently against consumers' rights and creates a hostile relationship where the consumer is now viewed as a civilian competitor.[3] The hostile relationship justifies (to rights-holders only) the use of security measures against the "civilian competitors" who are trying to diminish rights-holders' profits.

Instead, rights-holders use security measures and mining of users' private data to lock them in to their brand, making it near impossible for users to switch to another service or

[3] http://www.coreach-ipr.org/documents/Reinout%20van%20Malenstein%20[Compatibility%20Mode].pdf

device. Vendor lock-in is particularly unfair when the product becomes obsolete leaving users without a functioning product and monetary loss.

DRM removes basic control over technologies we rely on for our work and relationships, allowing rights-holders to control not just how we consume their works, but how we use our own tools.[4]

The UK government has called for parity of the online world with the offline world in other areas of the digital economy. This parity approach would improve the current inferior position of consumers when they encounter DRM. It would create an environment where consumers can enjoy the same rights reading their books in a digital format as they can enjoy when reading books in a paper form. It would mean that users could make copies for personal use, lend their products to as many users and as many times as they wish (in a non-commercial way), adjust them to be able to use them in specific ways, easily incorporate products in research, or use them with compatible products produced by other brands.

Consumers have certain expectations of products they buy. Their expectations tend to be similar whether the product is digital or not. However, deliveries of these expectations differ greatly for digital products due to digital rights managements mechanisms imposed on them. DRM limits what users can do with their products, which creates a tension between the technology and entertainment industries[5]. Consumers are not always properly aware of the existence of DRM on their products, which then leads to

[4] https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

[5] http://people.ischool.berkeley.edu/~pam/papers/notice%20of%20DRM-701.pdf

limitations on product use. These limitations include issues related to legitimate uses, disability, security, privacy, innovation and competition, obsolescence and vendor lock-in.

Legitimate uses

DRM is used to protect copyrighted material from being copied or used in other ways that have not been authorised by rights-holders. However, copyright legislation usually offers several exceptions when users do not need to seek authorisation from rights-holders to engage in certain uses. Terms describing activities users are able to perform without specific permission vary from “fair use" in the US to "fair dealing” in the UK and “exceptions and limitations” in EU law. In general, they can be described as legitimate uses of copyrighted material.

All of the above concepts allow users to use works that have been copyrighted in a way that does not infringe on the rights-holder’s profit from the work. Countries employ different tests to assess whether the use can be justified as fair or legitimate. The acts that can be classified as legitimate/fair use of copyrighted materials include, predominantly but not exclusively: copying for private use; use for education or research purposes; news reporting and parody; as well as pastiche.

In practice, this would mean that users should be able to make a copy of a music album, ebook or a film they purchased if they want to play it or read it on a different device or in a different format. Likewise, users should be able to use or access copyrighted works if they are subject to academic research or they are used illustratively during an educational process. These are just some of the activities that are permissible with copyrighted works provided that users do not offer them to the general public in their original form for profit.

Users already experience issues when attempting to claim legitimate use of copyrighted material. The issues are further exacerbated when DRM is used to prevent users from duplicating copyrighted material. DRM mechanisms are designed in a way that users cannot disable them, and as a consequence, they are prevented from utilising the exceptions afforded to them by law. As such, DRM is a barrier between users and their legitimate use of copyrighted products.

Libraries are one of the many actors that are affected by the DRM barrier. They often find that they are not allowed to lend or copy ebooks, even though it falls within their main function[6]. Publishers are worried that untrammelled lending of ebooks will impact on their commercial interests. Publishers have made very few arrangements to accommodate the needs of libraries to facilitate access to ebooks. Libraries often face problems when attempting to download a copy to make it available for people with disabilities or when the “lending licence” expires after a year. Such a situation makes it impossible for libraries to fully exercise the exception to which they are entitled.

DRM could harm user security, but experts conducting research in this area often face legal threats, despite the exception for research being available. Often, company interests have more weight than user interests even though user interests are supported by legal exceptions to copyright.

[6] https://www.theguardian.com/books/2010/oct/26/libraries-ebook-restrictions

In order to break down the barrier, users would need to appeal to the rights-holder to ask them to disable the protection measures in the name of legitimate use. If rights-holders require users to ask them for permission to disable DRM the principle of legitimate use is completely redundant. Legitimate use was introduced so the intermediary step of asking for permission could be left out but, because of DRM, it is still present.

The user's right to disable DRM to exercise their right to an exception is not automatic. Users are required to contact the rights-holder or other authorised third parties to provide them with tools to access a non-DRM copy of the copyrighted product since EU, UK and US laws all prohibit circumvention of DRM.

From the users' perspective, they have paid for their product and would expect to have full ownership of it. That would include the possibility to make copies for users' personal use. However, copyright-protected products have technological measures applied to them to prevent users from copying the products. In many cases, users are able to circumvent the measures but that puts them in a position where they have committed an offence.

Circumvention of protective technological measures is prohibited and criminalised, but the laws of the EU and the UK (not the US) accept it in certain cases. The exceptions to circumvention of DRM are broadly in line with the general exceptions for use of copyrighted material. The legislation allows for removing DRM when the user wishes to make a copy for private use, making it accessible to people with disabilities, and for teaching purposes, non-commercial research and private study, a as well as allowing access to the material for the purpose of parody or reporting the news.

DRM technologies are meant to protect against acts not authorised by the authors or permitted by law. In principle, this may sound sensible, but in fact, it is a complete rewriting of the relationship between consumers and rights-holders. Instead of selling a book, now the author can provide a closed list of options for how the book is to be used.

There are many potential uses of a work that may not have been foreseen but are completely legal, and DRM can be used to stop these, which could particularly affect consumers who have obtained lawful copies. DRM has been described by critics as “the right to make up your own copyright laws, the right to invent things that people aren’t allowed to do — even though the law permits it — and to embed these prohibitions in code that is illegal to violate”.[7]

Exceptions for reproduction of computer programs

Computer programs are generally covered by separate legislation protecting their copyright and exceptions to their copyright differ slightly. It is common for legal owners of computer programs to be able to create backup copies, modify them to correct errors, decompile the program or observe, study and test it (i.e. reverse engineering).

Otherwise, removal or circumvention of any technological measures protecting a computer program is prohibited by law. However, the interpretation of the law is not always straightforward and legitimate application of exceptions could end up being put aside in the name of the rights-

[7] http://www.theguardian.com/technology/blog/2014/feb/05/digital-rights-management

holders' interests. This was the case when the Recording Industry Association of America (RIAA) and the Secure Digital Music Initiative (SDMI) attempted to use the Digital Millennium Copyright Act in the US to stop the Princeton professor Ed Felten and his team from publishing their research into vulnerabilities of the SDMI.[8]

None of the DRM systems (in the above case SDMI) provide impenetrable protection for copyrighted content. DRM technologies encrypt protected content in certain ways and hide decryption keys from users. Finding ways of breaking DRM technologies goes hand in hand with creating DRM technologies. As soon as they are created, there will be attempts to crack them for both legitimate research and innovation purposes, as well as for malicious reasons.

DRM technologies are subjected to reverse engineering to understand how they work, or in the case of DRM-protected software, to study for purposes of further technological advancement. Reverse engineering is fundamental for interoperability of various products. Restricting reverse engineering would have a serious impact on software development. Furthermore, copyright owners would be able to develop a monopoly over related products (similar to the Apple business model).

Disability

The rights of people with disabilities are particularly affected by DRM. Those with a visual impairment may need to convert text to speech, or those with hearing difficulties may require specialist equipment to listen to music. All these activities may not be authorised by rights-holders.

[8] https://w2.eff.org/IP/DMCA/Felten_v_RIAA/faq_felten.html

People who have a certain form of sight disability might need to magnify the text or transform it into a synthetic audio or a temporary braille display. Often, in order to have the same access to material and content as people without sight disability, it is necessary for visually-impaired people to use "screen reader" software or another form of assistive technology. Digital rights management technology tends to classify assistive technology as an illegitimate add-on and blocks it, despite the use of assistive technology falling within the legitimate uses of copyrighted material.

This is a discriminatory practice. No case has been made for technical or commercial reasons to justify disabling assistive technology.[9]

Most text-viewing software can be configured to restrict or allow the use of access tools (e.g. screen readers). It is up to the publisher to choose the settings and enable the use. However, more often than not, publishers disable the permission for assistive technology and make it impossible for people with disabilities to access the material they legally purchased.

The issues with the use of the assistive tools are not specific to people with visual impairment. Those with hearing difficulties or learning disabilities share this struggle.

The situation can be easily improved by setting up a way so that the DRM system would be able to recognise a trusted assistive tool and unblock the content for the user by default. Alternatively, publishers could liaise with providers

[9] http://www.indicare.org/tiki-read_article.php?articleId=170

of assistive tools to disseminate instructions on how to access the material.

The law (Marrakesh VIP Treaty[10], WIPO Copyright Treaty[11] and WIPO Performances and Phonograms Treaty[12]) allows for form alteration in order to access the content through legitimate uses. However, the law is not strictly imposing this on rights-holders and offers loopholes that allow them to avoid making their content available for people with disabilities (more in-depth analysis of the law and disability can be found in the section on Law). This practice is particularly puzzling because it is also in the publisher's interest to make its content available to as many potential customers as possible.

Security

Security, when speaking of DRM measures, often relates to more than just security.

Companies normally employ various control measures into their products for three reasons:[13]

- to tackle data protection;
- to identify unique recipients to enable access control for the digital content;
- to enforce content usage rights.

DRM systems are able to collect data about users and, by law, in such cases, they should also engage in data

[10] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=301016#art4
[11] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295166
[12] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295578
[13] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.3484&rep=rep1&type=pdf

protection against unauthorised interception and modification.[14] Data protection measures in DRM technologies are there to protect users against outside threats. Most likely, this is what users envisage "security" means when companies present them with a statement informing them that their products contain security measures.

However, companies have been using the term "security measures" to describe technologies that control users' use of content. These technologies do not prevent against any outside threats but the user itself. In relation to DRM, users are the threats and DRM technologies protect companies from them and the undesirable ways they use their products.

The terms "security and control" have been used interchangeably by companies using DRM. By calling the measures "security measures", companies are able to force them against users' interests while convincing them the measures are in place for their own safety[15]. In reality, they are using the terms to help restrict what the users are able to do with the products they have purchased.

These "security measures" cause the user's loss of control over the product.

DRM helps companies to achieve their economic goals

[14] http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.12.3484&rep=rep1&type=pdf
[15] https://www.wired.com/2008/02/securitymatters-0207/

rather than protecting the product users. Users, after interacting with a digital rights-managed product, are often left less secure when confronted with a malware attack on their devices. Users are continuously misled about control measures applied to their products, and told they are there to protect them from outside harm; but predominantly, they are there to cause harm to their relationship with the product manufacturer/company, not a third party. This harm is demonstrated in cases where users lose control of their own property; hence, their consumer rights have been violated.

The control aspect of DRM technology is what makes it possible for companies to increase their ability to “lock in” customers.

Stifling innovation and competition

DRM affects businesses and other stakeholders because it stifles innovation, as any new and emerging uses that may not be covered are disabled and any technical attempts to bypass them are illegal.

The criminalisation of the circumvention of technological protection measures (DRM) has led to serious problems for technology developers trying to achieve interoperability and for security researchers, who are prevented from discussing vulnerabilities in such systems. These restrictive systems are becoming deeply integrated into technologies ranging from the obvious, such as computers, to cars and even coffee makers.

In the US there are concerns that restrictions on the analysis of DRM in car software have helped cover the manipulation of diesel emissions testing.[16] Volkswagen's software for repairs and diagnostics protected by DRM does not allow other "non-official" mechanics to service their cars. The official mechanics are bound by non-disclosure agreements and as such are prevented from disclosing any discrepancies. Circumvention of DRM technology is in many states considered an offence and prevents non-official software to be used for servicing Volkswagen cars. DRM technology made it impossible to carry out independent scrutiny and facilitated criminal fraud, which went undetected for a long time.[17]

This brings us back to the main control aspect of DRM. Despite ostensibly being about protecting authors and unlawful uses of works, DRM systems are used strategically by rights-holders to create and control markets. DRM is the basic enabler of the geo-blocking of content for example, but more importantly, it is used to lock in consumers and lock out competing firms.

Amazon uses its own DRM, and locks buyers out of their ebooks on their own Kindle readers, forfeiting potential sales to owners of other devices. Other large competitors have a similar approach. This has led to small independent distributors that cannot afford the costs of maintaining DRM and would prefer to sell ebooks on multiple platforms being

[16] https://supporters.eff.org/civicrm/mailing/view?reset=1&id=1234
[17] https://bbs.boingboing.net/t/vws-car-drm-let-it-get-away-with-cheating-on-its-diesel-emissions-testing/65920

locked out of the market.[18]

Successful companies such as Amazon can be challenged by market forces and other innovators. DRM is used by large firms to leverage copyright — and specifically anti-circumvention provisions — to convert their challengeable superior market position "into an unchallengeable legal monopoly".[19]

This is also the case with Apple's app stores and other sectors, such as media-playing devices. Legislation protecting anti-circumvention measures was used to block competition in laser printer toner cartridges, garage door openers, video game console accessories and computer maintenance services.[20]

The law aims to ensure copyright's technological protections. But the protection DRM provides can also be protected/provided through code and contract.[21] The number of protections provided by DRM measures makes the number of technical possibilities for innovation and exploration slimmer. DRM protection perpetuates a world where computer scientists need to get a lawyer's approval before conducting research. Innovation and competition are constantly stifled in many fields. Open development can only be achieved with new tools to challenge anti-

[18] http://www.theverge.com/2013/2/21/4010504/amazon-publishers-face-class-action-antitrust-suit-from-indie

[19] http://parkerhiggins.net/2014/05/accepting-amazons-drm-makes-it-impossible-to-challenge-its-monopoly/

[20] https://www.eff.org/pages/unintended-consequences-fifteen-years-under-dmca

[21] https://works.bepress.com/wendy_seltzer/1/

circumvention.

Privacy

Privacy and DRM relate to each other on several levels. Technologies protecting copyrighted content create tension between the protection of intellectual property rights and the maintenance of consumers' privacy rights. Most DRM systems will register some personal data of their users. In this situation users inevitably lose a certain part of their privacy due to DRM being used on a product.

Often it is not clear to users what data is being collected or that any of their data is being collected at all.

DRM technologies such as digital watermarks, encryption and electronic agents for monitoring information usage are all used to provide basic functions of DRM. These include controlling access to copyright works, restricting unauthorised reproduction, and identifying the copyrighted works and their owners while protecting authenticity.

Various DRM strategies exercise different levels of data collection[22]. The least amount of data is collected when digital content is directly downloaded with the files containing DRM metadata that carry the information about the user's rights. In practice, this could look like downloading a PDF document where a user would only be allowed to view it and print it but could not edit it. Content and rights are both transferred to a user's computer once,

[22] https://adam.shostack.org/privacyeng-wspdrm01.pdf

and there is no need for the DRM system to monitor the user's actions.

Another type of DRM strategy ties downloaded content to a particular device. This means that the server managing DRM will have to be updated every time the copyrighted digital content is used on a new device. Tying content to a set of devices could put some previously private information about the user at risk of excessive tracking.

More data collection through DRM occurs when DRM is designed to tie content not to a particular device but to a particular user. This DRM strategy involves signing into a service and then downloading the content. In this way, the DRM system can gather information about users, including their complete listening, reading and viewing history. The computer gaming platform Steam uses this model. It allows its users to purchase different games through their accounts. They can access their accounts on any computer and play the games on any device as long as they identify they are the account holder.

The most intrusive DRM strategy involves no content downloads. Instead, users subscribe to a service that offers content on their platforms that they can access from any device. This is the case when content provision is tied to a service, a service that allows for the massive collection of usage data as well as personal data.

All the collected data is protected by legislation covering data protection and as such, it should not be collected, stored or shared in excess. Users often enter into a contract when they merely purchase a product or a service. The contract is used as their consent to data processing. Company or rights-holders might need to process their data in order to allow them access to the copyrighted material. However, in many cases, it is not made clear to users that their data might be used for more than just their identification by the rights-holder.

Users' data can be used to track their behaviour in relation to copyright infringement and non-permitted acts, but also in other instances — i.e. whether they are engaging in copying, but also their general interaction with the product. Companies can use this information to adjust their service or target specific users for particular features and products. Additionally, the contract agreement could also allow them to sell users' data to other companies.

A particularly worrying aspect of DRM systems data collection is its interaction with copyright holders for the purposes of identifying users. DRM data has previously been sought after by rights-holders to identify users who repeatedly infringe copyright. This was the case when the Recording Industry Association of America demanded that the US Internet service provider Verizon disclose personal data of people accessing copyright-infringing material (RIAA v. Verizon[23]).

Obsolescence

On a regular basis, technological products become obsolete with further technological development. This has happened for example with cassettes and cassette players after CDs and CD players were found to be a more convenient medium for storing audio recordings. A technology product goes into technological obsolescence

[23] https://w2.eff.org/legal/cases/RIAA_v_Verizon/

once there is a new piece of technology that can be considered superior to the previous one that was fulfilling the same function.

If someone decides to play a cassette tape on a cassette player they still have in their possession, they are able to do so. But a problem arises when DRM is involved. The cassette player is capable of performing the function it was originally designed for, and DRM measures protecting tapes did not exist when it was created, so DRM never had an impact on it. It is obsolete purely because the quality of listening experience is better through other media. However, in general, if someone wishes to use cassettes, they can do so.

Once manufacturers decide to apply DRM technology to their product, when the product becomes technically obsolete, it is also very likely that it will become functionally obsolete. This means that the product would no longer be able to adequately perform the function for which it was created.

In cases of obsolescence, companies stop providing support for their products as it is no longer profitable for them to do so, or they cease the support because they go out of business.

This currently happens with ebooks and ebook readers, mobile phones[24] and MP3 players.[25] In one case, a retailer

[24] https://www.theregister.co.uk/2017/07/11/windows_phone_officially_obsolete/

decided to stop production of its ebook reader and offered to transfer customers' ebooks to an alternative system within a limited timeframe.[26] However, if the customers did not request the transfer within the specified time, they were left with "bricked" (unusable) devices and without any of the ebooks they had paid for (more detailed analysis of this case can be found in the next chapter).

Going out of business is not the only situation that can result in obsolescence. A DRM-protected product can be rendered functionally obsolete after an unauthorised retailer tinkers with its DRM mechanism. This was the case with several iPhone6 devices that had been repaired by repair shops not approved by Apple. When Apple released a software update, the devices were left "bricked"[27] and unable to perform the original function for which they were designed.[28]

DRM locked users into using a particular brand (vendor lock-in) and effectively prevented them from stopping their product from becoming functionally obsolete. If it was not for the ebook reader's DRM system, users could have easily downloaded ebooks they had purchased on to any other reader in any format they found suitable. This conduct should be permitted and should feature on the list of exceptions provided in the law for personal copying; however, none of the laws this paper examined offer

[25] http://www.cbc.ca/news/business/apple-ipod-nano-shuffle-gone-1.4225874

[26] http://www.thebookseller.com/news/nook-pulls-out-uk-323820

[27] "Bricked" refers to having the functionality or qualities of a brick

[28] https://www.theguardian.com/money/2016/feb/05/error-53-apple-iphone-software-update-handset-worthless-third-party-repair

special arrangements for personal copying or circumvention of DRM in the case of product obsolescence.

The issue of obsolescence demonstrates that physical ownership of products can be superior to digital ownership. Simultaneously it also shows that products that are technically obsolete still leave users with more consumer rights than functionally-obsolete products.

Vendor lock-in

Vendor lock-in[29] is an economic term that relates to the difficulty of switching from one product to a different or competing product. Every company aims to prevent their customers from switching brands and use various measures to achieve this. Many of them found that using DRM to achieve vendor lock-in is a very efficient way of doing it.

Lock-in can be created through:

- Use of proprietary software and obscure standards (for instance Microsoft's .doc)
- Network effect and active user base. People often feel obliged to use a product that can serve as a gateway to other services (Facebook and other social media platforms)
- App markets that are dependent on a company for add-ons. In the case of Apple's App Store, both vendors and users are dependent on Apple's approval.

[29] https://en.wikipedia.org/wiki/Vendor_lock-in

These techniques bind users to one technology platform and make it hard for users to extract themselves from the use of a product, as is the case when users find it difficult to switch from Apple products to Android products or PCs. A number of devices and software created to be compatible with each other improves users' experience once they are in the Apple "bubble". Better compatibility and experience then encourages users to stick to the same brand rather than face difficulties of cross-platform disharmony.

The line between copyright protection and consumer control is blurred when it comes to vendor lock-in. It is impossible to say in some instances whether DRM technology is being used to protect copyright or simply to facilitate a brand lock-in with copyright protection being its by-product. Such was the case with coffee makers Keurig[30] and printer ink cartridges.[31]

In both cases, users/customers were unable to use off-branded coffee pods/ink cartridges with their machines. The coffee pods and cartridges specifically produced by the companies to be used in the machines are higher in price than other pods and cartridges, but the machines would not work with any other substitutes that were cheaper. Lock-in strategies are developed to protect market shares while users have to face increased prices, which often go hand in hand with reduced customer service and a lack of innovation.

[30] https://www.wired.com/2015/05/keurig-k-cup-drm/

[31] https://arstechnica.com/information-technology/2016/09/hps-drm-sabotages-off-brand-printer-ink-cartridges-with-self-destruct-date

HP and other companies taking precautions to sustain lock-in are not just selling a printer; they are imposing the quality of ink and number of possible print-outs. It should be up to the user to decide how many good quality print-outs they want to get out of their ink cartridge. Customers merely purchased a printer. They did not knowingly enter into an agreement to only use corresponding branded cartridges.

A question that remains unanswered is how companies such as Keurig and HP can claim criminal protections against removing DRM from their products under anti-circumvention provisions of law if there if the coffee pods and ink cartridges have limited intellectual property value to be protected in the first place.

DRM not only results in people losing control over their devices, it is also one of the ways for companies to exploit their users by depriving them of options to use their own products in ways to which they should be entitled.

Vendor lock-in is made viable by a combination of factors. One of them is the fact that there is an imperfect set-up when it comes to exercising the right to legitimate use of copyrighted products. Data collection via DRM is another; it allows companies to obtain more information about their users. Security measures applied to DRM to prevent users from disabling it so as to unlock their device to other brand possibilities is another. Vendor lock-in is the underlying cause of product obsolescence.

DRM threatens the open web

In 2018, the World Wide Web Consortium (W3C) approved new web standards that will integrate DRM into browsers. The new standards allow the use of Encrypted Media Extensions (EME) that make it possible for video and audio providers to discover as well as enable DRM providers offered via a browser. EME provides a method for browsers to interact with a content decryption mechanism (CDM) and a server that provides decryption keys for encrypted media content. It enables encrypted video including audio playback directly in HTML5 without the need for additional third-party plugins that must be downloaded and updated by the user. EME allows the same encrypted videos to be played in any compliant browser regardless of the DRM system used.[32]

Prior to the EME standard, online video content could be encrypted and decoded by a third-party plugin applied to the video by the website owner or holder of the rights to the video. EMEs place the capability and responsibility to decrypt online video content on the web browsers themselves, but with closed blackbox components. EMEs have now been in place for some time but not as an open standard. Making it an open web standard will make DRM protection of online video content a default setting and will give it legitimacy. Online video platforms, thanks to EME, now possess all the necessary tools to control users' browsers so that they can only watch their content by

[32] https://drmtoday.com/faq/#html5eme

complying with their rules.

W3C skipped on any safeguards while regulating the EME integration into browsers. There are no protections for accessibility, security research or competition. These are legal exceptions that fall within fair-use/fair-dealing provisions provided in legislation in the UK, EU and US. However, there are also provisions in the copyright laws of different countries that prohibit circumvention of DRM and criminalise it. That could put people who attempt to remove it for legitimate purposes, such as providing accessibility for disabled people, in a position where they breach the law.

Many organisations and industry experts opposed[33] the new web standards. Among the objections raised were:

- Inadequate protection for users;
- Difficulties in supporting the specification in free software projects;
- Lack of definition for Content Decryption Module[34] implementation;
- Lack of a covenant regarding anti-circumvention regulations;
- Challenges for adaptation for people with disabilities;
- Challenges for new market entrants and inadequate specification for the open web;

[33] https://www.eff.org/deeplinks/2017/07/amid-unprecedented-controversy-w3c-greenlights-drm-web

[34] Content Decryption Module is the client component that provides the functionality of a decryption mechanism. If a browser supports EME, it needs to have a license for CDM, and these are mainly controlled by a handful of companies. This will stop new entrants to the market who would like to provide browsers, because they will find it difficult to obtain licences.

- Archiving of content.

In their statement,[35] the W3C said that some of the objections had already been addressed and others were overruled. Some organisations, including the Electronic Frontier Foundation (EFF), suggested a compromise that would still achieve what the proponents of DRM and EME hoped they would. EFF proposed a covenant[36] that would require members of the W3C to make a binding promise not to use anti-circumvention provisions of copyright law to attack people who bypassed EME standards for legitimate purposes. These could include students, researchers or people with disabilities.

However, the compromise was rejected, and the EME standards were supported by W3C's largest corporate members and leadership. Following this decision, EFF decided to resign from the W3C.[37]

Having EME included in web standards will legitimise the act of suing security researchers who discover flaws in the use of EME by online video services. The current legal framework, both in the UK and the US, prevents security audits. Both legislations hand too much power to the companies to control the disclosure of vulnerabilities. Provisions protecting against circumvention of DRM allow for a very limited application of exceptions for security research. [38] Previously these exceptions were disregarded, and security researchers were either threatened or taken to

[35] https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0000.html

[36] https://www.eff.org/deeplinks/2016/06/w3c-eme-and-eff-frequently-asked-questions

[37] https://www.eff.org/deeplinks/2017/09/open-letter-w3c-director-ceo-team-and-membership

[38] In the US every three years there is a review of DRM circumvention, with the last one taking place in 2015: https://www.fsf.org/news/library-of-congress-issues-limited-exemptions-to-dmca-anti-circumvention-provisions-but-leaves-users-without-full-control-over-their-own-computing

court over circumvention of DRM measures.

To prevent such situations, security standards bodies should provide legally-binding guarantees that there can be open and legal audits of the standard. The audits should be done without needing to ask rights-holders or CDM providers for permission.

Most companies have their own security disclosure policies. If the language of these policies was changed to agree to not prosecute security researchers involved in audits, then vulnerabilities introduced by DRM systems could be significantly reduced. Regarding the EME standard, change in the language of security disclosure policies would concern the four major browser vendors (Microsoft, Apple, Google and Mozilla) as well as one non-browser system (Netflix).[39]

There has not been a compelling argument for introducing DRM within browsers. Tim Berners-Lee, the director of W3C, outlined his position[40] by saying that since DRM already exists for video content and it is unlikely to disappear, it is better for DRM-protected content to be a part of the web ecosystem than to separate it from it. Long-term concerns about W3C remaining a relevant player in the future of the web as companies independently develop private standards have also played a role.

Online video services are hardly helpless without the EME as a web standard. The companies would still be able to use their own application or browser plugins that would deliver the same effect as the EME without the push for it to

[39] H. Halpin, (2017). “The Crisis of Standardizing DRM: The Case of W3C Encrypted Media Extensions”.

[40] https://www.w3.org/blog/2017/02/on-eme-in-html5/

be a default setting all standards-compliant browsers must implement. Moreover, the web standard will not protect online video services unequivocally. It will, for example, prevent users from using screen-capture software within an online video streaming service (such as Netflix) but it will not stop users from using screen-grabbing software outside the browser. This would still allow users to capture online video content on their computers despite the DRM web standard for browsers. CDM-protected series and films from services such as Netflix are routinely made available as unauthorised downloads or streams soon after their release.

Often an argument made by people and companies in favour of DRM is that if users are not happy with it, they can use other products not containing DRM.[41] This is not possible if web standards incorporate DRM into web browsers.

DRM applied to online video by default will make it impossible for innovators to make any future improvements to the systems. It also makes it difficult for security researchers to disclose any vulnerabilities without being prosecuted under copyright laws — e.g. Section 1201 of the US Digital Millenium Copyright Act and Article 6 of the EU Copyright Directive — that prohibit circumvention of technological measures such as EME. In many cases, DRM on online video platforms will render them unusable for people with visual or hearing disabilities who require additional software to make the online content accessible to them in other formats.

Berners-Lee argued that a large proportion of consumers

[41] https://boingboing.net/2017/01/30/google-quietly-makes-optiona.html

do not appear to be concerned with the issues caused by DRM since they continue to buy or subscribe to DRM-protected content. What he failed to note in his limited analysis of the DRM situation is how severely this will impact on certain groups of people.

DRM for video is there to protect rights-holders. There is nothing about DRM that makes the experience of viewing online video content better for the user. Users simply put up with DRM because they want to enjoy the convenience of the service. But once the service stops being convenient it becomes obvious that the new W3C web standards are merely a tool for these companies and rights-holders to protect their profits while disregarding the principle of equality or the right of access. Service demonstrably stops being convenient for many people with disabilities who by default will not be able to use the tools that enable them to use the online video service.

Companies and rights-holders see DRM solutions as a tool to empower creators, publishers, and distributors of proprietary, confidential or revenue-generating content. They claim the need for DRM has increased due to the growth of digital media and conversion from analogue to digital technologies.[42] Rights-holders find an increasing need to protect their profits, which are being threatened by consumers abilities to “rip” media or share it using peer-to-peer file-sharing tools.

Next, the report looks into the practices related to the use of DRM by various companies and industries.

[42] https://www.encoding.com/digital-rights-management-drm/

Case Studies

Ebooks

Since the development of web-publishing, publishers have tried to protect their online books/files from illegal copying by applying DRM to them. However, enforcing copyright protections on electronic copies raises distinctly different challenges when compared with copyright protection on physical copies.

Consumers copying physical books for more than just their private use would be highly impractical. Copyright protections that are placed on physical books are there to ensure that publishers do not misuse works for their own profits; consumers are not a threat to the physical book market. The circumstances are different for ebooks. Their digital format makes it possible and fairly easy for consumers to copy books and potentially distribute them on a commercial scale.

There are several ebook readers and providers of ebooks (Amazon Kindle, Sony's Kobo, Google, Barnes & Nobles' Nook, Apple etc.). The variety of providers for ebooks and ebook readers creates serious shortcomings in consumer experience. Three DRM systems are most frequently used by the major ebook retailers:[43]

- Amazon has its own DRM system for Kindle eBooks and it maintains complete control over it — only Kindle ebooks sold from Amazon's website will have DRM; ebooks sold on other websites in non-Kindle format will not be compatible with it.
- Apple uses its FairPlay DRM on ebooks purchased

[43] http://ebookarchitects.com/learn-about-ebooks/drm/

from its iBookstore. Similar to Kindle, FairPlay is not compatible with any other device other than an Apple product.

- Adobe Digital Editions Technology Protection (ADEPT) is used by several ebook retailers (apps for iPhone and iPad, Android devices, Barnes & Noble's Nook) and allows users to obtain a licence to host a DRM server for other ebook stores.

All three DRM systems have been circumvented. Customers can obtain software that converts different ebook formats, so they can be used on any devices regardless of their manufacturer. The converting software renders DRM for ebooks essentially useless. So the only benefit of using DRM systems is to keep "honest people honest".[44] Users who are unhappy with DRM placed on products they purchased are able to bypass it, but such action comes at a cost of breaking terms of service and most likely voiding their warranty.

DRM applied to ebooks does not serve its original function — to prevent copyright infringement. Instead, it is used to expand rights-holders' control and create "artificial" rights to the detriment of users.

Ebooks are a textbook example that justifies the need for more rules to govern DRM for the benefit of consumers. Many of the issues outlined below could be alleviated if there were rules in place about providing a warning that the ebook device contains "security features" that will limit what users can do with their devices and ebooks. Likewise, further regulation is necessary for cases of obsolescence to

[44] Fritz Attaway at House Judiciary Committee Hearing on the Broadcast Flag, March 6, 2003; transcript available from https://www.gpo.gov/fdsys/pkg/CHRG-108hhrg85490/html/CHRG-108hhrg85490.htm

avoid putting consumers at a disadvantage and causing any monetary loss or dissatisfaction.

Ebook providers locking in their customers

When wanting to switch to a different ebook provider, users often find that they lose the books they had purchased because the DRM systems used by the two providers are not compatible. This can result in users sticking to one brand, despite their dissatisfaction with the ebook provider's service.

DRM technologies used in the ebook industry have made the process of achieving lock-in for companies easier. Amazon's Kindle, Barnes & Noble's Nook and Sony's Kobo all offer books in formats that are incompatible with each other. As a result, users can only access the books they bought on the designated device or through the company's app.

If users want to switch to a competitor's product because it is technologically superior, they will not be able to. They will be prevented from doing so due to the investment they have made into the ebooks purchased from one provider. Of course, users can choose to circumvent DRM protections on their ebooks and readers, but they will lose their warranty. This is a price many consumers will choose not to pay.

A report by Author Earnings[45] showed that in reality DRM harmed the sales — 50% of non-DRM ebooks accounted for 64% of sales and independent titles without DRM sell twice as many copies each as those with DRM. Following the current trends, DRM to lock customers in might not be

[45] http://authorearnings.com/report/july-2014-author-earnings-report/

the best commercial strategy for ebooks. It could be argued that a universal design allowing cross-platform use of books and adaptation for specific disability needs would be beneficial not only to customers but also to ebook companies.

Ebooks readers collect their users' data

In 2012, the Electronic Frontier Foundation (EFF) produced a useful guide[46] to what data different ebook readers collect. Most of today's ebook readers connect constantly to the Internet**,** which allows them to record every purchase and book search. As explained in the Privacy Notice related to Kindle,[47] they also "collect session information, including page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), as well as methods used to browse away from the page". On mobile apps, they also acquired information about the location of the device. Other ebook services work in a similar manner.

Many of the ebook providers will make this information available to law enforcement. It is likely that this information is predominantly collected to alert law enforcement when someone is reading material that could be related to the preparation of a crime. However, it is not clear what reading list would make Amazon or Sony alert law enforcement.

Ebook magic — providers will make your book disappear

Ebook users have very little control over what they can do with their readers and ebooks. Rights-holders, or the providers of the ebook system, can control withdrawal of purchases, the number of devices an ebook can be

[46] https://www.eff.org/pages/reader-privacy-chart-2012
[47] https://www.amazon.com/gp/help/customer/display.html?nodeId=468496

accessed on or ebook accessibility based on a country of residence.[48]

Amazon was able to remove copies of 1984 by George Orwell from all the users who purchased the ebook after it emerged that the publisher did not have the rights to do so. This is one of the most blatant differences between online and offline books. Users would not encounter publisher's representatives at their doorstep demanding they return their books because the publisher and retailer made some mistakes along the way. It would be time-consuming and impractical to do, resulting in customers still having copies of 1984 on their bookshelves. However, Amazon can remove ebooks because data ties each ebook sale to a particular customer and because of the technology it uses that makes the process of removing the ebook automatic.

Printed books can be easily carried around without any issues regarding their geographical location and lent to as many people as the book owner finds fit. Unlike paper books, most ebooks are affected by the number of different devices on which they can be downloaded. Most often, ebooks can be downloaded on six different devices, but the number is at the discretion of a publisher. It is also at the discretion of a publisher or ebook service provider whether ebooks work when they are bought in one country and then taken to another country. If the other country does not offer the service, an ebook user will be unable to access it. This was the case with Google Play Books, when a user could not access his ebooks in Singapore because the service did not exist there. Such ebook arrangements essentially make it impossible for travellers to purchase ebooks whilst abroad.

[48] http://www.digitaltrends.com/mobile/ebook-drm-5-reasons-to-free-your-kindle-library/

What happens when an ebook reader becomes obsolete?

It is a common occurrence that when ebook stores go out of business their servers go down too. In these cases, ebook users who did not make arrangements to download copies of the books they purchased will find themselves losing their whole collection.

Closed-down businesses also raise the question of old formats and outdated software, as well as hardware, that is needed to read them. If it is not possible to convert old formats, users will be unable to ever access their books.

Users can avoid most of the issues caused by ebook DRM systems by creating a personal copy of their purchased book. That, however, can put them in a position where they breach terms and services that could potentially result in copyright infringement if the user’s country does not allow for a private use exception.

The constraints DRM systems place on the use of ebooks are not comparable with copyright protections placed on physical copies. Printed copies of books have their use restricted in a minimal way. In this sense, ownership of digital goods is inferior to physical ownership.

An overwhelming number of DVD producers opt for DRM technology to “protect" their DVDs. This makes DRM technology for DVDs one of the most widespread DRM technologies. Being one of the most widespread technologies, however, also means that it is one of the most extensively bypassed DRM technologies.

Shortly after the DRM technology for DVDs was developed, Jon Johansen released an application called DeCSS that allowed a CSS-encrypted DVD to play on a computer running a Linux operating system — effectively bypassing the CSS technology.[49] Johansen was prosecuted in Norway following a complaint from the US DVD Copy Control Association (DVD-CCA) and the Motion Picture Association (MPA). He was acquitted of all charges. However, reproduction of the decryption keys that allow bypassing DRM is subject to restrictions.

A DRM system for HD DVD and Blu-ray Discs created by the Advanced Access Content System (AACS) was bypassed when process keys were published online. The first set of process keys was revoked but more keys were later generated.[50]

At present, DRM technology on DVDs can be considered redundant, as most of the DRM technologies came after the lawsuit and cannot be applied to DVDS. DVDs (and CDs) can benefit from an exception for personal copying under some legislations but DRM technology makes this legally impossible. Taking into consideration that redundant DRM technology does not aid protection of intellectual property, application of DRM technology to DVDs should be reconsidered altogether.

Device manufacturers

Printers

Some companies that produce printers[51] (most notably HP

[49] https://www.theregister.co.uk/2005/09/02/dvd_jon_mediaplayer/

[50] https://web.archive.org/web/20090124055806/http://www.boingboing.net/2007/05/30/new-aacs-processing-.html

[51] https://arstechnica.com/information-technology/2016/09/hps-drm-sabotages-off-brand-

and Lexmark)[52] designed their devices in such a way that they were only compatible with branded ink cartridges. Customers who purchased them were unable to use cheaper off-branded cartridges because the printer was able to detect through a chip that they were not “genuine”.

A number of issues arise from this approach to product manufacturing:

1. Off-branded cartridges are cheaper and can offer a comparable quality of print-outs but users of HP printers are now bound to buying an HP cartridge or their printer will essentially become a “brick", i.e. unusable.
2. Consumers bought a printer but upon making their purchase, they did not knowingly commit to buying only branded cartridges to use with their printers. This choice was pushed onto them by the company wishing to increase its profits from additional sales of ink.
3. By imposing the ink cartridge choice on the customer, HP diminished the consumer’s right to make their own choice for what ink cartridge to buy based on quality and price.

Most of the cases where DRM affects users’ rights and experience concern digital products or the transfer of analogue products into a digital form. So it is easy to see the irony of placing DRM technology on a device that eases the move of digital products into an analogue form. It is hard to see what copyright HP was trying to protect by using DRM technology. It would appear that the DRM was purely in place to protect its sales and assist brand lock-in.

printer-ink-cartridges-with-self-destruct-date

[52] https://consumerist.com/2017/05/30/why-the-supreme-courts-ruling-in-toner-cartridge-case-is-a-win-for-consumers/

Due to the big public outcry, HP eventually released a firmware that would disable the DRM technology for ink cartridges and customers were able to use other brands.[53]

A new approach to using DRM in ink cartridges was recently adopted by Epson.[54] Epson patented alignment of contact points on their cartridges. Their patent has caused issues for compatible ink cartridges, which cannot work without these patented aligned contact points. This means that in order for compatible cartridges to work, they have to infringe Epson's patent or be locked out of the market.

Coffee makers

The coffee maker Keurig developed a similar strategy[55] in the instant single-serve coffee making market in order to increase its sales and prevent their customers from using other brands.

Having purchased a Keurig coffee maker, consumers were stuck with the Keurig brand coffee pods whether or not they liked the coffee Keurig offered or the price of the coffee pods. The choice was imposed on them by Keurig. The printer and coffee maker stories are nearly identical because again, after a public uproar, the company decided to revert back to its original technology, which enabled other coffee pod companies to offer options.

The case of coffee makers (and any other device manufacturers) will only become monumentally worse with the spread of the Internet of Things (IoT). The recent

[53] https://www.wired.com/2016/09/hp-printer-drm/
[54] https://www.openrightsgroup.org/blog/2017/epson-delete-ebay-listings-citing-patent-claims
[55] https://www.wired.com/2015/05/keurig-k-cup-drm/

introduction of a smart coffee machine on the market saw the machine mis-performing when its scanning function failed. The machine first needs to scan coffee pouches that will let it know what it is brewing and how many beans will be added to the roasting chamber. After scanning once, the chip is rendered unusable. Due to the presence of the scanning error, owners of the machine are left with coffee pouches they cannot use.[56]

Vendor lock-in as demonstrated by the two companies discussed above could be mitigated by stricter rules for using DRM exclusively to protect copyright, not to further economic interests of companies. Particularly in these two cases, the copyright protected by DRM is not strong and the use of DRM points to the companies wanting to increase their sales.

Medical Devices

One of the most recent additions to the list of products that can be negatively affected by DRM are medical devices. Medical devices are increasingly equipped with a wireless interface because it makes it easier for medical staff to access them. DRM applied to medical implements restricts the configuration of the device, which allows the manufacturers to generate profit by offering compatible services, such as diagnostic software. Manufacturers can charge licence fees, restrict access to the service, or limit what other products can be used with the medical equipment.

DRM in medical devices creates two issues:

1. Potential bugs will be exploited through the wireless

[56] https://www.digitaltrends.com/coffee-tea-maker-reviews/bonaverde-berlin-brewing-system-review/

interface and DRM will prevent the fixing of these bugs.

2. DRM will create a brand lock-in through limitations on compatible products and services for medical devices, which can lead to increased prices on vital equipment as well as medication.

Copyright laws prohibit circumvention of DRM technologies but allow for exceptions for research and study into cryptography. These exceptions have been overlooked in the past, when a group of researchers in the US wanted to publish a research paper on how to remove a digital audio watermark. The researchers were threatened with a lawsuit if they published their findings.[57]

Anti-circumvention provisions in copyright laws around the world could have a similar effect on researchers who discover insecurities and potential faults in medical devices. In this case, they could seriously threaten people's wellbeing and lives if researchers do not feel safe to publish their findings.

The first issue could be mitigated if manufacturers were required to commit to not using anti-circumvention provisions to attack security research as a condition for certifying their products. Additionally, copyright laws should be amended to clarify that protection of DRM does not apply to devices that have no nexus with copyright infringement.[58]

Game consoles

Xbox, Sony's PlayStation and Nintendo have all been using

[57] https://www.eff.org/cases/felten-et-al-v-riaa-et-al

[58] https://www.eff.org/deeplinks/2016/04/pacemakers-and-piracy-why-dmca-has-no-business-medical-implants

DRM features to facilitate brand lock-in. The consoles only play games that were specifically made for them and will not work with games made for other consoles or PC gaming.

Gamers face similar issues as those experienced by people who purchase ebooks. As with ebook readers produced by different manufacturers using different ebook formats, the cross-platform incompatibility makes it difficult for users to switch from one console to another. Their investment in the purchased games as well as the console often amounts to hundreds and thousands of pounds.

Microsoft launched a new service that partly improves this business model. By purchasing a digital game on either Xbox One or Windows 10, users receive a free copy to use on the other platform.

The case of Microsoft expanding the game accessibility to both Windows 10 and Xbox One partly addresses the issues with product interoperability, but at the same time further facilitates vendor lock-in. Microsoft is hoping to become the dominant force in the games market[59]. Establishing its presence on two platforms could deliver stronger brand lock-in — users could be less likely to leave the Microsoft products once they come realise they are able to get a free copy of a game on one more platform.

[59] https://www.fastcompany.com/3061081/xbox-and-play-anywhere-microsofts-plot-for-perpetual-platform-lock-in

Apart from providing an avenue for lock-in, DRM on consoles and games prevents gamers from making their own backup copy. It also contributes to the infringement of consumer rights as well as copyright law, allowing for private copying. Additionally, gamers have to face eventual technical obsolescence of their consoles that will likely leave them with a stack of games they will not be able to play on newer devices.

Game console manufacturers (and other digital device manufacturers) should be subject to legally-binding rules on obsolescence. Such rules would ensure that the consumer is not in a disadvantaged position where they would lose out if their console is not supported by the manufacturer anymore and they would be compensated for the inconvenience.

Vehicle manufacturers

DRM systems have been increasingly used in cars and motorcycles. Companies use them in a way that “locks their customers in” — they make it impossible for users to repair or alter their cars and motorcycles to their liking; as a consequence, they are forced to use more services provided by the company. Manufacturers substantiate their behaviour by claiming they offer more security to users and ensure compliance with various regulations.

John Deere

An agricultural machinery manufacturer, John Deere, said: "The embedded code within the controllers and processors on our equipment [...] is designed so that our machines operate as intended, in a safe and reliable manner, and meet all appropriate safety and emissions regulations."[60]

A statement submitted by John Deere to the US Copyright Office made clear that its customers do not own the software that controls their tractors.[61] Despite owning the physical frame of a vehicle, they merely own a licence to use software installed in their vehicle. Since the vehicles would be inoperable without the software, by extension John Deere customers can argue that they only own their vehicle for as long as their software license is valid.

Renault

Renault adopted a similar approach. For its electric cars, it only allowed customers to rent batteries.[62] The company specified in a clearly-worded contract that its customers were merely renting their batteries and could never own them. Since the car would not be able to function without a battery, a customer can never own a fully-functioning car. Renault can collect data from the battery regarding how fast the car is going and when, along with where the battery is charging, details of the journey and more. The company is also able to remote-control battery charging at the end of the rental period. However, if Renault can remotely-control the battery, so can someone else. Renault, by enabling remote access to batteries, could expose its customers to potential hacks and, as a consequence, put its customer's security, including private data, in danger.

Depending on the country, developing an independent diagnostic software for car repair might be considered a

[60] https://motherboard.vice.com/en_us/article/farmers-right-to-repair

[61] https://copyright.gov/1201/2015/comments-032715/class%2021/John_Deere_Class21_1201_2014.pdf

[62] https://blogs.fsfe.org/gerloff/2013/10/31/renault-will-remotely-lock-down-electric-cars/

breach of copyright since reverse engineering would be necessary to create it. Furthering their brand lock-in, vehicle manufacturers usually develop their own diagnostic software that they expect their customers to use.

Users own the vehicle, but the manufacturer owns the software that is used in the vehicle. The issue is that the vehicle is inoperable without the software, which is protected by the manufacturer's copyright. This arrangement further strengthens the notion that every time software (or DRM software) is part of a product, full ownership of the product is impossible. Digital components in cars and motorcycles are responsible for the users' loss of control over repairs and alterations. The software licence agreements imposed on consumers by vehicle manufacturers renders the legal exceptions for private use and repair unusable, which leaves consumers unable to repair their "own" vehicles.

This situation could be partially ameliorated if vehicle manufacturers made it clear to their customers prior to their purchase that they have used certain "security" measures that will make it impossible for them to use the vehicles in certain ways. The clear notice about security features would not improve the user experience per se, but it would allow customers to make a more informed decision about whether they still want to purchase a vehicle with this particular set of "security" measures.

Companies using DRM to control markets

Apple's lock-in strategies

iPhone

Several of the strongest examples of the vendor lock-in come from Apple. Even though it was always possible to install third-party software on Mac computers, the situation was quite different with iPhones. An iPhone software update released in 2007 erased unauthorised software from phones and even rendered some of them inoperative — “bricked”.[63]

Apple holds strong control over ancillary products that can be installed on iPhones. This setup gives it the ability to foster competition as it suits the company, whilst setting up standards for third-party software and accessories. Apple said it wanted to protect carrier networks and to make sure the phone was not damaged.[64] It has used the user security argument to justify the lack of control users can exercise over their phones. Moreover, Apple’s attitude directly stifles innovation by tightly regulating what appears in their market, possibly making it too elusive for some developers and manufacturers to enter the Apple market.

Many of the third-party applications that people installed on their iPhones were not available from an “authorised” app (e.g. a screen-shot capture app). Arguably, Apple could have already then created a system for third-party software providers that would ensure that iPhones do not get damaged if they operate the non-approved app. It is hard to see how user and device security could have been the only driving force behind Apple’s restrictive market setup. Together with the brand lock-in they have achieved on such a massive scale, this would be just a by-product of this

[63] The term “bricked” refers to the phrase of being “as technologically useful as a brick”.

[64] https://web.archive.org/web/20170717160313/http://www.nytimes.com/2007/09/29/technology/29iphone.html

effort.

iTunes

Until 2009, it was not possible for users of iTunes to listen to their legally-purchased music on other devices than those produced by Apple.[65] For six years, between 2003 when iTunes was launched to 2009 when Apple removed the DRM from iTunes, iTunes users could only listen to their music on their Apple device or face losing all of their time, effort and money put into creating their music library.

Even after the DRM technology was removed from iTunes, the technology would not have been removed from all the music purchased before 2009. Supposedly, Apple used DRM for its iTunes software to protect rights-holders and copyright. But it is not clear how providing access to iTunes on non-Apple devices would negatively impact the rights-holders. One thing that is clear is that if Apple did not offer the service on other devices, their users would have to stick with their products, whether they wanted to or not.

Often DRM features go beyond mere copyright protection. There was not a compelling enough reason for Apple to restrict third-party apps on iPhones or wait six years before letting users enjoy their iTunes on other devices not made by Apple.

Apple is probably the most well-known company for building its business model on vendor lock-in. If stronger rules on

[65] https://www.wired.com/2014/03/kill-itunes-drm/

using DRM to brand-lock customers were in place, it is possible that Apple’s revenue could be lower, but its customers could benefit from a wider choice of providers.

Microsoft’s implementation of “security” measures

NGSCB

In the early 2000s, Microsoft began developing the Next-Generation Secure Computing Base (NGSCB)[66], which would give a real-life dimension to Microsoft’s idea of a control-based security system built into the computing hardware. One of the effects of the NGSCB is that it would only allow a computer to boot from an authorised copy of the operation system. The user would be prohibited from using the unauthorised software.

The way Microsoft communicated the news about its new product to the public revolved around NGSCB being a security measure that was there to protect users from Trojans, worms, and malware in general. The company omitted from its message the fact that it would limit what consumers and users be could do with their own computers, and that Microsoft would have control over many of these actions.

Windows Vista

When Microsoft developed Windows Vista, it contained several of “security measures". Microsoft claims it put the measures in to comply with demands of the entertainment

[66] https://technet.microsoft.com/library/cc723472.aspx

industry. The security measures protecting rights-holders would also allow Microsoft to have more control over the entertainment industry since it already dominates 95% of the market.

Vista contained copy protection technology for the then-new media formats such as HD DVD and Blu-ray disks. It also reserved some high-quality audio and video output paths for protected peripheral devices, as well as sometimes even degraded output quality for these devices. Vista used CPU time to constantly monitor itself to be able to assess if the user was doing something they were not allowed to do. In some cases, when the user was trying to perform unauthorised activities, the computer's functionality would be limited, and occasionally it would restart the video subsystem providing output display to the user.[67]

Not only did the DRM mechanisms in Vista take over the control of users' computers, they also made the computers' performance worse and significantly affected user experience. The experience was affected to such an extent that Microsoft decided to discontinue the Vista generation of operating systems.

Sony embeds rootkit software in CDs

The most infamous case of mission creep involved Sony embedding sophisticated rootkit software in its audio CDs. This spyware installed itself in the host computer, becoming impossible to remove, and informed Sony of various activities, while leaving customers' computers vulnerable to

[67] https://www.schneier.com/blog/archives/2007/02/drm_in_windows_1.html

hackers.[68]

It was estimated that around 15 million music CDs were affected. Sony ended up being sued in three separate class actions lawsuits, which ended in Sony settling the cases and giving free download copies to all the affected users[69] on top of withdrawing the DRM software.

Sony, in this case, failed to disclose the full extent of data collection through DRM and also failed to obtain consent from users. Its copyright protection strategy is another example of how DRM can easily be used to exploit users' data and threaten their security while ensuring the rights-holders increases their profits.

[68] https://web.archive.org/web/20170717114354/http://www.pcworld.com/article/125838/article.html
[69] https://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html

Legal position

DRM relies on technology to fight the technological developments — digitisation and the Internet — that facilitate the reproduction and innovative uses and distribution of copyrighted works. Most modern DRM involves scrambling all or part of the content using some form of cryptographic cipher. But this in turn has led to an arms race where technology has struck back, usually with some degree of success, to allow users to bypass DRM.

The answer has been to simply make this illegal. The Copyright Treaty of the World International Property Organisation (WCT) from 1996[70] imposes an obligation on signatory countries to "provide adequate legal protection and effective legal remedies against the circumvention" of DRM and the removal or alteration of DRM without authority. These clauses have been incorporated into the European Copyright (Infosoc) Directive, and thus brought into UK law. In this context "UK" refers to the United Kingdom of Great Britain and Northern Ireland[71], and "Great Britain" refers to England, Wales, and Scotland. In general (but with exceptions for some court procedures in the distinct jurisdictions) the law applies to the whole of the UK.

The US Digital Millennium Copyright Act (DCMA) also incorporates similar clauses, and provisions based on them have been included in the intellectual property chapters of the last 10 bilateral or regional free trade agreements (FTAs) that the US has concluded – as trade-off for market access interests.[72]

[70] http://www.wipo.int/treaties/en/ip/wct/ articles 11 and 12

[71] https://www.legislation.gov.uk/ukpga/1978/30/schedule/1

[72] C. Rossini. "TPMs and access rights". *eff.org*. Available at: https://www.eff.org/files/filenode/eff_presentation_on_tpms_and_civil_rights_sd.pdf

DRM (and intellectual property) protections vary from one country to another and they tend to reflect national development priorities. In this way, DRM technologies can be a way of boosting national industries and protecting local entrepreneurs.[73] This approach is manifested by national governments enacting anti-circumvention laws. Legal regimes supporting measures against bypassing DRM — anti-circumvention — ensure that DRM regimes are effective. Without the anti-circumvention legal regimes, DRM systems would be useless, as they are not capable of effective functioning by themselves.

This section outlines various legislations that regulate DRM mechanisms in the EU, UK and USA.

WIPO treaties

Two World Intellectual Property Organisation (WIPO) treaties have made digital rights management internationally enforceable through national legislations. The "Internet Treaties," the World Copyright Treaty (WCT) and World Performance and Phonogram Treaty (WPPT), both provide for the protection of technological measures and rights management information.

Articles 11 and 12 of the WCT[74] and Articles 18 and 19 of the WPPT[75] require the countries that signed the Treaties to "provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures" and "against any person knowingly performing acts […] that will induce, enable, facilitate or

[73] https://www.eff.org/wp/digital-rights-management-failure-developed-world-danger-developing-world

[74] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295157

[75] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=295477

conceal an infringement of any right covered" by the two treaties. They provide legal protection for "authors" in general and "performers or producers of phonograms" (excluding audiovisual works) respectively.

In 2013 member countries of the WIPO adopted the Marrakesh Treaty, which allows for copyright limitations and exceptions to facilitate the creation of accessible versions of books and other copyrighted works for the visually impaired. Article 7 of the treaty binds the signatories to "ensure that when they provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures, this legal protection does not prevent beneficiary persons from enjoying the limitations and exceptions"[76]. The treaty came into force in 2016 when the EU issued a draft directive[77].

EU legal position on DRM

The obligations created by the WCT and the WPPT were implemented in the European Union through the Directive 2001/29/EC on Copyright in the Information Society.[78] Article 6 of the Directive defines technological measures, establishes a framework for their protection and protection against acts involving the means for promoting, enabling, and facilitating circumvention. It also outlines the relationship between protections and exceptions. The Directive covers copyrighted works that are not a computer program — technological protection of computer programs is covered by the Software Directive 2009/24/EC.

[76] http://www.wipo.int/wipolex/en/treaties/text.jsp?file_id=301016#art4

[77] https://ec.europa.eu/digital-single-market/en/news/proposal-directive-permitted-uses-works-and-other-subject-matter-protected-copyright-and

[78] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001L0029:EN:HTML

Provisions for DRM as set in the Copyright Directive are far reaching. Member states are obliged to provide adequate legal protection against circumvention under Article 6(1) and 6(2). However, the Directive also requires Members States to ensure that rights-holders make the copyrighted material available to the beneficiaries of exceptions and limitations (Article 6(4)).

Nevertheless, the Directive first encourages member states to promote voluntary measures taken by rights-holders (e.g. agreements between rights-holders and users or other third parties) to achieve the objectives of certain exceptions and limitations. If rights-holders fail to deliver the exceptions through voluntary measures within a reasonable period of time, the Directive instructs the member states to take appropriate measures to ensure that citizens can benefit from the exceptions if they already have legal access to a copyrighted work.[79]

The exceptions and limitations include the right to create reproductions for private use, for use by libraries, educational establishments, museums or archives, for scientific research, and for use by people with disabilities. They merely control the way users can make copies of the copyrighted material, but they do not tackle the problems people experience in accessing copyrighted material. The exceptions are limited in their scope and can only be enjoyed by people who already have access to the copyrighted material. This prerequisite excludes all the other potential beneficiaries of the exceptions.

The exceptions to copyright were specifically designed so users would not need to ask for authorisation from the

[79] http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1107&context=dltr

rights-holder to make copies. The DRM provisions in the Directive make this impossible, which means they disproportionately and unnecessarily preclude lawful use of copyrighted material. The DRM systems cannot differentiate between lawful and unlawful uses of the copyrighted works; as such they restrict not just unlawful access to the works but any access not authorised by the rights-holder.

Computer Programs Directive

The Directive on Copyright in the Information Society[80] explicitly mentions an exception for software and allows circumvention of DRM in some cases. These are outlined in detail in the Software Directive 2009/24/EC, which includes exceptions for achieving interoperability (Article 6) and observing, studying or testing the functioning of the program in order to determine principles of the program (Article 5(3)).

The exceptions in practice mean that the person circumventing DRM on a computer program would not be liable to penalties outlined in the Software Directive if they were only removing the DRM to ensure that the computer program can work in conjunction with another program. In the same way, if an assignment given within a learning environment requires circumvention of DRM, neither students or teachers would be liable under the Software Directive.

Article 7 of the Directive also prohibits provision of any tools that could facilitate removal or circumvention of protection

[80] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF

measures placed on a computer program, but it still respects the aforementioned exceptions.

UK legal position

The EU Copyright Directive was implemented in the UK through The Copyright and Related Rights Regulations 2003[81], which amended and complemented the Copyright, Designs and Patents Act 1988[82] (CDPA). The Regulations maintain the same provisions for DRM protections on works other than computer programs but they differ in how they provide exceptions for cryptographic research and reverse engineering.

The UK adopted the approach of preserving the exceptions that were already in the UK copyright law and not implementing any new ones. In 2014, the UK introduced an exception for private copying,[83] but following a backlash from several music industry actors who applied for a judicial review, the private copying exception was quashed.[84] This means that users in the UK are unable to make backup copies of copyrighted materials or copies in different formats to be used on different devices.

The UK's implementation sets out the applicability of the law in relation to the circumvention of technological measures (section 296ZA)[85], including where a person does anything that circumvents those measures "knowing, or with reasonable grounds to know, that he is pursuing that objective". The law also makes it an offence to promote, advertise or market the circumventing service for business

[81] http://www.legislation.gov.uk/uksi/2003/2498/contents/made

[82] http://www.legislation.gov.uk/ukpga/1988/48/contents

[83] http://www.legislation.gov.uk/ukdsi/2014/9780111116036

[84] https://www.gov.uk/government/news/quashing-of-private-copying-exception

[85] http://www.legislation.gov.uk/ukpga/1988/48/section/296ZA

purposes or in any way that would impact on the author's rights (section 296ZB). The non-commercial distribution of circumvention devices for private and domestic purposes is not covered by the legislation.

The UK's CDPA also allows for a defence for a person to demonstrate that they did not know or had no reasonable ground to believe that their products facilitate circumvention of DRM.

The CDPA only offers legal protection for "effective technological measures". These are considered effective if they protect the work through:

"(a) an access control or protection process such as encryption, scrambling or other transformation of the work, or

(b) a copy control mechanism, which achieves the intended protection."

Since the nature of exceptions awarded to users of copyrighted materials only relates to the copy control mechanisms (as discussed above), there is a clear discrepancy within the UK copyright law. The law awards legal protection of technological measures to services providing both access control and copy control, but it merely awards exceptions to regular users to circumvent measures that include copy control mechanisms, leaving access control mechanisms unsusceptible to copyright exceptions.

The CDPA makes sure (section 296ZF(2)) that the provisions covering protection of DRM only apply to those access and copy control technologies that are used to prevent acts unrelated to computer programs.

Section 296ZE(2) of the CDPA states that in cases where the application of DRM measures to a copyrighted work (but not a computer program) prevents a user from carrying out a permitted act then the user can issue a notice of complaint to the Secretary of State. Acting on the complaint, the Patent Office can open an investigation. If the investigation shows that the rights-holder did not put in place a voluntary measure to accommodate exceptions to copyright, the Secretary of State may direct the rights-holder to ensure that the complainant can benefit from the permitted act.

However, users can only raise the complaint with the Secretary of State if they already have access to the copyrighted work.

Legal protection of software copyright

In line with the EU legislation, the UK also implemented the Software Directive 91/250/EEC (later amended to the Software Directive 2009/24/EC) to govern circumvention of DRM on computer programs. The CDPA was amended to include the provisions from the Directive as well as, as with the EU Copyright Directive, referencing the exceptions for cryptographic research and reverse engineering when circumventing DRM measures.

The CDPA specifically allows legal owners of computer programs to create copies of them for the purposes of making backup copies (section 50A), decompiling them to secure interoperability with another program (section 50B), to observe, study or test computer programs in order to determine the ideas and principles that underlie any element of the program (section 50BA) or to adapt it to correct errors[86] (section 50C).

As such, the CDPA contains a specific exception for reverse engineering and circumventing of technological measures in computer programs.

US legal position

In the US, DRM is protected by provisions within the Millennium Digital Copyright Act (DMCA) of 1998[87] in Section 1201.

The DMCA distinguishes between technological measures that control access to a copyrighted work and measures of usage control — protecting rights of the copyright owner. The law also makes a distinct difference between the actual circumvention of technological measures and preparatory activities (production and distribution of tools that can be used for circumvention).

Section 1201(a)(1)(A) forbids circumvention of technical measures that control access to a copyrighted work.

Distribution and manufacturing of technologies primarily designed for circumvention of access controls is forbidden as outlined in the Section 1201(a)(2). This provision is further expanded on in Section 1201(b)(1), which prohibits other technologies facilitating circumvention.

The DMCA allows circumvention of technological measures in certain instances:

1. For the sole purpose of identifying and analysing

[86] http://www.legislation.gov.uk/ukpga/1988/48/part/I/chapter/III/crossheading/computer-programs-lawful-users

[87] https://www.copyright.gov/title17/title17.pdf

elements of a computer program in order to achieve interoperability with other programs
2. For reverse engineering
3. For encryption research
4. To assess product interoperability
5. To test computer systems
6. To test the security of a computer, computer system or network
7. To detect and disable technology collecting and disseminating personal information about online subscribers without authorisation

Non-profit libraries, archival and educational institutions are permitted to circumvent access control measures for the purpose of making a good faith determination as to whether they wish to obtain authorised access to the copyrighted work. The measures prohibiting circumvention of DRM do not apply to law enforcement or intelligence services.

However, the statutory exceptions users could enjoy are drawn very narrowly and do not recognise several other legitimate application of circumvention measures (e.g. research about non-cryptographic watermarking or computer virus and worm analysis).[88]

Under the DMCA, circumvention of technological measures and preparatory activities are prohibited with regard to access control. As mentioned above, the EU law (and by extension the UK copyright law too) prohibits circumvention of technological measures in regards to both accessing the copyrighted work and also making subsequent copies of the work. In the US, the rights-holder is only protected by the circumvention provisions in regards to users gaining access

[88] http://people.ischool.berkeley.edu/~pam/papers/Samuelson.pdf

to the copyrighted work. Copy control is not covered by the circumvention provisions in the DMCA since the users would be able to use fair-use defence.

This means that users would need to by-pass the technological protection measure (DRM) and use the fair use exception as a defence if sued. The EU and UK deals with this differently: it requires the rights-holder or DRM provider to make provisions for legitimates users to access the work without the need to by-pass the law illegally.[89]

The law explicitly states that it does not affect any of the rights, remedies, limitations, or defences for copyright infringement, including fair use. However, the fact that every time a user makes a copy of a protected work they risk being sued despite their actions falling within the remit of fair use would suggest otherwise.

Software protection under DMCA

Computer programs are protected as "literary works"[90] under Section102 (a)(1) of the DMCA. As such, DRM protections placed on software would be protected in the same way as other works that qualify for copyright protection under Section 102 are protected.

The owners of copyright to computer programs acquire the exclusive rights to: (a) reproduce the software; (b) prepare derivative works based upon the original software; (c) distribute the software; (d) publicly perform; and (e) publicly display the software. Rights-holders of computer programs

[89] https://www.inbrief.co.uk/intellectual-property/copyright-technological-protection-measures/

[90] According to Section 102(a)(1), Literary works are "works" other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phono-records, film, tapes, disks, or cards, in which they are embodied.

can limit the ways users make copies of their software through DRM; the limitations are subject to exceptions.

The exceptions to circumvention of DRM applied to software do not differ from exceptions placed on other works protected by technological measures. As mentioned above, this includes circumvention exceptions for achieving interoperability, reverse engineering, research into cryptography, assessment of product interoperability, computer system testing or the security of computer, system and network.

However, due to Section 1201 of the DMCA prohibiting manufacturing and distribution of circumvention tools, if users want to take advantage of any of the exceptions they would need to know themselves how to circumvent technological measures. This makes the use of the exception for the general public redundant.

Moreover, provisions of Section 1201 of the DMCA have been repeatedly used in legal cases where the copyright holder was trying to silence publishing of research papers describing cryptography used behind DRM. Since the circumvention exceptions are drawn very narrowly in the DMCA, they leave a lot of wiggle room for copyright holders to argue their case and threaten the potential users of exceptions.[91] The DMCA directly impacts on innovation and competition since several pieces of crucial research have been pulled due to fears of prosecution under Section 1201.

[91] The Section 1201 of the DMCA was used in Felten v. RIAA (https://www.eff.org/node/68101). Professor Neils Ferguson refused to publish his research into cryptography due to fears of being prosecuted under the DMCA (http://www.macfergus.com/niels/dmca/cia.html).
The Institute of Electrical and Electronics Engineers instituted a policy requiring all the authors in their journal to indemnify IEEE for any liabilities that might be incurred under the DMCA (http://www.eff.org/IP/DMCA/20020503_dmca_consequences.html).

Different approach to DRM in the UK and the US

Copyright operates in distinctly different environments in the UK and the US. The legal protection of technological measures significantly differs in these areas:

- Access control v. copy control
- Application of exceptions
- Intent to infringe
- Protection of software

The UK law applies to both access controls and copy controls placed on copyrighted works, whereas in the US, the law only addresses the protection of access controls. In practice this means that the UK law prohibits circumvention of protection measures that regulate access to the protected work, but also those measures that regulate making copies of protected materials. The US law does not regulate circumvention of measures restricting the act of copying because of the fair use exception. The fair use exception makes it possible for users to defend themselves in front of the court as to why they made copies of their legally-obtained copyrighted work by removing DRM.

As explained in the section above, the US law contains different exceptions to circumvention of DRM than the UK law. The US law explicitly provides exceptions, under certain circumstances, for nonprofit libraries, archives or educational institutions, and for purposes of encryption research, security testing, reverse engineering, interoperability etc. Unlike the UK law, the US DMCA does not specify permissions for circumvention to make temporary copies, copies for private use, or to allow access to people with disabilities. Exemptions of this type in the US would be covered by the “fair use” policy. This means that people who would fall within the permitted use causes in the UK would be liable for circumvention of DRM in the US but, if they were ever to be prosecuted, they would be able to claim fair use defence. Neither of these policies effectively allows circumvention in instances that should be permitted: the US legislation preemptively criminalises any circumvention instances and the UK has failed to put the exceptions into practical arrangements.

The scope of the circumvention offence varies in the two countries. The UK law specifies that the person circumventing technological measures must know or have reasonable grounds to know that they are pursuing the objective. The DMCA does not include this requirement. The circumventor does not need to have any knowledge of violating the law to be liable to charges for circumventing DRM. Circumvention of technological measures under DMCA is a strict liability offence.

The UK law contains separate provisions for protecting DRM used on software and enjoys separate exceptions to other works covered by copyright. The US law considers software a “literary work” and therefore uses the same protections as any other copyrighted work that falls within that definition.

Both legislations allow for exceptions for circumvention of protection measures for purposes of research into cryptography and reverse engineering. However, since the US law includes software among other copyrighted works to which the narrow exceptions apply, the UK protection of DRM in software is slightly more user-friendly than its US counterpart. Also, the UK law singles out copyright protection of computer programs, which means that the access control and copy control protections that apply to all other copyrighted works do not apply to computer programs; as a consequence only access controls are protected when it comes to software.

Summary

DRM provisions in all, EU, UK and US legal systems create and grant rights-holders an unprecedented "access right" over their works that does not exist in any international treaties governing copyright. Circumvention activities are hence outlawed without any link to the corresponding copyright infringement and without taking into account any exclusive right granted by copyright.

Moreover, the UK regulation expects companies to voluntarily provide the right of access to users, while companies predominantly ignore the voluntary arrangements. The right of access should be coined in national legislations instead of being a voluntary practice. This would help avoid any irregularities in access to copyrighted material.

What to do with DRM

In conclusion, Open Rights Group believes that, ideally, DRM should be abolished. However, if it is not, DRM technology should undergo significant reforms to stop harming consumers. Specifically:

- Consumers should be able to consent to the limitations imposed by DRM;
- DRM should not be used to allow consumers access to copyrighted works at the expense of their privacy;
- DRM should not be used to create extra restrictions that expand copyright's basic protections of copying and making available, including determining when and how information is consumed;
- DRM should not unduly restrict the resale or legitimate lending of digital works, making digital copyright much more restrictive than copyright that applies to physical goods;
- DRM should not impact on human rights and freedom of expression by preventing people with disabilities from legally creating copies of copyrighted works;
- Anti-circumvention laws should be reformed to stop the harm to the development of free and open source technologies;
- Criminal sanctions should be removed for those bypassing DRM for lawful purposes;
- Specific protections for cryptographic research into DRM technologies should be expanded to other research.

Abolition

Open Rights Group believes that DRM is fundamentally anti-consumer and presents the wrong approach to solve the challenges introduced by digitisation and the Internet, bringing more benefits for technological intermediaries than for creators themselves. However, it is hard to see how DRM can be completely abolished.

It is very important to distinguish between *technical protection* and *rights information* management. The latter component — if properly implemented — could be useful both for creators and consumers. For example, it would be an important part of any registration system for enhanced protections.

Technical protections are a lot more harmful, as Open Rights Group outlines above, but a complete legal ban on using technology to enforce licensing restrictions would be as pointless as the current complete ban on bypassing them. In some cases, such as subscription streaming services like Netflix or Spotify, it would be hard to see what alternative there would be but to encrypt the music.

Fundamental reforms

This does not mean that DRM does not need fundamental reforms to avoid harming consumers, both by enabling artificial restrictions on the use of media not provided under copyright law; and through distortions to markets.

Consumers need certainty that once they have obtained access to a creative work, they will not be subjected to further controls from rights-holders, or even deletion of the work — for example, if they want to play it on other devices. Interference with equipment that goes beyond what is strictly necessary to enforce basic access is completely unwarranted.

The preferred method for accessing restricted online content should be a simple credential-based access control with encryption on the server side, rather than installing blackbox client software on the user's device that restricts its capabilities and may allow unaccountable spying.

One critical aspects here is consent and transparency. Many consumers are not aware of the limitations imposed by DRM, raising issues of fairness, so there is a need for more transparency.[92] In addition, there are privacy issues with the growing collection of information on usage and other user profiling associated with DRM, which should never be a requirement for access.

Open Rights Group draws a red line at DRM hampering the limitations and exceptions on copyright. Libraries, disabled users and others who are lawfully authorised — or even mandated — to copy, modify or transmit properly-obtained works should never be stopped by DRM. In such instances, DRM can impact on fundamental human rights, including freedom of expression.[93]

EU law[94] provides some protections for limitations as well as exceptions from technical measures, but these are vague and only apply to a limited number of exceptions.[95] In addition, these protections do not extend to "online on-demand services" regulated by contracts, which currently form the bulk of digital media consumption. This introduces some very serious implications and needs to be addressed:

[92] P. Samuelson and J. Schultz, 2007. "Regulating Digital Rights Management Technologies: Should Copyright Owners Have to Give Notice about DRMS Restrictions. *… of Telecommunications and …*."

[93] http://www.ip-watch.org/2009/05/25/freedom-of-expression-versus-drm-the-first-empirical-assessment/

[94] Copyright Directive 2001 Article 6.4

[95] Mazziotti, G., 2008. *EU Digital Copyright Law and the End-User*, Springer Science & Business Media.

all exceptions, including parody, must be covered and the scope extended to all media.

The prevalence of DRM should not make us forget that there are successful businesses operating without DRM. The publisher Verso sells DRM-free ebooks[96] without any apparent downsides, while the popular games platform Good Old Games maintains a DRM-free stance.[97]

Additional reforms of anti-circumvention laws

UK copyright law[98] allows for complaints to the Secretary of State, who can issue a special licence in cases where excessive DRM "prevent[s] a person from carrying out a permitted act." This procedure is too cumbersome.

Restricting the applicability of DRM is important, but reforms are also needed around circumvention of technical measures. The absolute prohibition on circumvention creates a range of problems for people who are not committing any fundamental infringement, with the tail of DRM wagging the dog of copyright.

Open Rights Group believes that criminal sanctions should be removed for those bypassing DRM for lawful purposes, such as activities permitted by copyright, enforcing exceptions and limitations, providing interoperability, etc.

Anti-circumvention provisions are particularly harmful to the development of free and open source technologies, as we demonstrated in our response to the consultation on introducing DRM on BBC broadcasts.[99] They also present a

[96] https://www.versobooks.com/pg/verso-ebooks
[97] https://www.gog.com/?
[98] Copyright Act
[99] https://www.openrightsgroup.org/ourwork/reports/bbc-drm-sub

risk to security researchers, who are prevented from disclosing their findings, and, in the US, have even been imprisoned.

UK and EU law provide some protection for reverse-engineering software programmes for interoperability purposes, but these should also cover processing media files. The UK has specific protections for cryptographic research and these should be expanded to other research and mandated in EU law.