Technological Protection Systems for Digitized Copyrighted Works: A Report to Congress

I. INTRODUCTION

A. Background

On November 2, 2002, the President signed into law the "Technology, Education and Copyright Harmonization Act of 2002" (the TEACH Act), which updates certain provisions of the Copyright Act to facilitate the growth and development of distance education, while introducing new safeguards to limit the additional risks to copyright owners that are inherent in exploiting works in a digital format.[1] For information purposes only, the TEACH Act requires the United States Patent and Trademark Office (USPTO), after consultation with the Register of Copyrights, to submit a report to Congress on technological protection systems to protect digitized copyrighted works and to prevent infringement, including those being developed in private, voluntary, industry-led entities through an open broad-based consensus process.

Over the last several years, the educational opportunities and risks associated with distance education have been the subject of extensive public debate and attention in the United States. In November 1998, the Conference on Fair Use (CONFU), convened by the Administration's Information Infrastructure Task Force, issued its final report, which included a proposal for educational fair use guidelines for distance learning.[2] Following the enactment of the Digital Millennium Copyright Act of 1998 (DMCA),[3] the Copyright Office was tasked with preparing a study of the complex issues involved in distance education and to make recommendations to Congress for any legislative changes. In May 1999, the Copyright Office issued an extensive report on copyright and digital distance education.[4] After hearings before the Senate Judiciary Committee (March 13, 2001) and before the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property (June 27, 2001), Congress passed the TEACH Act as part of the "21st Century Department of Justice Appropriations Authorization Act."

---

[1] Pub. L. No. 107-273, 116 Stat. 1758 (Nov. 2, 2002).

[2] *See* The Conference on Fair Use: Final Report to the Commissioner on the Conclusion of the Conference on Fair Use (U.S. Patent and Trademark Office, November 1998). The report is available at: http://www.uspto.gov/web/offices/dcom/olia/confu/confurep.htm

[3] Pub. L. No. 105-304, 1122 Stat. 2860 (Oct. 28, 1998).

[4] *See* Report on Copyright and Digital Distance Education: A Report of the Register of Copyrights (U.S. Copyright Office, May 1999). The report is available at: http://www.copyright.gov/disted.

B. Overview of the TEACH Act

Subsection (b) of the TEACH Act amends section 110(2) of the Copyright Act to allow for the inclusion of performances and displays of copyrighted works in digital distance education under appropriate circumstances and subject to certain limitations. The Act expands the categories of works exempt from the performance right in section 106(4) of the Copyright Act, from nondramatic literary works and musical works to "reasonable and limited portions" of any work and permits the display of any work in "an amount comparable to that typically displayed in the course of a live classroom setting." The Act removes the concept of the physical classroom, while maintaining the requirement of "mediated instructional activity," which generally requires the involvement of an instructor. The exemption is limited to mediated instructional activities that are conducted by governmental bodies and "accredited" non-profit educational institutions. Subsection (c) of the TEACH Act amends section 112 of the Copyright Act to permit transmitting organizations to store copyrighted material on their servers in order to allow the performances and displays of works authorized under amended section 110(2).

The TEACH Act contains a number of new safeguards to limit the additional risks to copyright owners that are inherent in using works in the digital format. The Act limits the receipt of authorized transmissions to students officially enrolled in the course or to Government employees as part of their official duties "to the extent technologically feasible." With respect to "digital transmissions," transmitting institutions must apply technological measures that reasonably prevent "retention of the work in accessible form by recipients of the transmission … for longer than the class session" and "unauthorized further dissemination of the work in accessible form by such recipients to others." The statute also prohibits transmitting institutions from engaging in "conduct that could reasonably be expected to interfere" with technological measures used by copyright owners to regulate the retention and further unauthorized dissemination of protected works.

C. The USPTO Report

Subsection (d) of the TEACH Act requires the Under Secretary of Commerce for Intellectual Property, after consultation with the Register of Copyrights, and after a period for public comment, to submit to the Committees on the Judiciary of the Senate and the House of Representatives a report on technological protection systems to protect digitized copyrighted works, including those being developed in private voluntary industry-led entities through an open broad-based consensus process. The report, which is intended solely to provide information to Congress, is due not later than 180 days after the date of enactment of the Act.

Congress specifically directed the USPTO to include information "on technological protection systems that have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works

and prevent infringement, including upgradeable and self-repairing systems, and systems that have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad based consensus process." Congress also directed the USPTO to exclude "any recommendations, comparisons, or comparative assessments of any commercially available products that may be mentioned in the report."

Subsection (d) of the Act further states that the report "shall not be construed to affect in any way, either directly or by implication, any provision" of the Copyright Act in general or the TEACH Act in particular, including the requirement of transmitting institutions to apply certain technological controls and not to engage in conduct that could be reasonably expected to interfere with technological measures used by copyright owners (discussed more fully above), or "the interpretation or application of such provisions, including evaluation of the compliance with that clause by any governmental body or nonprofit educational institution."

Finally, the legislative history of the TEACH Act sheds some light on the purpose, benefits and possible limitations of the USPTO report. Some lawmakers noted that a report on technological protection systems would "only provide a snapshot in time," while others noted that such a report would be "out of date by the time it is finished due to continual advances in technology."[5] In preparing this study, USPTO became well aware of these inherent difficulties. Nonetheless, Congress also noted that such a study could be "useful in establishing a baseline of knowledge for the Committee and our constituents with regard to what technology is or could be made available and how it is or could be implemented."[6] In that spirit, this report is respectfully submitted to Congress.

D. Public Comments and Public Hearing

Under the TEACH Act mandate, and to assist in the preparation of the report, on December 4, 2002, USPTO solicited written comments from interested parties and scheduled a public hearing on February 4, 2003.[7] Written comments were due January 14, 2003. In particular, USPTO requested information in response to the following questions:

(1) What technological protection systems have been implemented, are available for implementation, or are proposed to be developed to protect digitized copyrighted works and prevent infringement, including any upgradeable and self-repairing systems?

(2) What systems have been developed, are being developed, or are proposed to be developed in private voluntary industry-led entities through an open broad-based consensus process?

---

[5] Congr. Rec. S5991 (June 7, 2001).
[6] Id.
[7] 67 Fed. Reg. 72,920.

(3) Consistent with the types of information requested by Congress, please provide any additional comments on technological protection systems to protect digitized copyrighted works and prevent infringement.

In response to these questions, USPTO received written comments from the following organizations: Infraworks Corporation; Blue Spike, Inc; Macrovision Corporation; OverDrive, Inc.; ContentGuard; Copyright Clearance Center, Inc.; NDS Americas, Inc.; 4C Entity, LLC; Protexis, Inc.; Association of American Universities; The Walt Disney Company; Digimarc; Motion Picture Association of America, Inc.; Software & Information Industry Association; Digital Transmission Licensing Administrator, LLC; and Information Technology Industry Council. Copies of the public comments are available on the USPTO web site at http://www.uspto.gov.

On February 4, 2003, USPTO conducted a public hearing to assist in the preparation of the TEACH Report. The following persons testified: Mr. William Krepick, President and Chief Executive Officer, Macrovision Corporation; Mr. Steven Potash, Chief Executive Officer, OverDrive, Inc.; Mr. Michael Miron, Chief Executive Officer, ContentGuard; Mr. Troy Dow, Vice President & Counsel, Technology & New Media, Motion Picture Association of America, Inc.; Mr. Bruce Funkhouser, Vice President of International and Business Operations, Copyright Clearance Center, Inc.; and Mr. Mark Bohannon, General Counsel and Executive Vice President, Government Affairs, Software & Information Industry Association. A transcript of the hearing is available on the USPTO web site at http://www.uspto.gov.

II. TECHNOLOGICAL PROTECTION SYSTEMS

A. Introduction

The 1996 World Intellectual Property Organization (WIPO) Copyright Treaty (WCT) and the WIPO Performances and Phonograms Treaty (WPPT) (collectively the WIPO Treaties) require signatories to provide "adequate legal protection and effective legal remedies against the circumvention of effective technological measures."[8] The U.S. legislation implementing the WIPO Treaties, the 1998 Digital Millennium Copyright Act (DMCA),[9] generally divides technological measures into measures that prevent unauthorized *access* to a copyrighted work and measures that prevent infringement of a work. Although the term technological protection system is not defined in the TEACH Act or in the DMCA, it is generally used in this report to refer to a range of technological methods to control unauthorized access to and copying of digitized

[8] WIPO Copyright Treaty ("WCT"), Article 11, adopted December 20, 1996, WIPO Doc. CRNR/DC/94; WIPO Performances and Phonograms Treaty ("WPPT'), Article 18, adopted December 20, 1996, WIPO Doc. CRNR/DC/95; Agreed Statements Concerning the WIPO Copyright Treaty, adopted December 20, 1996, WIPO Doc. CRNR/DC/96. The Treaties also require adequate legal protection and effective legal remedies for the protection of the integrity of copyright management information. WCT, Art. 12; WPPT, Art. 19.

[9] Pub. L. No. 105-304.

copyrighted works. This section briefly introduces some of the core technologies that underlie such technological protection systems.[10]

B. Core Technologies

1. Encryption

Encryption is a process that "scrambles" data using sophisticated mathematical equations in order to protect it and keep it private. In very general terms, encryption algorithms convert human readable data, such as a word processor document, into encrypted or scrambled data. The encrypted data can be made readable again by decrypting it with a corresponding decryption key. If the decryption key is given only to authorized parties and if the encryption algorithm used is sufficiently strong, unauthorized access to the data by the casual user is prevented. The whole point of encryption is that an encrypted work cannot easily be manipulated without authorization. A secret key or pair of keys, as discussed more fully below, is required for the encryption or decryption of the scrambled file. Encryption technology can be used to protect data and works transmitted over computer networks (such as e-mail and database information), or more broadly in connection with other information delivery systems, including telephone, satellite and cable communications.

Broadly speaking, encryption algorithms may be characterized either as "secret key" encryption (sometimes called "symmetric key" encryption) and "public key" encryption (or, "asymmetric key" encryption). Secret key encryption involves the use of a single key to encrypt and to decrypt the content. A common example of the use of secret key encryption to control access to content is pay-per-view television. In this illustration, the television program is encrypted using the secret key, and only paying customers have access to the secret key. Of course, as its name suggests, the successful application of secret key encryption to protect copyrighted works depends on keeping the key secret. Wide distribution of the secret key to numerous parties may result in compromising such a technological protection system. Thus, public key encryption, as explained below, is generally used as for distribution of content to a wide audience.

Public key encryption uses an algorithm requiring two keys – a "public" key and a "private" key. The data is encrypted using the public key, which is then made widely available to the public. The private key is kept secret by individuals. The fundamental point is that the encrypted content or secret message can only be decrypted using the corresponding private key. For example, a copyright owner could encrypt a work using the public key of the intended recipient. Once the recipient receives the encrypted transmission, he or she could use the private key to decrypt the transmission. No private keys need to be exchanged in this transaction. Without the private key of the intended

---

[10] For an earlier introduction to these technologies, *see* Information Infrastructure Task Force, Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights (1995). For a more recent survey of these technologies, s*ee* "Protecting Digital Intellectual Property," Chapter 5, in Committee on Intellectual Property Rights and the Emerging Information Infrastructure, National Research Council, Computer Science and Technology Board, *The Digital Dilemma: Intellectual Property in the Information Age* (1999).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.