Legal Issues Affecting Creation And Implementation Of DRM Systems

Gabriel M. Ramsey, Esq.
Overview of the DMCA (17 USC § 1201)

- Prohibits “circumvention” of “technological protection measures”

- In other words—DRM protecting copyrighted works

- Various remedies
  - Injunction
  - Devices impounded, modified or destroyed
  - Monetary damages (can be tripled for repeat offenders)
  - Defendant may pay plaintiff’s costs and attorneys fees

- Criminal penalties
  - Willful violations
  - For commercial advantage or private financial gain
Overview of the DMCA (17 USC § 1201)

Addresses Two Different Kinds Of DRM

- Measures that “effectively control access to a work”
- Measures that “effectively protect the right of a copyright owner”—i.e. protects against copying
- Different scope of liability for these different types of technologies
Overview of the DMCA (17 USC § 1201)

• “Access Control” Measures—who faces liability?
  • Manufacturers and distributors of technology which circumvents access controls
  • USERS of technology which circumvents access controls

• “Copy Control” Measures—who faces liability?
  • Only manufacturers and distributors of technology which circumvents copy controls
“Access Control” Measures

“Effectively controls access to a work” means:

“in the ordinary course of its operation, requires the application of information, or a process or treatment, with the authority of the copyright owner, to gain access to the work”
“Access Control” Measures

• “Access control” measures completely prevent any experience of the work

• Encryption is often a feature

• Examples:
  - CSS encryption and authentication for DVDs
  - Authentication handshake between PC and server
  - Region codes and authentication codes on
  - Authentication codes on game discs
“Access Control” Measures

- Must “effectively” control access
- If content easily obtained—measure does not “effectively” control access
- This is why encryption is important
- But, if unauthorized conduct leads to weakening of system, may still be considered “effective”
“Copy Control” Measures

“Effectively protects a right of a copyright owner [under the Copyright Act]” means:

“the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner . . .”
“Copy Control” Measures

- “Copy control” measures do not restrict initial experience of the work
- Rather, they limit what can be done with a work thereafter
- For example, may limit ability to reproduce, distribute, print, perform or display a work

Examples:
- DVD watermarks
- Adobe eBook use restrictions
- Macrovision Analog Copy Protection
“Copy Control” Measures

- Copy control measures may be intertwined with access control measures

- Like access controls—copy controls must “effectively” protect the copyright

- Content containing embedded “copying” preferences of the owner, but which does not enforce them is not effective
“Circumvention”

- To circumvent an access control measure:

  “to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner”

- To circumvent a copy control measure:

  “avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure”
“Circumvention”

- The troublesome issue of passwords

- Password authentication regimes are clearly “access control” measures as defined by the DMCA

- However, two courts have found that an unauthorized party obtaining access to and using passwords (to gain access to websites) is not “circumvention”

- Hard to see how this is different from obtaining access to and using CSS keys in the DeCSS software—found to constitute circumvention
Minimizing The Risk Of DRM

- So, you have your robust DRM
- You’re protecting your killer content!
- But your customers say that it broke their CD-ROM drive
- And they sue you . . .
Minimizing The Risk Of DRM

- A number of recent lawsuits by users claim that DRM harmed their computers or other interests

- Disputes turned on two key issues:
  - Alleged lack of user consent
  - Alleged affirmative misstatements about the nature of the DRM systems
Selecting A Strong DRM System

Overview of The DMCA

“Access Control” Measures

“Copy Control” Measures

“Circumvention”

Minimizing The Risk Of DRM

Obtaining User Consent

Use Care In What You Say

Minimizing The Risk Of DRM

User Consent

- End-user license must be accepted before DRM installed
- In the license, disclose the general nature of the DRM system
- Disclose in reasonable detail potentially contentious items
  - Low level drivers installed?
  - Collects or transmits information about the user or their computer?
  - Overwrites or replaces any files?
  - Anything that could degrade performance or pose risk to hardware?
  - Hidden files?
Minimizing The Risk Of DRM

Affirmative Statements

• The impulse is to downplay the functionalities of DRM

• Overly zealous “assurances” that user systems will not be affected can be risky

• Marketing and technical materials describing the system must, obviously, be accurate