1 Introduction

The Government of Canada is responsible for balancing the legal protection and financial incentives of copyright for content owners with the cultural benefits to society. Fair dealing rights are an intrinsic part of the balance in copyright between content owners and society. Copyright is to protect the right to make copies and not to control the use of legally purchased copyright material.

The upcoming copyright reform is of interest because of the possibility of DMCA like provisions coming to Canada. The main concern is the anti-circumvention provisions that make it illegal to circumvent TPMs that are part of DRM systems. Especially, when the circumvention is for preserving fair dealing rights that are unavailable because of the DRM.

Content owners (CO) view DRM as necessary in order to protect their legal rights, maximize their profits and protect their businesses. Information technology (IT) and consumer electronic (CE) manufacturers view DRM as a necessary feature in order to get access to content for their next generation technologies such as digital television (DTV) and high definition (HD).

Consumers want to enjoy entertainment at the highest level of quality that is available and affordable to them. However, entertainment is not the only requirement for people who purchase content. Fair dealing rights for consumers, educators, researchers and libraries are also required. The technological changes that are creating challenges and opportunities for IT, CE and CO companies are empowering people to become content creators and owners as well. Technological and cultural change go hand in hand and re-mixing culture is popular culture (e.g. rap, mashups, youtube, fan fiction, blogs).

By focusing on the design principles and actual implementations of DRM systems, the effects on consumers may be objectively determined. When evaluating new technologies it is important to separate the marketing hype from the actual behaviour and capabilities of the deployed system. Also, there can be no new technology deployment without its fair share of bugs and problems.

2 Assumptions

- Knowledge of common TPMs and DRM systems.
    - AACS information is from <http://www.aacsla.com/specifications/>.
- Knowledge of fair dealing rights.

3 Glossary

- AACS = advanced access content system
- CE = consumer electronic
- CO = content owners
- DRM = digital rights management
- DTV = digital television
- HD = high definition
- IT = information technology
- LA = licensing authority
- TPM = technological protection measure

4 Issues

How have DRM systems affected consumers fair dealing rights?

5 Analysis: How have DRM systems affected consumers fair dealing rights?

5.1 Who is DRM designed for and why?

Digital rights management (DRM) is fundamentally about control. Control over the content implies control over the technology used to create, distribute and view the content. The systematic controls in hardware and software are enforced through the use of cryptography and encryption to make up the foundation of a DRM system.

DRM systems are designed to satisfy CO requirements over the control and use of the copyrighted content they own. The design process and goals do not account for the

Canadian consumers' fair dealing rights. In fact, through the control afforded by DRM the fair dealing rights have been restricted to the point where they do not exist except at the discretion of the CO.

The restriction on consumer fair dealing rights can be understood through an examination of a modern deployed DRM system such as AACS. For example, AACS was developed by IT, CE and CO companies in cooperation. AACS is designed to "protect" content for CO - or from consumers - for the new technologies of high definition (HD) and digital television (DTV) to the specifications set by the CO. The IT and CE companies benefit by owning the market through standards and technologies that they developed and patented. The IT and CE companies also benefit because of the marketing advantages and the release of content for these new technologies.

The following excerpt is from AACS LA LLC, "Advanced Access Content System: Introduction and Common Cryptographic Elements" (February 17, 2006), <http://www.aacsla.com/specifications/specs091/AACS_Spec_Common_0.91.pdf> [AACS: Introduction and Common Cryptographic Elements].

> 1.1 AACS Purpose and Scope
>
> "The Advanced Access Content System (AACS) specification defines an advanced, robust and renewable method for protecting audiovisual entertainment content, including high-definition content."
>
> 1.2 AACS Objectives and Design Criteria
>
> AACS is designed to meet the following general criteria:
>
> - Meet the content owners' requirements for robustness and system renewability
> - Content encryption based on a published cryptographic algorithm.
> - Limit access to protected content to only licensed compliant implementations.
> - Support revocation of individual compromised devices' keys.
> - Limit output and recording of protected content to a list of approved methods.
> - Suitable for implementation on both general-purpose computer and fixed-function consumer electronics platforms.
> - Applicable to both audio and video content, including high-definition video.
> - Applicable to various optical media formats.
> - **Transparent to authorized use by consumers.**
>
> To meet these general objectives, AACS is based in part on the following technical elements:
>
> - Robust encryption of protected content using the AES cipher.

- Key management and revocation using advanced Media Key Block technology.

Note: Is there a competition issue here? Companies like Sony and Microsoft also have IT, CE and CO subsidiaries like Sony Electronics, Sony Pictures, Sony BMG, Microsoft Entertainment and Devices and MSNBC.

5.2 How does AACS affect Canadian fair dealing rights?

AACS's design and features are representative of the next generation of DRM systems. AACS attempts to overcome the flaws of previous generations of DRM systems by embracing the concepts of growth and evolution through system renewability and key revocation. Every connection of an AACS device is encrypted and controlled through various TPMs. All technology licensing, verification and cryptographic keys are controlled through the AACS licensing authority (AACS LA), this ensures that no entity can create an AACS compatible device without the AACS LA's authorization. Lastly, all commands to control all the hardware comes from the content owners through AACS protected content.

The design and features of AACS clearly illustrates that its major goal is to remove control from the consumer, keeping it with the content owners. The technology licensing aspect prevents other companies from innovating and creating interoperable products because patents protect the technology used in AACS. The specific effects on consumers will be illustrated as each feature of AACS is examined.

5.3 Encryption

AACS encrypts content using modern cryptographic techniques. The rest of the AACS system is designed to protect the keys required to decrypt the content and to protect the decrypted content as it flows to the output device (AACS: Introduction and Common Cryptographic Elements at pg. 7).

The encryption of content that can only be decrypted at the CO approval removes the consumers' expected fair dealing rights. Without unencumbered access to the content there can be no consumer use of the content and therefore consumers will have no fair dealing rights.

5.4 System Renewability and Key Revocation

System renewability is the ability to update the DRM system when a component of the system is cracked. CSS was the clearest example of a DRM system that was not upgradeable, once broken it remained broken. System renewability is achievable through various mechanisms and in AACS it is accomplished through key revocation.

All devices that can decrypt AACS encrypted content must have a valid cryptographic key which is issued by the AACS LA. If the playback device or software player is compromised and its keys are obtained or otherwise allows unauthorized access to the encrypted content, the LA can revoke its keys. Now, the device will not be able playback newly encrypted AACS content because its key will no longer be valid (i.e. they have changed the lock).

Key revocation in AACS will occur through Media Key Blocks (MKB). The MKB is an intermediate lock that holds the actual key to the prerecorded content. A device will use its key to decrypt the MKB and generate another key which can be used to decrypt the prerecorded content. The MKB is specific to each title (e.g. movie) and can be changed to exclude the specific keys of compromised devices. The excluded devices will be unable to decrypt the updated MKB and therefore will not be able to generate the key needed to playback the content. (AACS: Introduction and Common Cryptographic Elements at pg. 11).

The consumer who purchases a device or software program that has its keys revoked will lose the ability to view newer encrypted content through no fault or action on their part. In fact, until there is an actual use of key revocation it is unknown just how much functionality will be lost. The consumer is constantly in jeopardy of losing access to new content and can do nothing to prevent this.

The consumer with a compromised device or software player may be able to upgrade the firmware or patch the software and recover the lost functionality. But, only the manufacturer can provide upgraded firmware or software and they would have to fix the compromise to the AACS LA's satisfaction in order to get new device keys (assuming the AACS LA allows this).

5.5 Managed Copy

The managed copy feature is part of the AACS specification for prerecorded content and allows the consumer to make at least one additional copy. The managed copy feature can only be used if there is an online connection to a managed copy server (MCS). If the copy is authorized by the MCS then it can be moved by an approved managed copy machine (MCM) which may be part of a home media server. The copy by the approved MCM is then bound using a managed content output technology (MCOT) of which there is no clear description. There are exceptions to the managed copy rule and the CO is allowed to charge for use of the managed copy feature. (AACS LA LLC, "Advanced Access Content System: Pre-recorded Video Book" (February 17, 2006), <http://www.aacsla.com/specifications/specs091/AACS_Spec_Prerecorded_0.91.pdf> at pg. 29).

The consumer is possibly allowed to make one copy of the purchased content, may have to pay again for that copy and may only move it to an authorized device. The consumer still does not have the expected fair dealing rights and cannot use the prerecorded content for educational, research or archival purposes. If there was no DRM then the managed copy feature would be of no use because the consumer would be able to make their own decisions on how to backup or move the content. The managed copy feature has not been deployed yet and there are no further details at this point in time.

5.6 Closing the Analog Hole

Analog signals are difficult to protect with TPMs but are used extensively in existing CE devices. The problem is that analog signals can be easily digitized and then distributed on the internet without a significant loss of quality. In transitioning from analog televisions to digital televisions (DTV) and the use of encrypted digital connections; the AACS LA is attempting to protect, constrain, turn-off and remove analog outputs through analog copy protection (ACP), image constraint token (ICT), digital only token (DOT) and the analog sunset clause.

The analog sunset clause in the licensing agreement attempts to remove and turn off all analog outputs by December 31, 2013. The analog sunset will be enforced by the

firmware which is in each CE device (AACS LA LLC, "Advanced Access Content System: Interim Adopter Agreement" (February 15, 2006), <http://www.aacsla.com/support/AACS_Interim_Adopter_Agreement_060215.pdf> at pg. 82.)

AACS mandates the use of analog copy protection (ACP) which is also known as macrovision on all analog outputs. In modern devices, ACP is added to the output analog signal by an extra chip in the CE device. The receiving devices will look for an ACP signal and if it is detected disable the analog input or prevent output. Interestingly, in most modern devices ACP only works because the devices are mandated to generate and check for the signal (Ernest Miller, "Macrovision's Magical DRM that Drastically Reduces P2P Distribution" (June 16, 2005) <http://importance.corante.com/archives/2005/06/16/macrovisions_magical_drm_that_drastically_reduces_p2p_distribution.php>).

AACS allows the CO to set the ICT on prerecorded content. If the ICT is set and the consumer is trying to use the analog output, the device will downgrade the quality of the HD signal to standard definition (SD). The CO can also set the DOT on prerecorded content so that even if there is an available analog output and it is before the analog sunset there will be no right to output an analog signal. Currently, the AACS Interim Adopters Agreement forbids the use of the DOT but mandates the detection and enforcement of the DOT.

The consumer is clearly losing the battle over control of their CE devices and especially so when AACS is attempting to kill all analog connections in the move from analog TV to HD and DTV. Backwards compatibility has been an important design principle in technology because it allows consumers to keep using existing devices with new devices. Some of the early HDTVs have only analog connections or do not have an approved encrypted digital connection (e.g. HDMI/DVI with HDCP).

Consumers will only be able to use AACS approved devices with their older analog devices, if the CO allows it and even if allowed it may be of downgraded quality. There are no fair dealing rights for consumers to backup or use their content for education,

research or archival purposes because of ACP, DOT and ultimately the analog sunset clause.

5.7 Approved Digital Connections are always Encrypted

AACS will only allow decrypted full resolution HD content to flow over approved encrypted digital connections. Whether the connection is DVI, HDMI or IEEE1394 they are all protected by DRM systems such as HDCP and DTCP. The physical connection technology of DVI, HDMI and IEEE1394 are unencrypted and useful in that they make connecting devices easier. However, HDCP and DTCP are responsible for authenticating the other connected devices and ensuring that the connection is encrypted. HDCP or DTCP compliance and version checking will likely be limited to every device through which the decrypted content will flow (e.g. cable extenders, image scalers, DTV, etc.).

HDCP and DTCP are complete DRM systems and have system renewability and key revocation as a design principle. Key revocation will occur through system renewability messages (SRM). The SRMs can come from the internet, digital set-top boxes (this includes over the air broadcasts), prerecorded content and other connected devices. In fact, all connected devices will check for and update the SRM version of each connected device and only communicate with those that are not on the revocation list (Digital Transmission Licensing Authority, "5C Digital Transmission Content Protection White Paper" (July 14, 1998), <http://www.dtcp.com/data/wp_spec.pdf> at pg. 3), (Digital Content Protection LLC, "High-bandwidth Digital Content Protection System" (June 13, 2006), <http://www.digital-cp.com/home/HDCP_Specification_Rev1_2.pdf> at pg. 54).

The consumer loses control over the digital connections on devices with HDCP and DTCP support. They will not be able to use the content for any fair dealing purposes because they will not be able to access the content. Technically, even content that is not initially protected could end up being protected by HDCP or DTCP as it is being played back. How devices will handle amateur or homemade content is not clear.

5.8 Deploy, Crack, Patch and Fix

AACS has just been recently deployed in production HD DVD and Blu-ray devices and has not yet been cracked. Many consider it just a matter of time till AACS is broken. They point to the fact that CSS was cracked and broken permanently. However, deployed DRM systems like Microsoft's Windows Media DRM (WMDRM) and Apple's Fairplay DRM for iTunes have been repeatedly cracked and successfully patched.

In fact, over the past couple of weeks cracks for the latest version of iTunes and WMDRM have just been reported (Bill Rosenblatt, "Windows Media DRM Hacked" (August 31, 2006), <http://www.drmwatch.com/drmtech/article.php/3629681>). The released cracks (i.e. software programs) aim to strip the DRM in order to give consumers their fair dealing rights back. Unfortunately, anti-circumvention laws could make the development of such software illegal. Also, it may be illegal for consumers to exercise their fair dealing rights by downloading, using or sharing the crack under anti-circumvention laws.

It will take time for Apple and Microsoft to patch their DRM systems but it is highly unlikely that they will not be able to do it (apparently Microsoft patched the flaw in a record time of 3 days, after which it was promptly cracked again, see Bruce Schneier, "Quickest Patch Ever" (September 7, 2006), <http://www.wired.com/news/columns/0,71738-0.html?tw=rss.index>). This indicates that AACS, HDCP and DTCP will likely survive its attacks by hackers but it will become a never-ending battle. At least, not until all hardware is trusted with a black box owned by CO, CE and IT companies and not the consumer (but even then the attacks will continue).

Note: Development of the PC platform - especially as home media center - is going in the direction of the black box (e.g. Next Generation Secure Computing Base <http://www.microsoft.com/resources/ngscb/default.mspx> and Trusted Computing Group <https://www.trustedcomputinggroup.org/home>). Ideally for CO, the general purpose computer will become extinct and the replacement will be the CE limited purpose computer.

5.9 Summary of AACS Analysis

AACS is representative of many modern DRM systems. The designers clearly understand that the system will be attacked and cracked and that updating and patching the system will be necessary. The AACS system is only as good as its weakest link and subsequently HDCP and DTCP are also designed with system renewability in mind.

Although modern DRM systems may be cracked they will continue to deter and frustrate the average consumer. As long as AACS and associated are considered "effective" technological controls then they will receive the protection of any DMCA style anti-circumvention laws. The consumers' fair dealing rights are restricted or completely removed through the use of DRM systems that move control from the consumer to the CO.

6 What's next? DRM Ecosystems and Interoperability.

DRM is not a feature for consumers. It does not add anything of value that a consumer should want to pay extra for. The companies that have developed and deployed DRM systems know that when a consumer is educated about DRM it is very detrimental to their businesses. The current plethora of non-interoperable DRM systems creates headaches for consumers. DRM ecosystems are the next evolutionary step as they try to create interaction and interoperability between DRM systems.

The Coral Consortium's goal of "Make DRM Invisible!" will be a strong incentive to create the minimal amount of necessary compatibility among DRM systems in order to create a multi-DRM, multi-device ecosystem. This ecosystem will allow content to freely move among trusted CE devices owned by that consumer until the consumer runs into the invisible wall of DRM by trying to do something unauthorized. However, by addressing the inconvenience factor of the most common usage scenarios coupled with pricing incentives and technology lust, consumer resistance can be overcome and the true critical mass of DRM adoption may be achieved. A compelling example of interoperability - according to the Coral Consortium - is: download a video clip onto Motorola RAZR phone, then copy and play video on Sony PSP handheld game system and finally archive on HP laptop (Coral Consortium Corporation, "Coral

Consortium: An Overview" (February 2006), <http://www.coral-interop.org/main/faqs/Coral.Overview.pdf>).

For the consumer a DRM ecosystem is what fair dealing rights and DRM free content would naturally provide. It is ironic that the goal of a DRM ecosystem is what would naturally occur without DRM. Consumers would be free to innovate and use content in creative ways on multiple devices that they own. The most salient point is that in a DRM ecosystem control resides with the CO, CE and IT companies and that in the DRM free world control rests with the consumer.

7 Conclusion

The consumers' ability to exercise their fair dealing rights by using and controlling their legally purchased devices and content are being restricted by DRM systems. The CO, IT and CE companies realized that the more educated a consumer is about DRM and its effects, the more detrimental it is for their businesses. The goal of DRM ecosystems is to recreate the usage scenarios a consumer would have with their fair dealing rights. The pivotal difference is that the CO controls the usage scenarios available and not the consumer. This also restricts the ability of consumers to use their devices and content in novel and imaginative ways.

The design of AACS, HDCP and DTCP are modern but their deployment as new technologies may be filled with bugs and errors. The correct operation of this DRM ecosystem is already restrictive to consumers, but what about errors in operation or deployment mistakes? Why can the consumer not repair defective or overly restrictive DRM themselves, just like how they can repair their cars?

DRM systems are not perfect and never will be. They will be effective enough to attract the laws protection and therefore sufficient for the purposes they were created for. Those who believe that DRM systems will be easy to circumvent may not have accounted for the new evolving DRM concept because any simple attacks on the system should be easy to patch and fix. Brute force attacks and analysis may be ineffective because the underlying encryption technology could be robust enough. Neither "side" is smarter than the other but the well-funded corporations can lobby and pay for time with politicians.

The last word rests with the consumer and how they vote with their dollar. If consumers are willing to spend money on products that are protected or crippled by DRM then DRM will be the norm. Unfortunately, even conscious, freedom loving individuals will be hard pressed to find any CE devices without DRM in the marketplace. It is this unavailability of DRM free choices that is most burdensome on consumers. If CO, IT and CE companies are working together to create only devices with DRM then what DRM free choices will be available to consumers? The consumer can't vote with their dollar if their dollar can only buy technology with DRM.