

Re: Opening the Set-Top Box Market

(Response to FCC NPRM: “Expanding Consumers' Video Navigation Choices”, MB Docket No. 16-42; “Commercial Availability of Navigation Devices”, CS Docket No. 97-80)

Benjamin Kreuter

03/19/16

1 Introduction

Unlocking set-top boxes is a noble and worthy goal that the FCC should pursue, and the development of a robust market for cable receiver equipment and software would, without question, benefit American consumers. Unfortunately the FCC's recently proposed rules are unlikely to achieve such a goal, due to the inclusion of DRM requirements, which stand in direct opposition to the goal of opening the set-top box market. These requirements are not merely counter-productive; as discussed below, they would have a negative effect on consumer rights, and are likely to be widely abused by cable companies and the media companies they contract with. In many ways DRM represents an attempt to evade the very copyright laws it supposedly enforces: DRM curtails both fair use rights and the public domain, both fundamental and well-established aspects of copyright.

1.1 Background on DRM

Personal computers connected to the Internet present a unique challenge to copyright law. Prior to the Internet age, members of the general public did not have access to the equipment needed to make copies on a mass scale. If individuals did make copies for their own personal use, such activity would almost certainly have been protected by the fair use doctrine; indeed, this is what the Supreme Court found in the famous *Sony v. Universal* case.

In the Internet age, however, the general public has all the equipment needed to copy books, music, movies, and software in their homes, even in their pockets. What once required specialized industrial equipment now requires common household goods. Copyright-intensive industries, especially the music and movie industries, have struggled for years to prevent individuals from violating copyright en masse. This struggle has entailed both litigation and technical measures, with the latter commonly referred to as “digital rights management” or DRM.

In some sense DRM predated the widespread availability of the Internet. Two early DRM systems were entirely analog – HBO's scrambling of its satellite transmissions, which prevented unauthorized reception of HBO programming, and the Macrovision system, which exploited commonly used circuitry in VCRs to thwart copying efforts. Analog copy-restriction techniques were widely used by cable TV companies prior to widespread digital service to enforce payment requirements, especially for pay-per-view channels. Whether these technology properly qualify as *digital* rights management is debatable, but they shared a common purpose: to restrict copying and unauthorized access to electronic

media.

DRM, even in its early, analog forms, has long been controversial. HBO's use of scrambling attracted the ire of many Americans living in rural areas had purchased satellite receiver equipment and enjoyed watching HBO's broadcasts and ultimately received attention from the Senate [1]. HBO's scrambling system was not originally meant to penalize such low-level activities; rather, it was meant to penalize large-scale activities by hotels and other such businesses, whose public displays of HBO's broadcasts clearly ran afoul of copyright law [2]. A common theme among DRM technologies is collateral damage – common and legal activities are restricted or hindered by technical efforts to prevent copyright infringement. Even proponents of extensive DRM have admitted to the various problems DRM creates for consumers, which in many ways encourages consumers to seek media from unencumbered sources, both legal and illegal [3].

Another source of controversy is the inherently permission-oriented nature of DRM. For reasons explained below, DRM cannot work if it is possible to create playback equipment or software without some licensing or permission requirement. As a result, DRM precludes open-source software, even as open-source software has become the backbone of the Internet and the Web. The effort by the W3C to include DRM in a web standard has been met with fierce resistance by many open source software developers and users, as it represents a departure from the inherently open nature of the Web [4].

For reasons explained below, DRM has been largely ineffective, despite receiving strong legal protections. Even DRM system that has been analyzed by the computer security or hacker communities has been defeated. That the law forbids the dissemination of circumvention technologies or information on how to circumvent a DRM system, DRM-circumvention tools are widely available on the Internet. For the same reason copyright infringement has been difficult to prevent in the Internet age, the spread of DRM-circumvention technologies has been difficult to stop. DRM-circumventing tools can typically be downloaded as software; no industrial equipment is needed to disseminate copies of software via the Internet.

2 The Ineffectiveness of DRM

DRM has had only the most limited success; at best, it serves only to slow down copyright infringement, and rarely does DRM stop those who are determined to circumvent it. This is not simply coincidence, nor is it due to a lack of technical expertise by the purveyors of DRM systems. The failure of DRM is fundamental: DRM is an attempt to do not just the impossible, but the nonsensical.

Creating electronic media that cannot be copied is as nonsensical as creating water that is not wet; no technology could possibly accomplish such an inherently contradictory goal. The very nature of electronic media makes copying easy. Indeed, the very reason that media companies have come to rely on electronic media for their entire business model is the efficiency with which authorized copies can be made. Digital technologies have made copying even more efficient and has enabled the creation of perfect copies, and copyright intensive industries have largely switched to digital systems for those very reasons.

The normal course of operations for a computer involves making numerous copies of programs and data. Even if it were possible to achieve the goal of DRM, doing so would be incompatible with the broader goal of selling digital media to consumers. Indeed, DRM systems in practice do not truly attempt to prevent copying, but rather to *restrict* copying, though for all the reasons noted above, such a goal is inherently contradictory and cannot be achieved in general. The best any DRM system can hope to become is a temporary annoyance for those wishing to make copies, and eventually any DRM system can be expected to be permanently broken.

2.1 Smart Cow Problem

That DRM is *inherently* ineffective can be understood in terms of the “smart cow problem.” Only one cow in a herd of cattle needs to open the latch to release the entire herd from its pen; in other words, the latch must be absolutely effective to be effective at all. DRM suffers from a similar problem, in that the techniques used by even one hacker to break a DRM system can be rapidly disseminated over the Internet in the form of software, allowing anyone, even those with no hacking skills at all, to break the system. Furthermore, even if the hacker’s techniques cannot be encoded in software – for example, techniques requiring access to hardware – once digital media has been copied outside the boundaries of DRM, it can be copied without restriction. In other words, for a DRM system to be secure, it must be perfectly secure.

Experience has shown, however, that no system is perfectly secure, especially as the complexity of the system grows. Indeed, despite the widespread deployment of DRM and despite the fact that laws in various nations prohibit spreading DRM circumvention techniques, DRM presents little more than an annoyance to anyone intent on violating copyrights.

2.2 The Analog Hole

Even if it were possible to create a perfectly secure DRM system, it would still be ineffective at preventing copyright infringement. The reason lies with the greater context in which DRM is deployed. To be useful a DRM system must allow certain uses of the media it restricts. In the case of a cable receiver, it is necessary to allow consumers to watch television programs at least once. Nothing could prevent a consumer from pointing a camera at their television and recording a program as it is displayed; this fundamental weakness is known as the “analog hole.” At a minimum it will always be possible to produce lower-quality copies by such means; however, it is entirely possible that sophisticated techniques involving several cameras and software post-processing could allow high-quality copies to be made.

3 The Abuse of DRM

While DRM has been ineffective at preventing copyright infringement, it has been exploited for unrelated purposes. Egregious examples include the use of DRM to prevent the use of third-party printer cartridges, which has allowed printer companies to greatly inflate the price of ink; the use of

DRM to prevent independent mechanics from services computerized car parts, allowing auto companies to demand payment from licensed mechanics; and various other efforts to artificially reduce the usefulness of tools. Many consumers have complained about the inability to skip commercials on the DVDs they purchased; part of the DRM standard for DVDs is the ability to mark tracks as unskippable, a feature intended to be used for the copyright warning track but which has been widely abused by media companies.

It should come as no surprise that DRM is widely abused. The very nature of DRM makes it open to abuse: DRM must, as part of its operation, deny users and device owners full control over their devices. Device vendors and media companies receive, via DRM, control over their customers' property, with very few consequences for misuse or abuse of that control.

Indeed, rather than preventing unauthorized copying, DRM has become a tool for shaping the consumer electronics market [5]. DRM licensing regimes and lawsuits have been used to kill off whole classes of consumer electronics and software [6]. As a result, American consumers have been left with higher prices, less choice, less innovation, and a less competitive market.

4 Consumer Rights

DRM does not simply fail to protect copyright, but actively undermines copyright law; author Cory Doctorow has described DRM as a way to “make up your own copyright laws” [7]. Copyrights are not simply a hand-out to authors and media companies. Copyrights, as envisioned by the constitution, are a compromise meant to benefit society as a whole¹. Authors do receive a monopoly over their work, but that monopoly must, by law, expire, after which the work enters the “public domain” and may be freely copied. Authors do not receive unlimited control over the dissemination of their works, but control that is limited by, among other things, the fair-use doctrine and the first-sale doctrine, which have been well-established by courts. These various limits on copyright are fundamental consumer rights that ensure copyright benefits society as a whole.

Unfortunately the FCC's proposal thoroughly disregards consumer rights. By requiring cable receivers to respect “entitlement” information, the FCC's proposal places consumer rights in the hands of cable service providers. In the proposal the FCC even uses the revocation of a well-established right, the right to record programs for personal use, as an example of how entitlement information might be used.

Yet consumer rights are not granted by cable service providers or media companies, but by the law itself. There is no question that under the law consumers have the right to record television programs without, or even in opposition to, the wishes of copyright holders. This right is widely exercised by the American public, with both VCRs and DVRs being used by many millions of people. Despite decades of pressure by media companies, Congress has not revoked that right; it is unconscionable for the FCC to attempt to do so via regulation. The disregard for fair use rights and the public domain demonstrated in the proposed rules is deeply disturbing. Copyright exists for the benefit of society as a whole, not

¹ Article I, Section 8, Clause 8, “To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries.” The framers were unambiguous about copyright's purpose of benefiting society as a whole, and that copyrights are a limited right.

just for media companies, and any new rules should balance consumer rights with the interests of copyright holders.

4.1 Device Ownership

DRM raises troubling questions about who actually owns consumer electronics, particularly in cases where DRM allows third parties to disable various device functions at their convenience – exactly the sort of DRM the FCC proposes to standardize with its regulation. Such systems undermine the commonly accepted notion of *ownership*, which implies *exclusive* control over one's property.

The DRM on Amazon's Kindle e-book provides an infamous example of how ownership is called into question. In 2009, in response to a dispute over copyrights, Amazon deleted, without notice or consent, copies of *Nineteen Eighty Four* and *Animal Farm* that Kindle users had purchased, and refunded their money [8]. This challenged preexisting notions of ownership in two ways: first, it suggested that sales of e-books are not, in fact, final, and that the seller could rollback the transaction at will, something which would be unthinkable for physical products; second, Amazon had built into Kindle devices a form of back-door access, giving them control over their customers' Kindles long after the devices were sold.

5 Openness

One of the goals of the proposed rules is to give consumers greater choice in cable receiver equipment, including the possibility of software-only receivers. There is no question that this goal would benefit society in general. As the NPRM notes, to achieve this goal, it must be possible to create a cable receiver without having to seek the permission of each specific cable company, nor of cable companies in general. In other words, openness is critical to the creation of a market.

Unfortunately openness is fundamentally incompatible with DRM. It would be trivial to defeat any DRM system if receiver equipment could be created by anyone without any licensing or permissions required. The FCC clearly recognizes this fact in the proposal, and proposes a system of licensing that is antithetical to the goal of an open market.

5.1 HDCP

One effort to support a DRM system in an open market serves as an example of the problem. The High-bandwidth DigitalContent Protection system (HDCP) is an attempt to reduce the scope of the analog hole (see subsection 2.2 above) by encrypting video signals on the cables that connect consumer electronics. The general market for consumer electronics is highly competitive and consumers have many choices of display devices, media players, and related electronics.

Despite the non-discriminatory licensing process for HDCP, it has been a spectacular failure. Security researchers discovered flaws in the cryptography that forms the foundation of the system, which can be exploited at low cost, and which may have already been exploited by hackers [9]. The master secret key has been leaked, allowing the entire system to be circumvented even without exploiting the

cryptographic weaknesses and undermining the revocation process [10][11]. HDCP was designed to support revocation of leaked keys, but attempts to do so have resulted in headaches for consumers, as older electronics have been rendered unusable due to their use of the revoked keys. For cable companies this has been a particular problem, as they must provide working receiver equipment to their customers, even when those customers have older television sets. Consumer rights groups have complained of HDCP creating a form of planned obsolescence, forcing consumers to replace perfectly functional electronics; Professor Edward Felten described HDCP as, “less a security system than a tool for shaping the consumer electronics market.” [5]

5.2 DRM in HTML5

In the NPRM the FCC notes that HTML5 includes some support for DRM, which comes in the form of the “Encrypted Media Extensions” technical standard. EME, however, has been highly controversial, with many developers and members of web standards groups speaking out against it on both technical and moral grounds. The controversy is due to the departure EME makes from the free and open web that has been enjoyed by Internet users since its inception.

Prior to EME, implementing a fully-functional web browser that could display any web page that any other web browser could display was a matter of technical prowess. In other words, anyone with the necessary programming skill could read the relevant technical documents and create a functioning implementation of web standards without having to ask permission, and a user could freely choose among implementations of web standards². In the strictest sense EME does not break with tradition, as anyone can technically implement the standard; unfortunately, just implementing the standard is not actually sufficient to play media restricted by EME. As a standard EME specifies only how a browser should interact with an implementation of DRM, but no DRM system is standardized. So to produce a functional implementation a programmer must have a license for at least one DRM system.

6 Enforcement of Regulatory Requirements

The NPRM indicates that the FCC intends to require, by the same licensing regime used to enforce DRM, certain legally-mandated functionality in cable receivers. In particular the FCC wishes to enforce compliance with the emergency alert system, certain limits on advertising, and consumer privacy requirements.

This represents the same kind of abuse described above in section 3, and undermines the goal of developing a robust market for cable receiver devices, software, and services. It makes little sense to mandate emergency alert system requirements for software-only implementations, which could decouple a person's location from the TV programs they enjoy (e.g. by using the Internet to connect to cable services from a remote location; note that even if a cable company does not make its services available on the public Internet, such remote access would possible using extant software). The

² This principle ignores legal constraints, such as standards specifying patented algorithms, and deals primarily with technical requirements. The Internet community generally prefers standards that are not legally burdensome to implement, although standards requiring patented technology are not strictly forbidden; see RFC 1958, Section 5 [12].

receiver devices/software are the wrong place to enforce privacy requirements and advertising regulations, and it strains logic for the FCC to attempt to impose such requirements on receiver manufacturers / providers.

7 Suggestions

7.1 Require Open Technical Specifications

The most important thing the FCC should do in its new rules is to require that MVPDs make the technical specifications needed to build a complete and fully-functional receiver for their system available upon request to anyone, without requiring any payments or unnecessarily burdensome delays, and without requiring any licensing. Modern technology makes this possible, and the Internet itself provides a model: all Internet standards are available on the IETF's website, allowing anyone to completely implement any Internet protocol. The simplest way cable services could meet such a requirement would be to put such specifications on their website.

Such an approach would ensure that cable services remain free to experiment and innovate with their own video distribution systems, at all levels, from the encoding of videos all the way up to the APIs used for on-demand and other interactive services. It would ensure that cable services are able to differentiate themselves from competitors with more than just TV channels. On the other hand, it would ensure that third parties could create fully-functional receiver equipment, including interactive functions, without interference.

This approach is necessarily incompatible with DRM, as it requires cable services to allow *anyone* to build a fully-functional receiver. As discussed above, this is unlikely to have any meaningful impact on copyright infringement, because DRM does not effectively prevent copying. The purpose of this approach is to end the practice of “shaping” the consumer electronics market by using DRM and licensing requirements to block entire classes of innovation. It is hard to imagine how anything less would serve the purpose of “unleashing” the set-top box market.

7.2 Identifying Copyright Infringers

Unlike trademarks, copyrights do not require any particular effort on the part of copyright holders to remain valid. Even if media is distributed without DRM it would remain illegal to share unauthorized copies, unless fair use exceptions apply. Rather than encourage ineffective DRM systems that threaten consumer rights, the FCC could encourage systems that improve *accountability*, so that consumers who do violate copyrights can be identified and appropriately penalized.

Technical measures for identifying the source of unauthorized copies of movies are already used by the MPAA, to deal with the problem of movie theater employees using video recording devices to produce unauthorized copies of movies [13]. Similar “digital watermarking” technologies are reportedly used to identify infringers of 4K ultra-high-definition video [14]. Watermarking technology has already proved itself and is available from a variety of sources, and unlike copy-restriction systems,

watermarks impose no particular requirements on playback devices or software.

7.3 No Entitlement Data

Currently, what consumers are *entitled* to do is determined by Congress, the Courts, and the limits of available technology. This has served consumers, cable services, and entertainment companies well for decades, and there is no reason to believe it would not continue to benefit all Americans in the future. Under the status quo, consumers have enjoyed innovations such as the VCR – which has ultimately benefited cable companies and the entertainment industry, allowing them to reach consumers even in the middle of the night, and resulting in the rise of a very profitable market for recorded videos.

By mandating respect for entitlement data, the FCC is attempting to shoehorn future innovations into today's concept of how consumers enjoy video. Yet it is impossible for anyone to know what sort of new ideas will emerge. The only way for a set-top box market to be innovative is to give inventors room to try out new ideas, including ideas that do not align with the entitlement information conceived of by cable services or the entertainment industry. Entitlement data would place certain ideas about how consumers can enjoy cable programs in an off-limits category; it would stand in opposition to the very purpose of opening the set-top box market.

7.4 Optional Emergency Alerts

The emergency alert system has the potential to help Americans, but technology has advanced significantly since the EAS was first introduced. Mandating compliance with the EAS no longer makes sense; consumers may not be watching videos at the same time as an EAS broadcast, and with the rise of the Internet and mobile computing, they might not even be in the same geographic location. The EAS mandate should be reevaluated, to ensure that it is not chilling innovation or putting cable receivers and services at a disadvantage to Internet streaming services.

One approach would be to make EAS an open standard, and to require the cable services use that standard when broadcasting emergency messages. Makers of receiver equipment or software should be given the option, but not the obligation, to receive and display alerts. This would be valuable for software implementations especially – it may be the case that EAS is handled better by e.g. the operating system than by video playback software.

7.5 Privacy Requirements and Advertising Limits

As with DRM and the EAS, cable receiver equipment or software is the wrong place to enforce privacy requirements and regulations on advertising. Compliance with such requirements is the responsibility of service providers: cable services, and third parties providing services associated with cable receivers or software. There is no need to use a licensing regime, because there is nothing that needs to be licensed.

The FCC should bear in mind that modern technology allows for whole new approaches to privacy protection and protection against inappropriate advertisements. Various technologies are being used for

these purposes on the Internet and especially the Web. This is possible because consumers own and fully control their computers.

8 Conclusion

An effective market can only exist when its participants are able to try new ideas without having to seek permission from well-established players. It is clear that the set-top box market as of this writing is not effective and that there has been a dearth of new ideas. The various innovations consumers enjoy with Internet video services simply do not exist for cable TV.

The FCC is right to try to address this problem, but the proposed rules have major shortcomings and fail both to respect consumer rights and to encourage a robust and innovative ecosystem. The biggest problem in the proposed rules is the DRM mandate, which will almost certainly not serve its intended purpose but will instead be used to deny consumers their rights. In general, the proposed rules assume that a system of permissions and licensing is compatible with the goal of opening a competitive market that encourages innovation. That assumption is simply false.

An opportunity exists for the FCC to adopt a new and better approach. By relaxing various regulatory requirements, by scrapping the DRM mandate, and by extending to consumer rights the same respect given to copyrights, the FCC can achieve its goals. Technology has changed, and the new challenges and opportunities that come with those changes require new approaches to regulation. It is my hope that the FCC will embrace the reality of new technology and help to usher in a future of innovation for all Americans.

Bibliography

- [1] PETER W. KAPLAN, ISSUE AND DEBATE; SCRAMBLING TV SIGNALS FROM SPACE, New York Times, 1985
- [2] Orlando Sentinel, Satellite Dish Sales Scrambled By Hbo, Chicago Tribune, 1986
- [3] The Economist, Science Fiction?, 2005, <http://www.economist.com/node/4342418>
- [4] Lucian Constantin, Proposed encrypted media support in HTML5 sparks DRM debate on W3C mailing list, 2012, <http://www.itworld.com/article/2729888/enterprise-software/proposed-encrypted-media-support-in-html5-sparks-drm-debate-on-w3c-mailing-list.html>
- [5] Edward Felten, Understanding the HDCP Master Key Leak, 2010, <http://www.freedom-to-tinker.com/blog/felten/understanding-hdcp-master-key-leak>
- [6] Fred von Lohmann and Wendy Seltzer, Death by DMCA, IEEE, 2006
- [7] Mike Masnick, DRM Is The Right To Make Up Your Own Copyright Laws, 2014, <https://www.techdirt.com/articles/20140206/10323526118/drm-is-right-to-make-up-your-own-copyright-laws.shtml>
- [8] Brad Stone, Amazon Erases Orwell Books From Kindle , The New York Times, 2009
- [9] Scott Crosby, Ian Goldberg, Robert Johnson, Dawn Song, David Wagner , A Cryptanalysis of the High-bandwidth Digital Content Protection System, Springer Berlin Heidelberg, 2002
- [10] Richard Lawler, HDCP 'master key' supposedly released, unlocks HDTV copy protection permanently, 2010, <http://www.engadget.com/2010/09/14/hdcp-master-key-supposedly-released-unlocks-hdtv-copy-protect/>
- [11] Peter Bright, Intel confirms HDCP key is real, can now be broken at will, 2010,

<http://arstechnica.com/tech-policy/2010/09/intel-confirms-the-hdcp-key-is-real-can-now-be-broken-at-will/>

[12] Network Working Group, RFC 1958: Architectural Principles of the Internet, 1996

[13] Xeni Jardin, An Eye on Movie Theater Pirates, Wired Magazine, 2004

[14] The Register, Hollywood: How do we secure high-def 4K content? Easy. Just BRAND the pirates, 2013,

http://www.theregister.co.uk/2013/10/07/security_for_4k_to_be_toughest_hurdle_to_climb_in_digital_video/