Loyola of Los Angeles Entertainment Law Review

Volume 25
Number 1 *Symposia—At the Crossroads of Law & Technology: Fifth Annual Conference, Alternative Methods for Protecting Digital Content and Gamer Technology Conference*

Article 1

1-1-2005

Introduction: At the Crossroads of Law and Technology

Karl Manheim

FIFTH ANNUAL CONFERENCE AT THE CROSSROADS OF LAW & TECHNOLOGY

INTRODUCTION

Karl Manheim[*]

At the Crossroads of Law & Technology is the descriptive title of an annual conference sponsored by the Program for Law & Technology at California Institute of Technology and Loyola Law School. Started in 1999, the conference explores emerging technology issues that have profound impact on the law.[1] Previous conferences have involved jurisdiction in cyberspace and the patenting of individual human genomes. This year's conference looked at the protection of digital broadcast media, both from a technology feasibility standpoint and its intellectual property implications. Because the subject matter overlapped with the annual conference sponsored by the *Loyola Entertainment Law Symposium*, we combined the two events in 2004.

The focal point of the *At the Crossroads* conference is a mock trial where the technology and legal issues are joined in a hypothetical, but realistic, case. The trial, set before a real federal judge, is accompanied by panels of academic and industry experts who explain and debate the underlying issues. The topic for 2004 was the emerging field of Digital Rights Management (DRM)—technological and legal protection for digital information, specifically as it is applied to digital television broadcasts.[2] In our mock case, *United States v. Baltimore*, video content providers (i.e., the en-

[*] Professor of Law, Loyola Law School, and Co-Director, Program for Law & Technology at California Institute of Technology and Loyola Law Schoool.

1. The Program was inspired and facilitated by Dr. Henry C. Yuen, a joint alumnus of the California Institute of Technology (Caltech) and Loyola Law School.

2. *See* C.J. Alice Chen & Aaron Burstein, *Symposium: The Law And Technology Of Digital Rights Management: Foreword*, 18 BERKELEY TECH. L.J. 487 (2003) ("Generally speaking, DRM systems consist of 'secure packaging and delivery software designed to prevent purchasers and third parties from making unauthorized uses of digital works.' In other words, DRM systems provide a means of expressing usage rules, a means of associating those rule with content, and frequently, a means of enforcing these rules by preventing actions that the usage rules do not explicitly permit").

tertainment industry) persuaded the federal government to bring a criminal prosecution against students, a teacher, and university administration for teaching and facilitating the "circumvention" of digital content protection technologies used in digital TV.

Starting July 1, 2005, all consumer electronic devices capable of receiving digital video broadcasts (e.g., TVs, cable and satellite receivers, digital video recorders)[3] sold in the United States must recognize and implement a form of DRM known as "Digital Broadcast Television Redistribution Control."[4] The particular tool approved by the FCC is called the "broadcast flag."[5] The flag is a coded signal embedded in video broadcasts that contains a set of "permissions" set by the content owner (copyright holder or licensee). These permissions govern such things as when the content can be watched and how many times, whether it can be copied (e.g., by Tivo) or re-transmitted (say, within a home network). The flag determines whether the encrypted content which it accompanies can be decrypted, so as to make it viewable.[6]

What this means for consumers is simple, albeit unknown to most of us. The television broadcast that comes over the air may be as fleeting as the wave that carries it, just as in the days before time shifting devices such as VCRs. Sure, you can record a program, but that doesn't mean you'll be able to view it; you may only be able to view it once, or view it only until the weekend. It would be as if the books you bought self-destructed after the first read. Just try to loan them to a friend, or sell them used on eBay. And don't save those books for summer reading; the ink lasts only a few days.

Content providers have been keen on the broadcast flag for years, as a way to control downstream use (and misuse) of their copyrighted content. But, no one would voluntarily pay more for a receiving device[7] that limited their ability to watch broadcast programs. So, the FCC came to the entertainment industry's rescue by mandating the inclusion of flag chips in re-

3. *See* Report and Order, *In the Matter of Digital Broadcast Content Protection*, FCC-03-273 (Nov. 4, 2003), at ¶ 57. These are known as "demodulator products." *Id.* at ¶ 42.

4. *See* 47 C.F.R. 73 (2005).

5. The broadcast flag is also known as the ATSC flag. ATSC stands for Advanced Television Standards Committee, the consortium that developed technical standards for digital high-definition television (HDTV). The flag uses a variation of Digital Transmission Content Protection (DTCP) that was developed by the ad hoc "5C" group of consumer electronics companies: Hitachi, Intel, Matsushita, Sony and Toshiba Corporations. *id.*

6. In technical terms, the flag employs both content encryption and copy control information (CCI).

7. To be implemented, the broadcast flag requires extra hardware and software in receiving devices.

ceiving devices sold after July 1, 2005. From that point forward, every piece of equipment containing a "demodulation device" (i.e., tuner), will control the viewing of flagged broadcasts, pursuant to the DRM permissions set by the flag.

The broadcast flag is enforced practically and legally by several recent actions of the federal government. The first was Congress' plan to phase out analog broadcast television in the United States (familiar VHF and UHF broadcasts) and replace it entirely by digital TV in 2007. This transition plan is reinforced by the expiration of analog broadcast licenses[8] and the FCC's requirement that, beginning Jan. 1, 2005, new television sets contain digital tuners.[9]

Under the Digital Millennium Copyright Act (DMCA), it is illegal to "circumvent" (i.e., hack) effective Technological Protection Measures (TPMs), such as the broadcast flag. The DMCA provides both civil and criminal penalties for circumvention activities, and for teaching how to do so. The underlying goal was to protect copyrighted material from illegal copying, which has become nearly a fact of life in the digital age.[10]

The entertainment industry, including the Recording Industry of America (RIAA) and the Motion Picture Association of America (MPAA), has taken an aggressive stand both against actual copyright infringement and against TPM circumvention.[11] Many contend the DMCA stifles innovation and discourages legitimate uses of digital content. For instance, it is illegal to circumvent an effective TPM even if the underlying digital content isn't legally protected. As would be the case if the underlying content was not copyright protected or if the user had a right to the material.[12]

Notorious cases of hacking and DMCA prosecutions have created an

---

8. *See* 47 U.S.C. 309(j)(14)(A) (2000) ("A television broadcast license that authorizes analog television service may not be renewed to authorize such service for a period that extends beyond December 31, 2006.") (added by Balanced Budget Act of 1997).

9. *See* In the Matter of Review of the Commission's Rules and Policies Affecting the Conversion to Digital Television, 17 F.C.C. R. 15978, 15978-79 (2002).

10. In addition to the DMCA, a wide variety of other laws provide penalties for violating intellectual property rights. *See generally* Computer Crime and Intellectual Property Section, *Criminal Intellectual Property Laws*, http://www.usdoj.gov/criminal/cybercrime/iplaws.htm (May 22, 2001).

11. *See, e.g.*, 321 Studios v. MGM Studios, Inc., 307 F. Supp. 2d 1085 (N.D. Cal, 2004) (civil action under the DMCA against creator of DVD copying program); Recording Industry Ass'n Of America v. Verizon Internet Serv., 257 F. Supp. 2d 244 (D.C. 2003) (upholding discovery order against Internet service provider, seeking the identity of anonymous users downloading music titles).

12. The DMCA is not limited to traditional copyrighted literary works; it can also be used to protect technology copyrights. *See, e.g.*, Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004) (functional software code not infringed).

uncertain environment and cultural divide when it comes to protecting digital content. For instance, Norwegian programmer, Jon Johansen, became an overnight folk hero with his "DeCSS" program that decodes the Content Scrambling System used by DVD manufacturers. He was twice acquitted by Norwegian courts of charges similar to those covered by the DMCA.[13] More recently, Johansen cracked the iTunes anti-copying program, MPEG-4 Advanced Audio Coding,[14] and posted his new program, "QTFairUse," on his web site "So sue me."[15]

DMCA criminal charges have been brought against Russian programmer Dmitry Sklyarov and his employer ElcomSoft for conspiracy, trafficking, and marketing of software that circumvented electronic "vouchers" in Adobe Acrobat digital eBooks.[16] Princeton University Professor Edward Felten took preemptive action against the DMCA after he was threatened with prosecution for lecturing about access control technologies.[17] Efforts to strengthen or supplement the DMCA at both the state and federal level are underway, through what are known as "Super DMCA" laws.[18]

As these cases illustrate, the DMCA has been especially controversial in academic settings. The intersection of this law and the technology mandate of the broadcast flag provided an excellent backdrop for the Fifth Annual *At the Crossroads* conference.

This was the first mock case in the Program's history to involve a criminal prosecution. It was made all the more lively by the faux criminal charges brought against Daniel Baltimore, president (and Nobel laureate) of Calculating Institute of Technology, for condoning and encouraging the teaching of circumvention technologies at CalTech.[19]

---

13. Norwegian Criminal Code section 145 (2). *See* Thomas Rieber-Mohn, *Court of Appeal Decision in Norwegian DVD case*, http://merlin.obs.coe.int/iris/2004/3/article29.en.html. (last visited Feb. 12, 2005).

14. Johansen uses a simple Windows command line utility that installs a DLL to dump the output of a QuickTime stream to file. The C program is called "QuickTime for Windows AAC memory dumper."

15. *See* Jon Lech Johansen, *So Sue Me, at* http://www.nanocrew.net/blog (Nov. 16, 2004).

16. *See, e.g.*, United States v. Elcom Ltd., 203 F. Supp. 2d 1111 (N.D. Cal. 2002).

17. *See* Felten v. RIAA, No. 01 CV 2669 (D. N.J. Nov. 28, 2001). The case was dropped after assurances were made by the government and recording industry that "threats against Felten were ill-conceived and will not be repeated." *See* Electronic Frontier Foundation, *EFF Media Release: Felten Drops RIAA Case, at* http://www.eff.org/IP/DMCA/Felten_v_RIAA (last visited Feb. 12, 2005).

18. For a catalog of state efforts, *see* Electronic Frontier Foundation, *State-Level "Super DMCA" Initiations Archive, at* http://www.eff.org/IP/DMCA/states/

19. Any resemblance to California Institute of Technology (Caltech) and its esteemed president, Dr. David Baltimore, is purely coincidental.

In addition to the headliner, other fictitious defendants included Dr. Stephen Law, a professor at CalTech, whose class on encryption provided the groundwork for student John Johnson's class project in TPM circumvention.[20] The fruits of that project were posted on Professor Law's website, hosted by CalTech. In the mock case, Johnson pioneered the use of distributed "brute force" computing to parcel out bits and pieces of code and algorithm to thousands of like-minded individuals around the globe.[21] In concert, these anonymous hackers were able to decode a sample "copy control" mechanism. To ascertain the vitality of the decryption method, Prof. Law posted a few seconds of video that had been encoded with "5C" encryption, the same as used in the Broadcast Flag.[22] It too was successfully decrypted.

When CalTech declined MPAA's request that Prof. Law's website be dismantled, and forbade him from teaching circumvention techniques, charges were filed against the university, its president, Johnson and Law. Defendants resisted the charges by bringing a motion to dismiss the indictment on two grounds. They first argued that 5C technology is readily susceptible to hacking. As a result, the Broadcast flag is not covered by the DMCA, because the law applies only where content is effectively controlled by a technological measure, which has been circumvented.[23] They next argued that their activities, occurring in an educational context, were protected by the First Amendment.

The case was filed and the motion heard in the United States District Court for the Western District of California, Judge Ronald S.W. Lew, presiding.[24] The prosecution team consisted of two students from Caltech (Iram Parveen Bilal and Meng-Meng Fu) and two from Loyola (John Egly and Michael Matoba). The defense was also comprised of two Caltech students (Rachel Medwood and Graham Yoakum) and two Loyola students (Benjamin Shapiro and Emily Wada). Judge Lew was assisted by Toby

20. Further apologies to Dr. Stephen Low, an advisor to The Program for Law & Technology, and to Jon Johansen, the creator of DeCSS, the program that hacked the Content Scramble System (CSS), used to encrypt Digital Versatile Disks (DVDs). Mr. Johansen has twice been acquitted by a Swedish court of violating that nation's copyright laws.

21. This is the idea behind SETI@Home and other distributive computational programs that run in the background on linked computers.

22. *See supra* note 5.

23. 17 U.S.C. § 1201(a)(3)(B) (1999). In an analogous context, a federal court recently ruled that a simple encryption technology was not protected by the DMCA, because "it did not effectively protect[] the right of [the] copyright owner." Agfa Monotype Corp. v. Adobe Systems, No. 02 C 6320 (ND Ill, Jan. 13, 2005).

24. Although Judge Lew is a real Federal District Judge (C.D. Cal.), the Western District of California is the fictitious venue for mock cases of the Program for Law & Technology.

Huong (Caltech) and Phillip Stuller (Loyola), who served as law clerks.

While the students do all the hard work for the mock trial, practicing lawyers provide backup assistance and essential resources. This year, we were fortunate to have major players in the actual controversy on board. Assisting the prosecution team were Arif Alikhan, from the US Attorney's Office in Los Angeles, and James Spertus, a staff attorney for the MPAA. Assisting the defense were Fred von Lohmann, senior staff attorney for the Electronic Frontier Foundation (EFF), and Robert Corbin and Michael Fitzgerald (Corbin & Fitzgerald), whose practice includes criminal defense of DMCA cases. Appearing as an expert witness for the prosecution was C. Bradley Hunt, Senior Vice President & Chief Technology Officer, for the MPAA. His counterpart, for the defense, was Seth David Schoen, Staff Technologist for the EFF. Finally, Stephen Low (Caltech) and Bry Danner (Southern California Edison), provided technical and overall direction to this year's program.

As this introduction may illustrate, the technical and legal issues are often complex. Neither technologists nor lawyers are usually versed in the other's discipline. Hence, the principal mission of the Program for Law & Technology is to bridge this gap by introducing law students on the one hand, and science and engineering students on the other, to each other's language and modes of action. While the mock trial is the centerpiece of the annual conference, it is usually helpful both to participants and the invited audience to provide background tutorials and discussion panels on the technology and legal issues.

This year's conference included panels on DRM and the DMCA. Dan L. Burke (Professor, University of Minnesota Law School) provided the legal background, while Brad Hunt and Seth Schoen continued their expert debate on technology issues. A third panel, on Alternate Methods for Protecting Digital Content, included a lively discussion by Fred von Lohmann (EFF) and Ronald C. Wheeler (Senior Vice President for Content Protection, Fox Entertainment Group). We were very fortunate to have such prominent individuals continue the essential debate as part of this year's Program.

Following this introduction, you will find the transcript for the mock trial, including the truly expert testimony. Next is Judge Lew's Opinion in the case (the Loyola of Los Angeles Entertainment Law Review is the official reporter for the Program for Law & Technology). The final piece in this symposium is the panel transcript on Alternative Methods of Protecting Digital Content. Taken as a whole, you will find that these make significant headway into the problem of content protection in the digital age, even though the contesting sides are still far apart on the appropriate legal and

technological protections that should be used.

I want to thank all of the participants in this year's *At the Crossroads* conference, and especially my colleagues Jay Dougherty (Loyola) and Ed McCaffery (Caltech) who, as usual, provided the inspiration for another successful conference.