



Critique of "NAVSHP (FP6) DRM Requirements Report."

Cory Doctorow, European Affairs Coordinator, Electronic Frontier Foundation
cory@eff.org

Introduction

On September 13, 2005, the EU's "Networked Audiovisual Systems and Home Platforms" group released a paper called "NAVSHP (FP6) DRM Requirements Report." This is a set of technical and commercial requirements for developing a harmonized system for restricting public access to creative works, intended for use across Europe. The restriction technologies discussed in the paper (sometimes called "Digital Rights Management" or DRM) are already widely deployed in the field today, and have failed totally to reduce copyright infringement or to enrich creators. Indeed, the most striking effect these systems have had to date is to reduce competition, retard innovation, and misappropriate user-rights to the benefit of American-based entertainment giants.

The NAVSHP group had the opportunity to consider DRM in light of this real-world disaster, and formulate requirements that would be likely to produce better outcomes. The report does have a lot of high-minded material about protecting the public interest, but the requirements themselves neuter all of these principles.

Indeed, when read closely, the requirements themselves are nothing more but the same-old-same-old, not overly distant from failed American initiatives like the Broadcast Flag.

- The requirements fail to accommodate rights reserved to public under national copyright regimes.
- The requirements are flawed because they are based on an analogy with contract law. This is factually erroneous and legally misleading because it implies that consumers have voluntarily and consciously assented to changes in their rights and customary expected uses of digital media.
- The chief characteristic of many DRM systems is that consumers are not advised of, nor able to learn in advance of, the restriction of uses of purchased digital media content or limitations in device use.
- The requirements are not neutral as between different business models for distribution of content- for instance, the requirements would preclude development and use of free and open source devices and would not permit use of works released by authors under Creative Commons licences.

Alternative Approaches

Given the total failure of DRM to date to enrich creators or prevent unauthorised Internet distribution of works, it is a pity that NAVSHP started with the premise that the world needs more DRM, rather than exploring whether that is indeed the best way to foster the development of the home audiovisual market.

A more reasonable and balanced approach would be to start by asking, "How can we enrich creators and encourage creation?" and "If DRM vendors claim to be able to enrich creators and prevent unauthorised Internet distribution, what evidence can they offer in support of these claims?"

The EU -- and the world -- is experiencing a revolution in creativity thanks to the Internet. An entire generation of remixers, talented amateurs, and Creative Commons enthusiasts have created over fifty million works that do not require DRM to thrive. A useful work product from NAVSHP would be a set of technology standards recommendations for systems that embrace unrestricted copying, in support of these new, Internet-native business-models. These European creators deserve every bit as much attention from the EU as do American film studios and other incumbents.

It is the author's opinion that NAVSHP should begin a fresh inquiry to look at the broader question of how DRM technologies impact the marketplace for home audiovisual technologies. This inquiry should be based on the wide range of available empirical data at hand and focus on the following issues:

- Has DRM technology been successful at preventing the unauthorized Internet distribution of material, or have overly broad use-restrictions provided otherwise law-abiding consumers with incentives to find unrestricted material on peer to peer networks?
- What technological systems can enrich creators?
- What technological systems can encourage the creation of new works and new business models?
- What technological needs do "copy-friendly" creators have, and how could standardisation aid them?

The NAVSHP Requirements undermine existing public rights under copyright

No nexus with copyright law

The NAVSHP Requirements document nominally concerns itself with matters related to copyright but appears to have been penned without even a cursory nod to how copyright law actually works.

The liberal use of non-legal terms like "copyright circumvention" and the occasional non-sequitur like "Downloading is not freeloading, and yet many content consumers fail to make the distinction." (P33, Socio-Economic Requirements) suggests that the authors of this paper attended only lightly, if at all, to the realities of copyright law. Rather, this document represents a dramatic reshaping of copyright law, one that excises the public side of the copyright bargain in order to deliver windfall monopoly rents to entertainment companies.

For example, the definition of copyright law on page 6:

Copyright law: Copyright law is a law (DMCA, EUCD...) defining certain rights to content of rights holders. Each country has its own copyright law and, in the case of Europe, each country handles a specific roadmap for the national transcription of the EUCD [AD.9]. The economic role of Copyright law, "is to provide incentives in intellectual creation by giving the owner a temporary monopoly on exploitation" [AD.9]. (*P6, Glossary of Terms*)

While this is correct as far as it goes, it conveniently omits one of copyright's most important traits: copyright is a monopoly of limited *scope* as well as temporary duration. The scope of copyright is set by statute, and every activity that falls outside of this scope (notably criticism, research, parody, quotation, private use, resale and other traditional elements of the public's side of copyright) is *not* part of the author's monopoly.

One of DRM systems' worst failings is that they indiscriminately restrict uses regardless of whether those uses are a rightsholder's to control -- for example, DVDs use a region-control system to restrict which country a lawfully acquired DVD can be viewed in, but nowhere does copyright grant a filmmaker the right to tell a customer where she can and can't enjoy her property.

Incomplete view of "social uses"

The paper does attempt to come to grips with the public's side of the copyright bargain with statement like these:

End-user rights: a collection of rights and exceptions granted to end-users by certain legislations (sic) (*P6, Glossary of Terms*)

By social use, we envisage cases such as time shifting, private backup copying or uses for educational purposes. (*P14, The Goal of DRM Systems*)

These definitions are incomplete. End-user rights are not merely those set by legislation: they are also embodied in case-law and custom. Indeed, many of the most important public rights under copyright including home recording (taping a TV programme) and private copying (moving a song from a CD to an MP3 player) are not found in many countries' laws, but rather in their court rulings or common practices.

The list of "social uses" conspicuously lacks many of the most important of these uses: research, parody and criticism to name just a few.

Misleading analogies to contract law

The implication in the requirements is that the outcome of this work item will be a world where rightsholders offer a rich variety of services and the public negotiates to get the best deal. Indeed, the document describes "contracts" in its definitional section:

Contract law: Contract Law designates a contractual agreement between parties (e.g. content owners and/or service providers and end-users or subscribers).

The reality of DRM is very far from this, though. In DRM systems, the deal is rarely competitive and even more seldom is it negotiated. For example, an iTunes DRM song often costs 2-3 times what it would cost if bought as part of a CD, yet a CD offers tracks that can be played on unlimited devices, ripped to MP3, and many other rights that do not come with the DRM version.

Does a user form a "contract" to eschew playing a DRM CD on her MP3 player simply by bringing it to the cash-register and paying for it? The entertainment industry argues that the simple act of buying a good like a DVD or a CD is a contract through which consumers agree to waive their rights under copyright to their detriment and a rightsholder's benefit. Unfortunately this report reinforces that spurious assumption without any analysis of the underlying legal reality.

Unilateral renegotiation of terms

Even these slippery "contracts" are subject to further abuse. Through the use of revocation and renewal mechanisms, the entertainment companies and DRM vendors unilaterally re-negotiate the terms of the contract even after a customer has bought her devices and media. For example:

- iTunes customers have had the right to burn a playlist 10 times unilaterally reduced to seven; have had the ability to stream to an unlimited number of friends reduced to five streaming sessions per 24 hours; have had the right to stream from a home server to their office computer taken away, and many other iTunes rights have been confiscated from people who'd already paid for their music
- TiVo customers in the USA have had their devices reprogrammed to allow broadcasters to erase programs from their libraries

DRM devices that are capable of being "renewed" and "revoked" by rightsholders are devices that can with impunity break any "contract" the user forms when she hands her money over.

The NAVSHP document explicitly requires renewability capabilities for DRM systems:

There is a need to give the DRM system the ability for the essential security elements of the DRM system to be renewable in case of hacking of the system. (P25, *TSC-0014 Renewability*)

Misappropriating analogue-world rights

The NAVSHP document speaks of "[preserving] the rights enjoyed with traditional analogue content" (P16, 2.2.2 Ease of access to and use of content), but in the actual requirements, traditional analogue uses get short shrift:

For instance, some business might want to allow the buyer of a vinyl record to get access to a digital counterpart as well, or to give that buyer some other benefit that can be managed using a DRM toolkit. (P14, *The Goal of DRM Systems*)

That would, indeed, be nice: but consider that today the public don't need a business to "allow" it to make digital copies of analogue media: a customer can convert her own records, cassettes, films, photos, and even books to digital format, legally and simply, using scanners, digital audio recorders, and tuner-cards.

There is a need to give the DRM system the ability to force the presence of certain content segments as a condition for playing it (e.g., author details or copyright information), even if content is allowed to be modified. (*P26, TRA-0003 Content segments*)

Owners of analogue media never have their fast-forward buttons disabled at the pleasure of rightsholders. It is only with DRM media where we see this "feature" deployed. In DVD, the no-fast-forward function was ostensibly created to force users to sit through Interpol warnings, however, its presence proved all too attractive to Hollywood studios, as anyone who has sat through ten minutes of mandatory child-targeted advertisements each time she puts on a Disney DVD can attest.

There is a need to give the DRM system the ability to ensure the integrity of the protected content (avoiding any modification to the content), in a manner independent of the transport mechanism. (*P25, TSC-0011 Protected content integrity*)

For half a century, users of analogue media have enjoyed the ability to "format-shift" their media. They have been able to record their LPs to tape, their CDs to MP3, their laser discs to VHS, and so on. This has been of great benefit particularly to users who invest in media for platforms that vanish from the marketplace: the ability to migrate one's music and other entertainment products from a dying format to a new one means that the public can preserve its investment in entertainment product.

Home tapers aren't the only ones who make use of format-shifting, though. Disabled people and those who provide access to them routinely format-shift copyrighted work to assistive formats, without rightsholder permission. In many countries, this right is enshrined in national law.

Treats users as attackers

But home-tapers and all other end-users are considered the attackers of the DRM system envisioned in the NAVSHP paper. It is telling that a long section of requirements is called "Motivating obedience." The user is the entity least trusted by DRM, the entity whose will DRM is designed to foil.

Thus, we have a DRM system that will dispense with the presumption of innocence:

When acquiring protected content, if all, or some portion, of the information associated with an item of content that would be used to determine a trusted usage rule mapping, is found to be corrupted or unintelligible due to errors (but still recognisable as protected content licence (sic)), the appropriate Usage Rule shall be deemed to be the most restrictive states of contextually applicable Usage Indicators for that portion of the information that is in question due to those errors. Consumers should be notified of corresponding

usage restrictions (*P17, BME-0003, Copyright circumvented protected content access and consumption*)

The requirement above would guarantee that the smallest error in a file-transfer would be treated as an attempt on a user's part to cheat a rightsholder, and the user's DRM devices must respond by locking her out of all but the most primitive rights to her property.

Attackers have no right to privacy, so despite requirements like SPV-0001, which allows (but does not require) a rightsholder to offer systems that "respect and ensure user privacy," we have the demand that DRM should:

Make it difficult for violators to stay anonymous. (*P14, The Goal of DRM Systems*)

and

There is a need to give the DRM system the possibility for the license issuer to reliably identify and authenticate the device or a specified domain, for the purpose of either issuing or refusing a license to that device or specified domain. (*P17, BMM-0012 Device identification and authentication*)

and

There is a need to give the DRM system the capability of reporting copyright violations to the management/accounting systems, making the best effort to identify the violators. (*P26, TMO-0003 Report violations to management systems*)

The NAVSHP Requirements attack legitimate businesses

Inconsistent with innovative content businesses

The NAVSHP requirements purport to be about preserving and encouraging commerce, but they are only concerned with the commercial fortunes of one party, the entertainment companies, to the exclusion and detriment of others.

The NAVSHP requirements attack the idea of general-purpose devices and the businesses that make them, free and open source software and the businesses that produce it, and Creative Commons licensed works and the artists who create them.

Creative Commons (creativecommons.org) is a licensing scheme that allows creators to give some of their copyright back to the public, to permit copying, reuse and sharing. Over 53 million works have been licensed under Creative Commons licenses in the two years since the project's inception, and the licenses themselves have been translated into twenty-plus legal systems and languages (with more than 80 translation projects in total underway at present). The author's own highly successful novels, published by a division of Holtzbrink, are released under these licenses.

Creative Commons licenses prohibit the use of DRM in connection with their use. Nevertheless, we have statements like this:

Eliminate the proliferation of unprotected copyrighted content. (*P16, Efficient Use Control*)

This statement not only seeks to restrict access to Hollywood's movies and music, but it also seeks to eliminate competing models for authorship. It tells the authors of fifty-three million Creative Commons-licensed works that they are slated for elimination under the regime proposed by NAVSHP.

Attack on general-purpose PCs and Free and Open Source

But Creative Commons users aren't the only creators shorted by this proposal. Since the dawn of the Industrial Age, the practice of end-users modifying and improving on their tools has been understood to be of great social benefit. "Remixing" one's devices is a way of extracting fallow economic value from one's investments, and an engine of innovation.

The NAVSHP requirements attack this idea in several places:

Device: A device is an entity, were a user is able to exercise a defined set of utility functions to a content item. A 'device' can be either a software application or a hardware device. (*P6, Glossary of Terms*)

A device that can only exercise "a defined set of...functions" is a device that users must not be able to modify or improve upon, something confirmed by a later requirement:

There is a need to give the DRM system the ability to prevent the compromise of the whole system security, if a single key or a small number of devices are hacked, by using tamper resistance mechanisms (hardware and software) to enhance the global security. Every sensible element in the content supply chain is required to be tamper resistant in proportion to the threat. (*P22, TCL-0004 Global System Security*)

Many hundreds of thousands of programs and devices are built on Free and Open Source Software (FOSS), software that is licensed in a way that encourages its users to understand, modify and improve on it. A general requirement for "tamper-resistance" is a blanket ban on FOSS techniques and on the myriad of businesses (from giants like IBM and Red Hat to thousands of SMEs) that are built on FOSS.

Attack on manufacturers' business-models

As noted above, there are innumerable businesses built on manipulating the analogue outputs of digital devices, such as the Slingbox, the Orb, the TiVo, and video-capture-cards like the All-in-Wonder. These devices allow users to realise dividends on their technology investments by extending their functionality. The legitimate, lawful uses they enable are reserved to the public under copyright law (and are given to users by these companies for free).

Yet the emphasis on enabling entertainment company business-models necessarily undermines the business-models of these companies. Hollywood intends to charge money for the features that these companies give users for free, and for that to happen, the entertainment companies must find a way to eliminate competing technologies.

Nothing could make this clearer than section 3.3.1., "Affordability" in which there is no mention of the need to make DRM affordable for device vendors.

There is no way that DRM can be made affordable to a company using Free and Open Source Software (since mandatory tamper-resistance would require rewriting their code from scratch). DRM cannot be made affordable to companies whose businesses are built on Creative Commons licenses (since none of those works may be used in connection with DRM). DRM cannot be made affordable to companies whose products DRM seeks to eliminate.

Conclusion

The NAVSHP process, with its emphasis on input from rightsholders and DRM vendors like Intel, has yielded a skewed, unbalanced set of requirements that have no coherence with copyright law nor with marketplace realities.

A more balanced approach would take the technology needs of all creators into account, and at a minimum ask how more DRM can solve the problems that all the DRM to date have failed to address.