My name is John M. Zulauf and I am writing as private citizen and information technology professional. My comment is directed specifically at the questions posed regarding Section 109 regarding first sale and Section 117 archival, interoperability, and temporary copies. My comments will also contain references to "fair use" subjects -- space shifting, excerption, criticism, and time-shifting -- based on questions in the section "2. General."

The form of my comments today is to take a detailed view of a proposed comprehensive copy management and control architecture. This review address specifically the impact on 106 and 117 of comprehensive content protection systems now envisioned by the media and consumer electronics industry. This review will show a pattern of systematic elimination of the traditional first sale restrictions on the copyright holder, and further a systematic elimination of archival and all other fair use "rights" as traditionally held. The system achieves absolute control over the use of digital content by a comprehensive set of licensing restriction on the behavior of digital-media consumer electronics devices. This license is imposed by use of encryption protected (in the system architect's view) by an absolute anti-circumvention protection under DMCA section 1201.

The proposed system reviewed CPSA -- "Content Protection System Architecture; A Comprehensive Framework for Content Protection" is documented at http://www.dvdcca.org/4centity/data/tech/cpsa/cpsa081.pdf . The document itself is subject to copy controls such that it can neither be downloaded from the web nor saved from the Adobe PDF reader. The only means by which this criticism is possible is by page by page cut and paste from the document. Ironically and chillingly, were the CPSA document protected by CPSA, no such excerption or criticism would be possible at all. Because of this, were this document to prove to be a significant embarrassment to the DVDCCA and its authors, they could simply unpublish the work by removing it from their website -- thus removing all first source evidence of their current proposals.

While this is a lengthy response to these questions, and the detailed review of the CPSA is necessary to show the devastating extent to which traditional consumers rights can be erode using anti-circumvention as the wedge. The CPSA provides a chilling vision of our future unless broad exemptions to the DMCA 1201 anti-circumvention provisions are granted. These exemptions are discussed in the “3. Conclusions” section.

0. Abstract

A review of the proposed CPSA content control system and it's probable impact on fair use and first sale. Conclusions include the need for broad exemptions from the DMCA 1201 anti-circumvent provisions for all non-pay-per-view publish works and all works access for fair use.

1. Introduction:

The proposed CPSA gives us a view of the future of access and use control without the limitations imposed on the copyright holders and distribution channel that broad exemption to 1201 would bring. In this possible future, first sale is discarded, archival and other fair use abandoned in favor of a "comprehensive" control of all access and use of digital media. Note that no differentiation is made between published and broadcast work, nor between pay-per-view and unlimited view works. This lack of differentiation show the utter disregard for both first sale and fair use, as well as an intentional desire to eliminate the consumer rights granted in "Betamax" and "Vault v. Quaid" case law.

The following are excerpts from the current draft of the CPSA document identified as "Revision 0.81", dated February 17, 2000, and authored jointly by Intel Corporation, International Business Machines Corporation, Matsushita Electric Industrial Co., Ltd. and Toshiba Corporation. The excerpts are denoted by lines beginning with ">" and are quoted directly from the cited web document.

> *The protection comes from compliant devices responding*

> *appropriately to manage the content according to the CMI.*
> *Such protection is realized only if there is some*
> *means, or "hook", to compel devices to be compliant.*
>
> *Encryption is that hook. Encryption is a way of scrambling*
> *digital content so that it is unusable (not recognizable)*
> *unless it is first descrambled (decrypted). To get the*
> *necessary intellectual property to be able to decrypt the*
> *content, a license is required. That license contract*
> *specifies requirements to manage the content according to*
> *its CMI.*

The first expert from the CSPA document show the intent to utilize encryption systems not as content protection but as a negotiating "hook." The encryption is specifically disclaimed as not being the means of content protection "protection comes from compliant devices." This is of concern particularly as it is the position of the MPAA and the DVD-CAA that this "hook" encryption has unlimited DMCA 1201 protection and thus has the force of the entire US government behind it. That's no "hook," that's fishing with high explosives!

Further, it says that the encryption has nothing to do with protecting the content -- it's all about controlling the behavior of devices that want to use the content. This is explicitly use control after first sale. What it enables, as we shall see below, is explicitly taking away the end-users first sale and fair use with a non-party agreement.

2: CPSA Axioms

The CPSA system architecture comprises a set of axioms. As used in software and systems design, an architecture has to do with functional blocks, subsystems, key algorithmic components. The CPSA axioms function more like a set of contractual obligations than an overall system design. Aside from that the axioms are themselves collectively and separately a harmful to first sale and fair use, especially when considering non-pay-per-view content (broadcast or published). Ironically, there's still nothing in the axioms to prevent wholesale commercial piracy of published media. This content is still subject to DVD-stamping wholesale piracy. Thus the consumers' rights have been abridged with the copyright holder gaining no commercially meaningful protection.

> ==========
> *CPSA Axioms*
> ==========
> *CPSA provides a framework of 11 axioms that describe how*
> *CPSA-compliant devices handle the*

Note that the role of the axioms is explicitly control over the behavior of devices and thus "use control" as it in turn limits the functionality available to the consumer.

> *three major areas that are critical to ensuring a*
> *comprehensive, consistent content protection scheme:*
> *content management information, access, and recording.*

Fair use and first sale are not even a consideration in the design of this system. This is unsurprising in one sense, no system can be made which judge the intent of a use. However, their choice is thus to allow only the most limited use, disregarding other legitimate uses utterly prohibited by the design.

> *Content Management Information Axioms*
> *Content Management Information (CMI) is information carried*

> *with content that indicates limitations on its allowed usage,*
> *such as constraints on making copies.*
> *1. Content Owner Selects CMI*

This first axiom and all below it reveal a particular world view. In place of "copyright holder" -- the subject of the DMCA and other copyright law -- CPSA consistently refers to the "content owner." This implication of ownership stretches the copyright holders rights far past first sale and includes the ability to control the consumers use of legitimately acquired, published works.

While I am not a lawyer (IANAL) it is my understanding that the concept of "content owner" -- is pure fiction. There is a copyright holder who holds certain limited rights (limited by the "limited times" clause, and first sale and fair use) over their works, but there is no "content owner." Ownership of published content is not granted -- a copyright is. This distinction is important as the CPSA axioms all assume unlimited rights of the copyright holder over the digital work before and after first sale.

> *Axiom: The content owner selects the content management*
> *information (CMI) from the supported options.*

Implication: CPSA allows total control over the use past first sale of content regardless of the traditional balance in copyright law, case law (Sony Corporation of America v. Universal Studios, 464 U.S. 417 (198), hereafter referred to as "Betamax") to suit the needs of a media company's business model.

> *The content owner selects the appropriate content management*
> *information for his or her content from the supported options.*
> *The available options vary for different types of content according to*
> *agreements made between content owners and device manufacturers.*

Implication: the CPSA will allow non-party agreements to control the behavior of digital media purchasers after first sale through controlling the functionality of available devices.

> *2. Ensure Digital CMI Integrity*
> *Axiom: While the content remains in the encrypted digital form,*
> *the CMI integrity is ensured*

... by licensing terms imposed by the "hook" of encryption and backed up by the anti-circumvention provisions of the DMCA ...

> *during transmission and storage using the encryption and key*
> *management protocols.*

Implication: CPSA will allow copyright holders to ignore the Betamax decision and control the user's storage of broadcast content.

> *CMI is stored and/or transmitted along with the content.*
> *While the content remains in the encrypted digital form,*
> *the CMI can be carried digitally. For example, the CMI*
> *may be encrypted along with the content.*

Implication: CPSA can hide the CMI rules such that non-protected content cannot be known to be non-protected without decrypting the content. This ensures that only CPSA-compliant devices can be used even if the CMI rules would allow unlimited copying or access -- clearly controlling consumer use of digital media past first sale.

> *3. Optional Watermarking*

> *Axiom: At the content owner's option, the original content*
> *may be watermarked for the purpose of transmitting the CMI*
> *with the content, independent of its specific analog,*
> *digital or encrypted digital representation.*

Implication: Using CPSA the copyright holder can hide the CMI in the content so you can't know whether you can copy it without first decrypting the content. Also it means -- "if we're paranoid, we can reduce your image quality to encode our paranoia in the picture." Note below.

> *Some content owners may not want to include a watermark*
> *in portions of content where they are concerned about*
> *transparency, for example.*

> ==========
> *Access Control Axioms*
> ==========
> *In CPSA, encryption can be used to prevent non-compliant*
> *devices from accessing protected content. Alternatively,*
> *where encryption is not present, compliant devices*
> *control access by detecting watermark CMI and responding*
> *appropriately.*

Note that the purpose of encryption is not to protect the content but control the implementation of the devices. Note that nothing is said about the authority of the user (as granted by first sale or other means) or the "authority of the copyright holder", only the compliance of the device. While ignores the language of the DMCA, the use of encryption as the "hook" allows effectively bringing DMCA protection (under the view of the DVD-CCA) to these clearly unprotected implementation details.

> *4. Encrypt Prerecorded Content*
> *Axiom: All CPSA content on prerecorded media is encrypted.*
>
> *Content encryption is a key facet of CPSA. It ensures that*
> *the content cannot be accessed until it is decrypted.*

"All ... media is encrypted." What we have here is death sentence for public domain works, and the "limited times" clause. All digital content is locked up for the unlimited time of the non-party CPSA license agreement. Fair use and archival are dead -- all future media is owned by the media companies to serve their business models. This cannot be what the framers of the Constitution nor the authors of the DMCA had in mind.

> *In conjunction with licensing structures, it is the "hook"*
> *that compels users to honor the provisions of the content*
> *protection system. Thus, all digital content that has usage*
> *restrictions on prerecorded media (e.g. DVD-ROM) is encrypted.*

This not access control, this is use control. A LICENSE between an agent of the COPYRIGHT HOLDERS (the DVD-CCA) and the device MANUFACTURERS "compels the user." Note here the explicit non-privity. The user has signed no agreement giving up his or her fair use or first sale rights. Note also that the encryption isn't the protective measure but only the "hook" here again.

> *5. Encrypt Authorized Copies*
> *Axiom: All authorized copies of CPSA content are encrypted,*
> *except where specifically agreed otherwise.*
>
>*Just as all content with usage restrictions on prerecorded*
> *media is encrypted, so are all authorized digital copies*

> *of such content (meaning content that arrives encrypted*
> *and/or containing watermark CMI). For example, when a*
> *CPSA-compliant device receives analog*
> *content with watermark CMI, a digital copy of the analog*
> *input will be encrypted. This allows the encryption "hook"*
> *mentioned previously to remain in place even for authorized*
> *copies.*

So the copyright holders can (a) control by technical means when I can copy and (b) they will force my copy to be encrypted when they do allow it (c) and they can control this after first sale. By this means even the copies they allow me are walled off from me. Even where some copying is allowed, the real fair use, space shifting, first sale etc. are prevent as the content remains behind the CPSA wall of "axioms" -- unable for access except by CPSA-compliant devices.

> *An exception to this is the DVD-audio framework, which*
> *allows an unencrypted copy on legacy media (CD-R, CD-RW,*
> *Mini-Disc or DAT) of any audio content with a sound*
> *quality equivalent to CD-Audio or less.*

Oddly, CD-R and MP3's are explicitly excepted. From earlier testimony before the Library of Congress, "Napster" was the end of the world, doomsday scenario. Here CPSA does nothing to address it. In any case this isn't technically feasible and is only a bow to reality.

> *6. Playback Control*
> *Axiom: Compliant playback modules detect the watermark*
> *CMI when present in unencrypted content and respond*
> *appropriately to prevent playback of unauthorized copies.*
>
> *Before playing back unencrypted digital content, compliant*
> *playback modules check for watermark CMI. If present in*
> *unencrypted digital content, compliant modules will not*
> *allow playback, since all digital copies of content with*
> *watermark CMI should be encrypted.*

Note the authorization circular logic here. All unencrypted copies are de facto unauthorized. What is a the test for the "authority of the copyright holder"? Merely the presence of the encryption scheme. This is how the encryption hook is "set." Only encrypted copies are valid, and to play encrypted copies you need to licenses the CPSA IP. To do that you must agree to all their axioms. This is euphemistically referred to as "compliance."

> *7. Output Protection*
> *Axiom: For encrypted content, compliant playback and*
> *source modules apply an approved protection scheme to*
> *all outputs, according to the digital CMI settings,*
> *except where specifically agreed otherwise.*

> *Protection of encrypted CPSA content must continue during*
> *transmission, either by encryption (e.g., DTCP) or by an*
> *approved analog protection scheme such as Macrovision™.*

More contractual device control beyond the scope of the encryption. Every link, from player, to AV receiver, to video recorder, to television or video monitor must be compliant. As single piece of CPSA equipment forces all other new components to be compliant or be incompatible. Note the added cost and complexity now built in to every piece of consumer electronics.

> *8. Manage Protected Output of Unencrypted Content*

> *Axiom: Compliant source modules check the watermark CMI*
> *of unencrypted content prior to protected digital output,*
> *and if present, set the digital CMI for the output accordingly.*

This shows that the encryption is pure pretext and not needed except as the licensing "hook." Unencrypted data is given the same protection by compliant devices as encrypted data.

> *A compliant source module may optionally forward content*
> *that arrives unencrypted to a protected digital output.*
> *If it does so, the module must first check for watermark CMI,*
> *and if it is present, set the digital CMI of the protected*
> *output accordingly. This ensures that the digital CMI*
> *corresponds to the watermark CMI, which is necessary since*
> *compliant recording modules downstream will check only the*
> *digital CMI of encrypted content to determine if a copy is*
> *authorized.*

Note that encryption is not even needed once a critical mass of "compliant" devices is deployed. For a user, CPSA-compliant devices are viral. Once a CMI is detected, the content is treated as if it was encrypted (and in fact will be encrypted if recorded).

> *==========*
> *Recording Control Axioms*
> *==========*
> *Recording devices maintain content protection by examining*
> *digital or watermark CMI and making copies only if authorized*
> *to do so. Copies of content are encrypted (except as noted*
> *previously), and the digital and watermark CMI are updated*
> *to continue the protection of the copied material.*
>
> *9. Examine CCI Before Copying and Respond Accordingly*
> *Axiom: Compliant recording modules detect and respond*
> *appropriately to the CCI, if it is present, before creating*
> *a copy, if authorized to do so.*
>
> *o Digital CCI is examined for encrypted content*
> *o Watermark CCI is examined for unencrypted content*
> *Before making a copy, a compliant recording module checks*
> *the CCI information. If the module is making a copy from an*
> *encrypted source, it checks the digital CCI; otherwise, it*
> *checks the watermark CCI. The copy is made only if the CCI*
> *indicates that it is authorized.*

How can a device know when I have fair use rights? It cannot. Under the CPSA it can arbitrary control my ability to copy. Note again the implication that encryption is not necessary to protect works if devices are CPSA-compliant. Encryption is the "hook" to enforce the license, but unneeded functionality.

> *10. Update CCI Before Copying*
> *Axiom: Compliant recording modules appropriately update both*
> *the digital CCI and the watermark CCI, when present, before*
> *creating a copy.*

This is implementation housekeeping. Note again that encryption is not required for CCI as unencrypted but watermarked content receives the same protections.

> *Prior to creating a copy of CPSA content, compliant recording*

> *modules will appropriately update both the digital CCI and the*
> *watermark CCI, if present. Since the watermark CCI is always*
> *updated when a copy is made, compliant playback modules are*
> *not required to have watermark updating capability.*

> *Note that*
> *for non-CPSA content (unencrypted content without watermark*
> *CMI), a protection system may still support making an*
> *encrypted copy, in which case the digital CCI of the copy is*
> *set as defined by that system.*

It doesn't say what the CCI of the system is. Some CCI -- either "unlimited copies" or "no copies" -- is applied to my home videos or other non-CPSA at the devices discretion. Note that once CCI is applied, the content is then treated as CPSA content and always encrypted when recorded -- fully locking the user into using only CPSA-compliant devices even for content on which they (or no one) holds the copyright.

> *11. Temporary Images*
> *Axiom: Compliant recording modules do not inspect or update*
> *either the digital CCI or the watermark CCI when making an*
> *image that is both temporary and localized.*
>
> *To allow for enhanced (e.g. time-shifted) viewing of copy-*
> *never*

This is reveals another attack on fair use. It presumes that broadcast digital content (the only sort one would reasonably "time-shift") can be tagged as "copy-never." This is clear erosion of the Betamax decision. While below "time-shifting" is allowed within a given CPSA-compliant device, it is under far stronger limitations than those applied by Betamax with respect to archival and fair use.

> *content, compliant recording modules do not inspect or update*
> *either the digital CCI or the watermark CCI when making an*
> *image that is both temporary and localized.*
>
> *Content controlled in this manner must exist in a playable form*
> *for only a limited time, and must be stored in such a way that*
> *it can only be played back from the system used to create the*
> *image. Since such an image is not useful as an archival copy,*
> *it may be made independent of restrictions on copying indicated*
> *by the CCI.*

Here they pay some limited lip service to the Betamax decision and its implications regarding fair use "time shifting." However space-shifting, excerpting, and archival are clearly ignored. Also, it is unclear how can this be implemented on a software player without intrusive modifications of the file system, backup and network subsystems.

> *Note that although CCI is neither checked nor updated*
> *in this case, some types of content might contain other types of*
> *CMI, such as bits related to time shifting, that would need to*
> *be checked and*
> *updated appropriately.*

While the CCI always allows for the limited, same-device time shifting, CMI is allowed to prevent it. This is an interesting and deceptive approach. CPSA-compliant devices can claim that "time-shifting" is always allowed by the copy control subsystem. Since it can be prevented by the CMI, it’s much like proclaiming an open door policy thus, "The door is always open -- but sometimes we electrify the porch."

3. Conclusions

As you can see above, current technological developments threaten the very essence of first sale and fair use. Under the CPSA or other potential, future schemes these are systematically eradicated for the sake of the mythical "content owner." How is this achieved? The use of encryption and the anti-circumvention provisions of the DMCA provide an irresistible "hook" for any arbitrary set of restriction to be imposed on device manufacturers. This is true (in the view presented within the CPSA draft) even if the designers of the system assert explicitly that the encryption is merely a pretext (a "hook") to force compliance to rest of the content control scheme.

Only broad exemptions to the anti-circumvention measures in the DMCA can dull this "hook" and prevent abusive and arbitrary schemes such as those proposed in CPSA. My recommendation for a sufficient set of exemptions are: (Note: in the following PPV is the abbreviation for "pay-per-view")

Class 1: published, non-PPV works

Exemption: full exemption from all anti-circumvention measures based on traditional first sale.

Class 2: works accessed for fair use

Exemption: full exemption from anti-circumvention for works after first sale (non-PPV) or first access (PPV) when utilized for fair use.

Class 3: broadcast works (including webcast, cable and pay-per-view)

Exemption: rights granted in the Betamax decision -- including non-encrypted archival, time and space shift, if access to work is legitimate (i.e. legal cable access, and pay-per-view authorization)

Without this we can expect that this dark, restrictive vision of CPSA will come to pass in the all to near future. Please remember that this document itself would not have been possible if the axioms described in the CPSA document had been applied to the CPSA document.

I thank you for you attention to this lengthy response.