



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

Digital Rights Management for the Enterprise

Frederic M. Wilf

Morgan, Lewis & Bockius, LLP

Philadelphia



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

Overview

- What is “Digital Rights Management”
- Pre-DRM: Traditional rights management
- DRM:
 - Digital Millennium Copyright Act
 - State “Super DMCA” statutes
 - Cases (*Reimerdes/Corley*, *Bunner*, *Lexmark*, *Chamberlain*)
 - Then v. Now
- In process
- Q & A



What is DRM?

- “Digital Rights Management” or “DRM”
 - (1) Any technology (called “technological protection measures” or “TPMs” a/k/a “access control technology”) used by an owner of an intellectual property right or other proprietary right to control, track and manage the use of those rights by others
 - (2) Specific laws and regulations that affect or enforce the use of TPMs, e.g., by prohibiting circumvention of those TPMs



Technological Protection Measures

- TPMs currently fall into two basic classes:
 - Containment
 - » Encryption or other technology (e.g., “handshake” process) designed to limit access to the protected item
 - Watermarking
 - » Embedding of data (text, graphic, symbol, etc.) that cannot easily be separated from the protected item



Goals of DRM

- Establish technologies that reduce or limit access to and use of digital works
 - » Only the right users
 - » Only the right uses
- Track works *and their users* across any network
 - » Internet, cable networks, satellite networks
- Limit or eliminate reverse engineering
- Punish any one who breaks TPMs or distributes technology used to break TPMs, regardless of whether any protected works are infringed
 - » Analogy to possession of burglary tools



Why Now?

- Why is DRM prominent and growing?
 - The technology is better
 - » Today's "technological protection measures" or "access control technology" generally better than yesterday's "copy protection"
 - Sui generis statutes provide civil and criminal liability for breaking the technology
 - » Can you spell "DMCA"?
 - Contract law now enforces previously-questionable contracts of adhesion
 - » Electronic Signatures in Global and National Commerce (E-SIGN)
 - » Uniform Electronic Transaction Act (UETA)



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

Talkin' About DRM

- It's a good thing...
 - “We can never abandon the fight to preserve intellectual property rights, just because it is difficult. The stakes are too high. Should law enforcement stop fighting crime just because efforts are difficult?” — the MPAA (www.mpaa.org)



Talkin' About DRM

- It's a bad thing...
 - “DRM is ... a private governance system in which computer program code regulates which acts users are (or are not) authorized to perform - than as a rights management regime or as a copyright-enforcement mechanism. ... The main goal of DRM mandates is not ... to stop ‘piracy’ but to change consumer expectations.”
— Prof. Samuelson in the April 2003 issue of *Communications of the ACM*
 - “The DMCA ... actually puts constraints on legitimate R&D in reverse engineering, ... it gives private firms a right of action to sue.” — Dr. Eugene “Spaf” Spafford on *Greplaw* 4/5/04



Before DRM: Past as Prologue

- Law has long required intellectual property rights owners to take specific actions to obtain, renew, and maintain their rights
- Traditional intellectual property rights management (“TRM”) (okay, it’s a retronym in counterpoint to “DRM”)
 - Applications for patents, trademarks, copyrights
 - Notice requirements
 - Mandatory licenses



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

Copyright Registration as a TRM

- Free forms at Copyright Office
 - » 202/707-3000 for hard copy
 - » <http://www.copyright.gov/forms> (.pdf)
- \$30 filing fee per application
- Copy of work on disk or hard copy



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

Copyright Registration as a TRM

- Registration required:
 - For U.S. citizens, to file a copyright infringement action in court
 - For any copyright owner, file prior to infringement to qualify for the best remedies
 - » Attorney's fees
 - » Statutory damages (\$200 - \$150,000)



Vault v. Quaid (Back in the Day)

- *Vault Corp. v. Quaid Software Ltd.*, 847 F.2d 255 (5th Cir. 1988)
- Vault’s software
 - Vault made “Prolok” software, a copy protection technology licensed to software vendors



Vault's Software

- Each software vendor used Prolok to prevent copying of the vendor's disks by its users
 - “Key disk” system using software and a hidden code
 - Vault included a shrinkwrap license agreement under Louisiana law that prohibited reverse engineering or copying of the technology
 - Louisiana passed the Software Licensing Enforcement Act (“SLEA”), which made the terms of shrinkwrap agreements enforceable in Louisiana



Vault v. Quaid

- Quaid’s software
 - Quaid bought a copy of Vault’s Prolok, reverse-engineered it, and then began selling the “Ramkey” utility as part of its “Copywrite” utilities package
 - Licensees of Prolok-protected software use Ramkey to break Prolok, make back-up copies or infringing copies of third party software
 - » Ramkey had no other use
 - One Ramkey version had a 30-character sequence found in Prolok



Vault v. Quaid

– Vault sued

- Copyright infringement, contributory copyright infringement
- Breach of contract
- Trade secret misappropriation under Louisiana UTSA



Vault v. Quaid

- Held,
 - No direct or contributory copyright infringement
 - 17 USC § 117 permits Quaid to copy Prolok into RAM
 - Ramkey “capable of substantial noninfringing uses” under *Sony v. Universal*, 464 US 417 (1984); no contributory infringement
 - 30 characters copied from 50 pages of source code not substantially similar to original, so there was no infringement of Vault’s copyright



Vault v. Quaid

- Shrinkwrap agreement not enforceable
 - SLEA prohibitions on reverse engineering pre-empted by Copyright Act
- Trade secret misappropriation does not apply when legitimate reverse engineering techniques used
 - Trial court so held; no appeal of this point by Vault
- Thus, Quaid could dismantle Vault's Prolok with impunity



DRM: Digital Millennium Copyright Act

- Digital Millennium Copyright Act (DMCA) is the best known DRM law
- DMCA \neq ©
 - (“DMCA is not necessarily copyright law”)
- Several discrete pieces, including
 - Online Copyright Infringement Liability Limitation Act
 - Copyright Protection and Management Systems
 - Vessel hull design
 - » Not discussed here



DMCA:

Online Service Provider (17 USC § 512)

- “Online Service Provider” designation
 - File a simple form, \$30 fee with the Copyright Office
 - » <http://www.copyright.gov/onlinesp>
 - » *ALS Scan Inc. v. Remarq Communities, Inc.*, 239 F.3d 619 (4th Cir. 2001)
(substantial compliance with notice provision required)



COMPUTERWORLD

ENTERPRISE MANAGEMENT WORLD

SOLUTIONS FOR THE DATA CENTER



www.morganlewis.com

September 12-15, 2004 • Philadelphia Marriott • Philadelphia, Pennsylvania

DMCA:

Online Service Provider (17 USC § 512)

» *Hendrickson v. eBay, Inc.*, No. CV 01-0495,

<http://news.findlaw.com/cnn/docs/ebay/hendrickson.pdf> (C.D. Cal., Sep. 6, 2001)
(§ 512 protects eBay against liability for sale of allegedly-infringing copies of videos)

– Problem: Mistaken notice leads to entire sites being taken down



DMCA:

Copyright Mgmt Info (17 USC § 1202)

- Copyright management information
 - Information about a work, including owner & title
 - Copyright notices
 - Embedded data (e.g., digital watermarks)



DMCA:

Copyright Mgmt Info (17 USC § 1202)

- Remedies when copyright mgmt info is falsified, removed or altered for the purpose of infringing a copyright
- *Kelly v. Arriba Soft Corp.*
 - Trial court: Online display of photographs without accompanying copyright notice does not violate §1202



DMCA:

Access Control Technology (17 §1201)

- §1201 is what most people mean when they say “DMCA”
- Access control technology (“ACT”) is any technology that limits access to content
 - In other words, it’s a technological protection measure (“TPM”)



DMCA:

Access Control Technology (17 §1201)

– ACT examples

- “CSS” used to protect DVD-based movies
- Handshake process between printer and toner cartridge
- Handshake process used in streaming media
- Rolling codes in garage door openers(?)



DMCA: Access Control Technology

- Key ACT provisions under 17 U.S.C.
 - § 1201(a)(1): Prohibits any circumvention of an ACT that protects a copyrighted work
 - § 1201(a)(2): Prohibits trafficking in any device (e.g., a program) that circumvents an ACT that controls access to a copyrighted work, and which has no substantial non-infringing purpose



DMCA: Access Control Technology

- § 1201(b): Prohibits trafficking in any device that circumvents protection provided by an ACT that protects a copyright owner's rights in a work
- §1201(f): Reverse engineering of ACT for software interoperability



DMCA:

Access Control Technology

- Other provisions limit applicability of §1201, and establish procedures by which Copyright Office creates exemptions
- Civil (lawsuit) and criminal (prosecution) provisions



DMCA: Access Control Technology

- Several criminal prosecutions reported
 - *United States v. Elcomsoft* (Adobe e-Book case)
 - » Dmitry Sklyarov dismissed
 - » Elcomsoft acquitted by jury
 - *United States v. David Rocci a/k/a crazy8*
(www.isoNews.com)
 - » Rocci pled guilty to illegally importing and distributing chips used to modify game consoles (“mod chips”) that circumvent TPM designed to prevent the use of pirated games
 - » Web site at www.isoNews.com now redirects to www.CyberCrime.gov



State “Super DMCA” Acts

- Model bill by Motion Picture Association of America
 - Prohibits circumvention of technological protection measures (TPMs)
- Passed in several states in various forms
 - Pennsylvania (Devices for Theft of Telecommunications Services, 18 Pa.C.S. §910), Delaware, Illinois, Maryland, Virginia, Wyoming
- Vetoed in Colorado (May 21, 2003)
- No cases reported, yet



“DeCSS” Cases

- Content Scramble System (CSS) is a TPM that protects movies on DVDs
 - CSS cracked
 - Cracking program (DeCSS) distributed online
 - In each case, defendants’ web sites distribute copies of DeCSS and link to other web sites that distribute DeCSS



“DeCSS” Cases

- 2600 Case (*Universal City Studios v. Reimerdes/Corley*)
 - *Universal City Studios, Inc. v. Reimerdes*, No. 00-Civ-0277, 111 F. Supp. 2d 294, <<http://www.nysd.uscourts.gov/courtweb/pdf/D02NYSC/00-08117.pdf>> (S.D.N.Y. Aug. 17, 2000), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, No. 00-9185, 2001 U.S. App. LEXIS 25330 (2d Cir. Nov. 28, 2001)



2600 DeCSS Case

- Permanent injunction granted
 - » CSS is an ACT designed to protect copyrighted movies
 - » DeCSS has no commercially significant purpose, other than to crack CSS ACT
 - » Distribution of DeCSS violates prohibition on trafficking in devices that circumvent ACT
 - » Hypertext links to copies of DeCSS on other web sites violate anti-trafficking provisions
 - » Reverse engineering exception under §1201(f) does not apply where the ACT protects non-software copyrighted works, such as movies
 - » Courts turn away all First Amendment arguments
- Defendants enjoined from distributing or linking to DeCSS



DVD CCA DeCSS Case

- Trade secret suit against web sites hosting DeCSS
 - *DVD Copy Control Ass'n, Inc. v. Bunner*,
 - » No. S102588 (Cal., Aug. 25, 2003)
<http://news.findlaw.com/hdocs/docs/dvd/dvdcca_bnnr82503opn.pdf>
 - » 21153 (Cal. App. Feb. 27, 2004)
 - Distributors of DeCSS software and hard copy versions
 - » Includes t-shirts (and ties?) with copy of DeCSS code



DVD CCA DeCSS Case

- Cal. Supreme Court upholds injunction
 - » CSS may be a trade secret under UTSA, remands
 - » After remand, the plaintiff dismisses, but Cal. App. Ct. holds reverse engineering is a proper way to learn a trade secret, so injunction should not have been granted
- Four years of litigation to overturn an injunction that should not have been granted in the first place



Lexmark v. Static Control

- *Lexmark Int'l, Inc. v. Static Control Components, Inc.*,
 - No. 02-571-KSF (E.D. Ky. Feb. 27, 2003)
(preliminary injunction granted), *appeal pending*, No. 03-05400 (6th Cir.).
- Lexmark adds microchips and software to some of its toner cartridges, which the printer queries on start-up and other times



Lexmark v. Static Control

- “Are you a Lexmark cartridge?”
 - » Authentication, using 6 codes stored in each cartridge chip
 - » If authentication succeeds, Toner Loading Program downloaded to printer and checksum performed
 - » L XK ticker symbol (ASCII 4C 58 4B) embedded (“salted”) in Toner Loading Program in chips attached to toner cartridges



Lexmark v. Static Control

- Static Control Components makes remanufactured toner cartridge components, including parts to remanufacture Lexmark cartridges
 - SCC's chip includes copies of all of Lexmark's chip-based software



Lexmark Case Holding

- Lexmark's software protected by copyright, despite relatively small size (37 bytes, 55 bytes) and slight originality and creativity
 - SCC argues slavish copying because of complexity of Lexmark's original, but it is still copying, and thus an infringement
 - L XK ticker symbol embedded in Toner Loading Program was a marker, not a lock-out code, so it proves infringement because SCC did not have to copy it
 - Court concludes that SCC could have written non-infringing software to make SCC's chips work, but failed to write new software



Lexmark Case Holding

- SCC also violated DMCA's anti-circumvention provisions at 17 USC § 1201(a)(2) and anti-trafficking provisions at § 1201(b)
 - Even if SCC's copying of the software did not infringe, the point of the copying was to circumvent the authentication ACT
 - » Is this circular logic?: The software is used as an ACT, so copying the software circumvented ACT used to protect a copyrighted work, namely itself
 - Limited reverse engineering exception did not help as SCC did not have an independent computer program to interoperate with Lexmark's software



Chamberlain v. Skylink

- *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*
- Chamberlain makes garage door openers (“GDOs”), with “rolling code” technology, which change the code transmitted to the GDO each time the transmitter button is pressed
- Skylink makes replacement transmitters, including one that replaces rolling code transmitters
 - » Mimics “resynchronization” of rolling codes



Chamberlain Holding

- Rolling code technology may be an “access control technology” for DMCA purposes
- Insufficient discovery creates several disputes of material facts
 - » Plaintiff’s failure to promptly provide source code for its GDOs to defendant creates dispute about whether plaintiff’s software is protected by copyright law, which is an element of § 1201(a)(2)
 - » Open issue of whether plaintiff expressly or implicitly permits customers to purchase and use third party transmitters, such as the one made and sold by defendant



Then v. Now: Technology

- Then (Copy Protection, ~1980s):
 - Content limited to delivery format
 - Cost of copying device is high
 - Cost of each copy is high
 - Copying is difficult
 - Anti-copying technology doesn't work ("copy protection")
- Now (Technological Protection Measures, ACT):
 - Content formats easily converted
 - Cost of copying device is low
 - Cost of each copy is low
 - Copying is easy
 - Anti-copying technology mostly (not always) works ("TPM" and "ACT")



Then v. Now: Contracts

- Then (Copy Protection):
 - “Shrinkwrap” contracts on outside of boxes, then move inside the box
 - Small number of shrinkwrap cases
 - Online signatures in question
 - » Utah law specifies encryption
 - Software Licensing Enforcement Act (SLEA) passed in 2 states
 - *Vault v. Quaid* guts SLEA, ignores shrinkwrap
- Now (TPMs, ACT):
 - “Clickwrap” agreements online, and when software installed
 - Larger number of clickwrap cases
 - Online signatures enforceable (UETA, E-Sign)
 - UCITA passed in 2 states; others pass bomb shelter acts
 - Many cases uphold clickwraps as agreements *signed* by the users



Then v. Now: DRM Laws

- Then (Copy Protection):
 - No law prohibits breaking security (copy protection)
 - May only sue for making infringing copies
 - Reverse engineering, fair use allowed
 - » Copyright Act's fair use provision pre-empts SLEA
- Now (TPMs, ACT):
 - Law prohibits breaking security (TPM)
 - Can sue for making infringing copies, & sue for breaking the TPM
 - Reverse engineering, fair use restricted or inapplicable
 - » Copyright Act's fair use provision not applicable



Then v. Now: *Vault v. Lexmark*

- *Vault v. Quaid* (1988)
 - Secret code that prevents software copying discovered by reverse engineering
 - No trade secret misapprop. for reverse engineering
 - Some copying, but no copyright infringement as only 30 characters copied
 - Contractual restriction on reverse engineering unenforceable
- *Lexmark v. SCC* (2003)
 - Secret codes that prevent competing toner cartridge discovered by reverse engineering
 - No trade secret misapprop. for reverse engineering
 - Lexmark's code copied 1:1
 - » Copyright infringement
 - Circumvention of ACT a separate violation, regardless of right to reverse engineer



In Process

- More bills pending in Congress and state legislatures
- Copyright Office exemption determinations
- DMCA spans the globe
 - » U.S. Bilateral agreements, e.g., Singapore Free Trade Agreement, Chile Free Trade Agreement, Central American Free Trade Agreement <<http://www.ustr.gov>> (visited April 15, 2005)
 - » European Union Directive 2001/29/EC (“Copyright Directive”) (May 22, 2001)
<http://europa.eu.int/information_society/topics/multi/digital_rights/doc/directive_copyright_en.pdf>
- Increased use of law to reduce, strangle competition
 - » Add a little bit of encryption, and a thimbleful of software, to get a cause of action against your competitors



Fred Wilf
Special Counsel

Technology, intellectual property
and business matters

fwilf@morganlewis.com
215.963.5453



Morgan, Lewis & Bockius LLP • 1701 Market Street • Philadelphia, PA 19103-2921

Boston Brussels Chicago Frankfurt Harrisburg Irvine London Los Angeles Miami New York
Northern Virginia Palo Alto Philadelphia Pittsburgh Princeton San Francisco Tokyo Washington