

MAIN MENU:

[CALENDAR](#)[SYLLABUS](#)[DISCUSSION](#)[ADMINISTRATION](#)

NOTICES:

Copyright in Cyberspace III: The DMCA

READINGS

The Digital Millennium Copyright Act (DMCA), enacted in late 1998, modified the US Copyright Law in several ways, two of which are especially relevant to our discussion here:

Title II, the "Online Copyright Infringement Liability Limitation Act," creates limitations on the liability of online service providers for copyright infringement when engaging in certain types of activities.

Title I of the DMCA implemented provisions relating to World Intellectual Property Organization (WIPO) treaties signed in 1996 (as part of the Uruguay Round of GATT negotiations). These provisions established two new prohibitions under Federal Copyright Law -- one on circumvention of technological measures used by copyright owners to protect their works and one on tampering with copyright management information -- and adds civil remedies and criminal penalties for violating the prohibitions. (This portion of the DMCA is called the "WIPO Copyright and Performances and Phonograms Treaties Implementation Act of 1998".)

Of the two provisions, the anti-circumvention provisions have been extremely controversial. In part because of this, the limitations on liability provisions have gone relatively unnoticed. Yet, as we'll see below, these sections of the statute are quite important in a number of ways.

We'll consider these provisions in turn, and review their impact on eCommerce.

Limitations on Liability for Online Service Providers

In preparation for our discussion, read the following:

[17 U.S.C. § 512 \(2001\)](#)

[Hendrickson v eBay, Inc., 2001 US Dist. LEXIS 14420 \(C.D. Cal. Sept. 4, 2001\)](#) [pdf, 40 kb, edited]

[eBay, Verified Rights Owner \(VeRO\) Program™: Protecting Intellectual Property \(2001\)](#)

Consider the following:

Why do you think that Congress passed the "safe harbor" provisions of the DMCA? What problem were they trying to address?

How do the "safe harbor" provisions work -- what is the order of activity? What happens if the service provider fails to seek the safe harbor? (Do you think many providers will do this?)

The Hendrickson case considers the scope of the "notice" that must be given to trigger the takedown provisions. Do you think the court got it right? As a matter of law? As a matter of policy?

Should we be concerned about the safe harbor provisions? Can it be moused by either the content owners or the providers?

Anti-Circumvention and Anti-Tampering Measures

Broadly speaking, this portion of the DMCA makes persons who circumvent "copyright management systems" ("CMS") (i.e., the "trusted systems" we discussed earlier in the course), create "devices" which circumvent CMS, or distribute devices which circumvent CMS, subject to criminal and civil liability.

As an initial matter, one might wonder why such an important (and expansive) set of new prohibitions was enacted as a part of an international treaty, rather than being brought through the normal course of Federal Legislation. Why do you think this was the case?

In preparation for our discussion, read the following:

[17 U.S.C. § 1201 \(2001\)](#) (anti-circumvention)

[17 U.S.C. § 1202 \(2001\)](#) (anti-tampering)

[Universal City Studios v. Reimerdes, 55 U.S.P.Q.2D 1873 \(S.D.N.Y. 2000\)](#) [pdf, 32 kb, edited]

[Pamela Samuelson, Anticircumvention Rules: Threat to Science, 293 Science 2029 \(Sept. 14, 2001\)](#) [pdf, 80 kb]

[Roger Parloff, Free Dmitry? Spare Me.: Why the FBI Was Right to Arrest the Internet's Latest Martyr, Inside, August 1, 2001.](#) [pdf, 20 kb]

Consider the following:

1. **Fair Use and Anticircumvention.** One of the most significant holdings in the Reimerdes case is the denial of a "fair use" justification for circumvention. Do you think the Reimerdes court got it right on this holding? As a matter of the law? Policy? That is, **should** fair use be a justification for circumvention?

2. **Free Speech and Anticircumvention.** As can be seen in the discussion above, one avenue of challenge to the DMCA Anticircumvention provisions is the suggestion that they interfere with free speech. Because much of this question involves matters of First Amendment theory beyond the scope of this course, we'll only touch on it briefly in our discussion. Note, however, that the 2nd Circuit, after oral argument on the Reimerdes appeal, requested that the parties file supplemental papers discussing the following questions:

ORDER

The panel modifies the oral instruction for supplemental letter briefs in the captioned case, given at the close of the argument on May 1, 2001, by authorizing the parties and the Intervenor to augment their responses to no more than 25 pages, and inviting responses to the following questions:

1. Are the anti-trafficking provisions of the Digital Millennium Copyright Act content-neutral? See 111 F. Supp., 2d 294, 328-29 (S.D.N.Y. 2000).
2. Does DeCSS have both speech and non-speech elements?
3. Does the dissemination of DeCSS have both speech and non-speech elements?
4. Does the use of DeCSS to decrypt an encrypted DVD have both speech and non-speech elements?
5. Does the existence of non-speech elements, along with speech elements, in an activity sought to be regulated alone justify intermediate level scrutiny?
6. If DeCSS or its dissemination or its use to decrypt has both speech and non-speech elements and is not subject to intermediate level scrutiny simply because of the non-speech elements, is intermediate level scrutiny appropriate because of the close causal link between dissemination of DeCSS and its improper use? See 111 F. Supp. 2d at 331-32.
7. If the District Court is correct that the dissemination of DeCSS "carries very substantial risk of imminent harm" 111 F. Supp. 2d at 332, does that risk alone justify the injunction? In other words, does that risk satisfy the requirements for regulating speech under *Brandenburg v. Ohio*, 395 U.S. 444 (1969), thereby rendering unnecessary an inquiry as to whether non-speech elements of DeCSS or its dissemination or its use (if such exists) may be regulated under *United States v. O'Brien*, 391 US 367 (1968)?
8. Are the three criteria identified at 111 P. Supp. 2d 333 the correct criteria for determining the validity, under intermediate level scrutiny, of the use of DeCSS that has been enjoined?
9. If not, what modification or supplementation would be required to conform to First Amendment requirements?
10. Are the three criteria identified in 111 F. Supp. 2d 341 and the "clear and convincing evidence" standard the correct criteria and the correct standard of proof for testing the validity of the injunction's prohibition of posting on the defendant's website and of linking?
11. If not, what modification or supplementation would be required to conform to First Amendment requirements?

3. The Case For Anticircumvention Prohibitions. Although the view supporting the DMCA Anticircumvention provisions is not well represented in either the media or the legal commentary, there are at least two significant arguments in favor of these laws:

a. *Price Discrimination.* Under this theory, we should view the sorts of "trusted systems" that the Anticircumvention provisions support as a social benefit. Copyright law extends to content creators a limited monopoly; under traditional economic theory, the social costs of monopoly can be diminished by price discrimination (charging

individuals according to their reserve price, rather than a fixed-rate for all users). In the era of digital goods, price discrimination becomes even harder (and perhaps more important, as works get more broadly distributed) -- the ability to widely disseminate a digital work means that content owners will have to factor-in the costs of this distribution when selling the work itself, thereby raising the costs of the work for all involved. In a world where trusted systems are extant and legally supported, content owners will sell works much more cheaply, thereby increasing the distribution.

b. *The "Arms Race" Theory*. Under this theory, the Anticircumvention provisions are socially beneficial because they reduce or eliminate the costs of continuing a technological "arms race" between content owners and copiers / pirates. This argument recognizes that the content owners have the ability to create ever-stronger trusted systems, and these efforts will be met with ever-greater attempts to create software that will circumvent these systems. This race has the potential to be endless, and will certainly be costly. By resolving the 'race' in favor of the content creators, Congress has greatly reduces the social costs of digital distribution.

What do you think of these theories?

<

US Copyright Law

17 U.S.C. § 512 (Supp. 1999)

§ 512. Limitations on liability relating to material online

(a) Transitory Digital Network Communications.-A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections, if-

(1) the transmission of the material was initiated by or at the direction of a person other than the service provider;

(2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;

(3) the service provider does not select the recipients of the material except as an automatic response to the request of another person;

(4) no copy of the material made by the service provider in the course of such intermediate or transient storage is maintained on the system or network in a manner ordinarily accessible to anyone other than anticipated recipients, and no such copy is maintained on the system or network in a manner ordinarily accessible to such anticipated recipients for a longer period than is reasonably necessary for the transmission, routing, or provision of connections; and

(5) the material is transmitted through the system or network without modification of its content.

(b) System Caching.-

(1) Limitation on Liability.-A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the intermediate and temporary storage of material on a system or network controlled or operated by or for the service provider in a case in which-

(A) the material is made available online by a person other than the service provider;

(B) the material is transmitted from the person described in subparagraph (A) through the system or network to a person other than the person described in subparagraph (A) at the direction of that other person; and

(C) the storage is carried out through an automatic technical process for the purpose of making the material available to users of the system or network who, after the material is transmitted as described in subparagraph (B), request access to the material from the person described in subparagraph (A), if the conditions set forth in paragraph (2) are met.

(2) Conditions.-The conditions referred to in paragraph (1) are that-

(A) the material described in paragraph (1) is transmitted to the subsequent users described in paragraph (1)(C) without modification to its content from the manner in which the material was transmitted from the person described in paragraph (1)(A);

(B) the service provider described in paragraph (1) complies with rules concerning the refreshing, reloading, or other updating of the material when specified by the person making the material available online in accordance with a generally accepted industry standard data communications protocol for the system or network through which that person makes the material available, except that this subparagraph applies only if those rules are not used by the person described in paragraph (1)(A) to prevent or unreasonably impair the intermediate storage to which this subsection applies;

(C) the service provider does not interfere with the ability of technology associated with the material to return to the person described in paragraph (1)(A) the information that would have been available to that person if the material had been obtained by the subsequent users described in paragraph (1)(C) directly from that person, except that this subparagraph applies only if that technology-

(i) does not significantly interfere with the performance of the provider's system or network or with the intermediate storage of the material;

(ii) is consistent with generally accepted industry standard communications protocols; and

(iii) does not extract information from the provider's system or network other than the information that would have been available to the person described in paragraph (1)(A) if the subsequent users had gained access to the material directly from that person;

(D) if the person described in paragraph (1)(A) has in effect a condition that a person must meet prior to having access to the material, such as a condition based on payment of a fee or provision of a password or other information, the service provider permits access to the stored material in significant part only to users of its system or network that have met those conditions and only in accordance with those conditions; and

(E) if the person described in paragraph (1)(A) makes that material available online without the authorization of the copyright owner of the material, the service provider responds expeditiously to remove, or disable access to, the material that is claimed to be infringing upon notification of claimed infringement as described in subsection (c)(3), except that this subparagraph applies only if-

(i) the material has previously been removed from the originating site or access to it has been disabled, or a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled; and

(ii) the party giving the notification includes in the notification a statement confirming that the material has been removed from the originating site or access to it has been disabled or that a court has ordered that the material be removed from the originating site or that access to the material on the originating site be disabled.

(c) Information Residing on Systems or Networks at Direction of Users.-

(1) In General.-A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider-

(A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;

(ii) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(B) does not receive a financial benefit directly attributable to the infringing activity, in a case in which

the service provider has the right and ability to control such activity; and

(C) upon notification of claimed infringement as described in paragraph (3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.

(2) Designated Agent.-The limitations on liability established in this subsection apply to a service provider only if the service provider has designated an agent to receive notifications of claimed infringement described in paragraph (3), by making available through its service, including on its website in a location accessible to the public, and by providing to the Copyright Office, substantially the following information:

(A) the name, address, phone number, and electronic mail address of the agent.

(B) other contact information which the Register of Copyrights may deem appropriate.

The Register of Copyrights shall maintain a current directory of agents available to the public for inspection, including through the Internet, in both electronic and hard copy formats, and may require payment of a fee by service providers to cover the costs of maintaining the directory.

(3) Elements of Notification.-

(A) To be effective under this subsection, a notification of claimed infringement must be a written communication provided to the designated agent of a service provider that includes substantially the following:

(i) A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(ii) Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site.

(iii) Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material.

(iv) Information reasonably sufficient to permit the service provider to contact the complaining party, such as an address, telephone number, and, if available, an electronic mail address at which the complaining party may be contacted.

(v) A statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law.

(vi) A statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

(B)(i) Subject to clause (ii), a notification from a copyright owner or from a person authorized to act on behalf of the copyright owner that fails to comply substantially with the provisions of subparagraph (A) shall not be considered under paragraph (1)(A) in determining whether a service provider has actual knowledge or is aware of facts or circumstances from which infringing activity is apparent.

(ii) In a case in which the notification that is provided to the service provider's designated agent fails to comply substantially with all the provisions of subparagraph (A) but substantially complies with clauses (ii), (iii), and (iv) of subparagraph (A), clause (i) of this subparagraph applies only if the service provider promptly attempts to contact the person making the notification or takes other reasonable steps to assist in the receipt of notification that substantially complies with all the provisions of subparagraph (A).

(d) Information Location Tools.-A service provider shall not be liable for monetary relief, or, except as provided in subsection (j), for injunctive or other equitable relief, for infringement of copyright by reason of the provider referring or linking users to an online location containing infringing material or infringing activity, by using information location tools, including a directory, index, reference, pointer, or hypertext link, if the service provider-

(1)(A) does not have actual knowledge that the material or activity is infringing;

(B) in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or

(C) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;

(2) does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and

(3) upon notification of claimed infringement as described in subsection (c)(3), responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity, except that, for purposes of this paragraph, the information described in subsection (c)(3)(A)(iii) shall be identification of the reference or link, to material or activity claimed to be infringing, that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate that reference or link.

(e) Limitation on Liability of Nonprofit Educational Institutions.- (1) When a public or other nonprofit institution of higher education is a service provider, and when a faculty member or graduate student who is an employee of such institution is performing a teaching or research function, for the purposes of subsections (a) and (b) such faculty member or graduate student shall be considered to be a person other than the institution, and for the purposes of subsections (c) and (d) such faculty member's or graduate student's knowledge or awareness of his or her infringing activities shall not be attributed to the institution, if-

(A) such faculty member's or graduate student's infringing activities do not involve the provision of online access to instructional materials that are or were required or recommended, within the preceding 3-year period, for a course taught at the institution by such faculty member or graduate student;

(B) the institution has not, within the preceding 3-year period, received more than 2 notifications described in subsection (c)(3) of claimed infringement by such faculty member or graduate student, and such notifications of claimed infringement were not actionable under subsection (f); and

(C) the institution provides to all users of its system or network informational materials that accurately describe, and promote compliance with, the laws of the United States relating to copyright.

(2) For the purposes of this subsection, the limitations on injunctive relief contained in subsections (j)(2) and (j)(3), but not those in (j)(1), shall apply.

(f) Misrepresentations.-Any person who knowingly materially misrepresents under this section-

(1) that material or activity is infringing, or

(2) that material or activity was removed or disabled by mistake or misidentification,

shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it.

(g) Replacement of Removed or Disabled Material and Limitation on Other Liability.-

(1) No Liability for Taking Down Generally.-Subject to paragraph (2), a service provider shall not be liable to any person for any claim based on the service provider's good faith disabling of access to, or removal of, material or activity claimed to be infringing or based on facts or circumstances from which infringing activity is apparent, regardless of whether the material or activity is ultimately determined to be infringing.

(2) Exception.-Paragraph (1) shall not apply with respect to material residing at the direction of a subscriber of the service provider on a system or network controlled or operated by or for the service provider that is removed, or to which access is disabled by the service provider, pursuant to a notice provided under subsection (c)(1)(C), unless the service provider-

(A) takes reasonable steps promptly to notify the subscriber that it has removed or disabled access to the material;

(B) upon receipt of a counter notification described in paragraph (3), promptly provides the person who provided the notification under subsection (c)(1)(C) with a copy of the counter notification, and informs that person that it will re-place the removed material or cease disabling access to it in 10 business days; and

(C) replaces the removed material and ceases disabling access to it not less than 10, nor more than 14, business days following receipt of the counter notice, unless its designated agent first receives notice from the person who submitted the notification under subsection (c)(1)(C) that such person has filed an action seeking a court order to restrain the subscriber from engaging in infringing activity relating to the material on the service provider's system or network.

(3) Contents of Counter Notification.-To be effective under this subsection, a counter notification must be a written communication provided to the service provider's designated agent that includes substantially the following:

(A) A physical or electronic signature of the subscriber.

(B) Identification of the material that has been removed or to which access has been disabled and the location at which the material appeared before it was removed or access to it was disabled.

(C) A statement under penalty of perjury that the subscriber has a good faith belief that the material was removed or disabled as a result of mistake or misidentification of the material to be removed or disabled.

(D) The subscriber's name, address, and telephone number, and a statement that the subscriber consents to the jurisdiction of Federal District Court for the judicial district in which the address is located, or if the subscriber's address is outside of the United States, for any judicial district in which the service provider may be found, and that the subscriber will accept service of process from the person who provided notification under subsection (c)(1)(C) or an agent of such person.

(4) Limitation on Other Liability.-A service provider's compliance with paragraph (2) shall not subject the service provider to liability for copyright infringement with respect to the material identified in the notice provided under subsection (c)(1)(C).

(h) Subpoena to Identify Infringer.-

(1) Request.-A copyright owner or a person authorized to act on the owner's behalf may request the clerk of any United States district court to issue a subpoena to a service provider for identification of an alleged infringer in accordance with this subsection.

(2) Contents of Request-The request may be made by filing with the clerk-

(A) a copy of a notification described in subsection (c)(3)(A);

(B) a proposed subpoena; and

(C) a sworn declaration to the effect that the purpose for which the subpoena is sought is to obtain the identity of an alleged infringer and that such information will only be used for the purpose of protecting rights under this title.

(3) Contents of Subpoena.-The subpoena shall authorize and order the service provider receiving the notification and the subpoena to expeditiously disclose to the copyright owner or person authorized by the copyright owner information sufficient to identify the alleged infringer of the material described in the notification to the extent such information is available to the service provider.

(4) Basis for Granting Subpoena.-If the notification filed satisfies the provisions of subsection (c)(3)(A), the proposed subpoena is in proper form, and the accompanying declaration is properly executed, the clerk shall expeditiously issue and sign the proposed subpoena and return it to the requester for delivery to the service provider.

(5) Actions of Service Provider Receiving Subpoena.- Upon receipt of the issued subpoena, either accompanying or subsequent to the receipt of a notification described in subsection (c)(3)(A), the service provider shall expeditiously disclose to the copyright owner or person authorized by the copyright owner the information required by the subpoena, notwithstanding any other provision of law and regardless of whether the service provider responds to the notification.

(6) Rules Applicable to Subpoena.-Unless otherwise provided by this section or by applicable rules of the court, the procedure for issuance and delivery of the subpoena, and the remedies for noncompliance with the subpoena, shall be governed to the greatest extent practicable by those provisions of the Federal Rules of Civil Procedure governing the issuance, service, and enforcement of a subpoena duces tecum.

(i) Conditions for Eligibility.-

(1) Accommodation of Technology.-The limitations on liability established by this section shall apply to a service provider only if the service provider-

(A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and

(B) accommodates and does not interfere with standard technical measures.

(2) Definition.-As used in this subsection, the term "standard technical measures" means technical measures that are used by copyright owners to identify or protect copyrighted works and-

(A) have been developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process;

(B) are available to any person on reasonable and nondiscriminatory terms; and

(C) do not impose substantial costs on service providers or substantial burdens on their systems or networks.

(j) Injunctions.-The following rules shall apply in the case of any application for an injunction under section 502 against a service provider that is not subject to monetary remedies under this section:

(1) Scope of Relief.-

(A) With respect to conduct other than that which qualifies for the limitation on remedies set forth in subsection (a), the court may grant injunctive relief with respect to a service provider only in one or more of the following forms:

(i) An order restraining the service provider from providing access to infringing material or activity residing at a particular online site on the provider's system or network.

(ii) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(iii) Such other injunctive relief as the court may consider necessary to prevent or restrain infringement of copyrighted material specified in the order of the court at a particular online location, if such relief is the least burdensome to the service provider among the forms of relief comparably effective for that purpose.

(B) If the service provider qualifies for the limitation on remedies described in subsection (a), the court may only grant injunctive relief in one or both of the following forms:

(i) An order restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is using the provider's service to engage in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in the order.

(ii) An order restraining the service provider from providing access, by taking reasonable steps specified in the order to block access, to a specific, identified, online location outside the United States.

(2) Considerations.-The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider-

(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network;

(B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement;

(C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and

(D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.

(3) Notice and Ex Parte Orders.-Injunctive relief under this subsection shall be available only after notice to the service provider and an opportunity for the service provider to appear are provided, except for orders ensuring the preservation of evidence or other orders having no material adverse effect on the operation of the service provider's communications network.

(k) Definitions.-

(1) Service Provider.-(A) As used in subsection (a), the term "service provider" means an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received.

(B) As used in this section, other than subsection (a), the term "service provider" means a provider of online services or network access, or the operator of facilities therefor, and includes an entity described in subparagraph (A).

(2) Monetary Relief.-As used in this section, the term "monetary relief" means damages, costs, attorneys' fees, and any other form of monetary payment.

(l) Other Defenses Not Affected.-The failure of a service provider's conduct to qualify for limitation of liability under this section shall not bear adversely upon the consideration of a defense by the service provider that the service provider's conduct is not infringing under this title or any other defense.

(m) Protection of Privacy.-Nothing in this section shall be construed to condition the applicability of subsections (a) through (d) on-

(1) a service provider monitoring its service or affirmatively seeking facts indicating infringing activity, except to the extent consistent with a standard technical measure complying with the provisions of subsection (i); or

(2) a service provider gaining access to, removing, or disabling access to material in cases in which such conduct is prohibited by law.

(n) Construction.-Subsections (a), (b), (c), and (d) describe separate and distinct functions for purposes of applying this section. Whether a service provider qualifies for the limitation on liability in any one of those subsections shall be based solely on the criteria in that subsection, and shall not affect a determination of whether that service provider qualifies for the limitations on liability under any other such subsection.

[edited version]

**ROBERT HENDRICKSON v. EBAY INC., LUCKYBOY ENTERTAINMENT,
STEVEN REILLY, and DOES 1 through X, Defendants. and related cases**

**UNITED STATES DISTRICT COURT FOR THE
CENTRAL DISTRICT OF CALIFORNIA**

2001 U.S. Dist. LEXIS 14420

September 4, 2001, Decided

ROBERT J. KELLEHER, United States District Judge.

ORDER GRANTING DEFENDANTS EBAY INC., MARGARET C. WHITMAN AND MICHAEL RICHTER'S MOTION FOR SUMMARY JUDGMENT OR, ALTERNATIVELY, MOTION FOR PARTIAL SUMMARY JUDGMENT

This case involves a matter of first impression in the federal courts: whether one of the "safe harbor" provisions of the Digital Millennium Copyright Act ("DMCA") affords protection to the operator of the popular Internet auction web service, www.ebay.com, when a copyright owner seeks to hold the operator secondarily liable for copyright infringement by its sellers. On August 20, 2001, the Court heard Defendants eBay, Inc. ("eBay"), Margaret Whitman and Michael Richter's (collectively, the "eBay Defendants") motion for summary judgment on the copyright and trademark [*2] claims in the consolidated Hendrickson v. eBay, Inc. et al. cases. After the hearing, the Court took the motion under submission. After considering the papers submitted by the parties, the case file and oral argument, the Court hereby GRANTS the motion.

I. FACTUAL BACKGROUND

eBay provides an Internet website service where over 25 million buyers and sellers of consumer goods and services have come together to buy and sell items through either an auction or a fixed-price format. Pursuant to their agreement with eBay, users set up user IDs or "screen names" to conduct business on eBay's website in a semi-anonymous fashion. n1 Buyers and sellers reveal

their real identities to each other in private communications to complete sales transactions.

n1 This is akin to what users of CB radios do when they give themselves a handle that identifies themselves over the radio waves. Some eBay user IDs referenced in the records of this case include "emailtales" and "luckyboyentertainment," and "vidjointyc."

eBay's [*3] website allows sellers to post "listings" (or advertisements) containing descriptions of items they wish to offer for sale; and it allows buyers to bid for items they wish to buy. People looking to buy items can either browse through eBay's 4,700 categories of goods and services or search for items by typing words into eBay's search engine. Every day, eBay users place on average over one million new listings on eBay's website. At any given time, there are over six million listings on the website. n2

n2 In this case, eBay repeatedly characterizes its website as merely an online venue that publishes "electronic classified ads." (See, e.g., Motion at 3.) However, eBay's description grossly oversimplifies the nature of eBay's business. A review of eBay's website shows eBay operates far more than a sophisticated online classified service. (To the extent some of the descriptions about eBay's website are not in the record, the Court takes judicial notice of www.eBay.com and the information contained therein

pursuant to Federal Rule of Evidence 201.) Indeed, eBay's website is known first and foremost as an Internet auction website. See, e.g., Leslie Walker, *Ebay Goes Off-Line To Train Its Next Block of Dealers*, Wash. Post, Aug. 9, 2001, available at 2001 WL 23185584 ("eBay, the giant Internet auction house"); Pradnya Joshi & Charles V. Zehren, *Bidders' Remorse Online Auctions Now No. 1 Source of Internet Fraud*, Newsday, Aug. 30, 2000, available at 2000 WL 10031214 ("eBay, the world's largest online auction service"). eBay's own website describes itself as "the world's largest online marketplace." See "Overview" page, at <http://pages.ebay.com/community/aboutebay/overview/index.html>. eBay "enables trade on a local, national and international basis" and "features a variety of ... sites, categories and services that aim to provide users with the necessary tools for efficient online trading in the auction-style and fixed price formats." *Id.* eBay's Internet business features elements of both traditional swap meets -- where sellers pay for use of space to display their goods -- and traditional auction houses -- where goods are sold via the highest bid process.

[*4]

On or about December 20, 2000, eBay received a "cease and desist" letter from pro se Plaintiff Robert Hendrickson. The letter advised eBay that Plaintiff dba Tobann International Pictures is the copyright owner of the documentary "Manson." The letter also stated that pirated copies of "Manson" in digital video disk ("DVD") format were being offered for sale on eBay. However, the letter did not explain which copies of "Manson" in DVD format were infringing copies; nor did it fully describe Plaintiff's copyright interest. The letter demanded that eBay cease and desist "from any and all further conduct considered an infringement(s) of [Plaintiff's] right" or else face prosecution "to the fullest extent provided by law." (See Richter Decl., Ex. C.)

Promptly after receiving this letter, eBay sent Plaintiff e-mails asking for more detailed information concerning his copyright and the alleged infringing items. (See *id.*, Exs. D-G.) eBay advised Plaintiff that he has to submit proper notice

under the DMCA. For example, on December 20, 2000, eBay sent the following e-mail to Plaintiff:

Recognizing that some posted items may infringe certain intellectual property rights, [*5] we have set up specific procedures which enable verified rights owners to identify and request removal of allegedly infringing auction listings. These procedures are intended to substantially comply with the requirements of the [DMCA], 17 U.S.C. section 512. Click on the following link to access the [DMCA].

(*Id.*, Ex. D.) In that e-mail, eBay also encouraged Plaintiff to join its Verified Rights Owner ("VeRO") program, by submitting eBay's Notice of Infringement form. n3 As eBay explained, some of the benefits of the VeRO program include, among other things: (1) access to a customer support group dedicated to servicing the VeRO participants; (2) dedicated priority email queues for reporting alleged infringing activities; and (3) ability to use a special feature called "Personal Shopper," which allows users to conduct automatic searches for potentially infringing item. (*Id.*, Ex. D.)

n3 eBay's Notice of Infringement form quotes the notification provision of the DMCA, as set forth in 17 U.S.C. § 512(c)(3)(A). (See Richter Decl., Ex. B.)

[*6]

On December 28, 2000, Defendant Richter, eBay's Intellectual Property Counsel, followed up with another e-mail:

We have tried to contact you numerous times concerning your letter dated December 14, 2000. [P] We would like to assist you in removing items listed by third parties on our site which you claim infringe your rights. However, in order to do so, we would need proper notice under the [DMCA]. Specifically, we would need you to, among other things, identify the exact items n4 which you believe infringe your rights. In addition, we would need a statement from you, under penalty of perjury, that you own (or are the agent of the owner) the copyrights in the documentary. As you can understand, a statement that we immediately CEASE and DESIST from any and all further

conduct considered an infringement(s) of my right granted under Copyright and other laws of the land' gives us no indication of what your rights are, and gives us no indication as to which items infringe such rights.

(Id., Ex. G.) Plaintiff refused to join eBay's VeRO program and refused to fill out eBay's Notice of Infringement form. n5 Before filing suit, Plaintiff never provided eBay the specific [*7] item numbers that it sought.

n4 Each listing on eBay's website has its own item number.

n5 In his response to eBay's First Set of Requests for Admissions, Plaintiff explained why he refused to join the VeRO program:

Knowing that EBAY's so called VeRO program is nothing more than a wickedly concealed scheme to defraud unknowledgeable proprietors of Copyrights, out of their LAWFUL rights, Plaintiff refuses to join in, become a member of, participate in, act in concert with, be associated with, lend his name to, or in any way, be a part of a scheme intended to deprive anyone of their hard earned LAWFUL rights.

(Richter Decl., Ex. P at 2.)

* * *

B. The Copyright Claims Against eBay

1. The Infringing Activity

Plaintiff alleges that eBay participated in and facilitated the unlawful sale and distribution of pirated copies of "Manson" DVDs by providing an online forum, tools and services to the third party sellers. (See Opp. at 3; see also Complaint in Case No. 1, PP 18, 20, 21 & 30.) Plaintiff does not allege that the advertisements that sellers posted on eBay's website violate his copyright in "Manson." The type of secondary liability that Plaintiff seeks to impose on the eBay Defendants is similar to the type of secondary liability the Ninth Circuit allowed in *Fonovisa, Inc. v. Cherry Auction, Inc.*, 76 F.3d 259 (9th Cir. 1996). There, the court held that the complaint stated causes of action for vicarious

and contributory copyright infringement against the operators of a traditional swap meet for sales of counterfeit recordings by independent [*13] vendors. n6 Thus, the issue raised by Plaintiff's copyright claim is not whether eBay can be held secondarily liable for "third party advertisements." (See Reply at 3.) Rather, the question is whether eBay can be held secondarily liable for providing the type of selling platform/forum and services that it provided, however limited or automated in nature, to sellers of counterfeit copies of the film "Manson." Before the Court reaches the merits of that question, the Court must address a preliminary issue: whether the DMCA shields eBay from liability for copyright infringement.

n6 In April of this year, the Ninth Circuit in *A & M Records, Inc. v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001) extended *Fontovisa* to the Internet context. Napster operates an Internet service that facilitates the transmission and retention of digital audio files by its users. The Ninth Circuit affirmed the district court's conclusion that the plaintiffs -- record companies and music publishers -- have demonstrated a likelihood of success on the merits of their contributory and vicarious copyright infringement claims against Napster under the standards set forth in *Fontovisa*. The Ninth Circuit declined to reach the question of whether the safe harbor provisions of the DMCA applied, concluding that "this issue will be more fully developed at trial." 239 F.3d at 1025.

[*14]

2. The DMCA

The DMCA "is designed to facilitate the robust development and world-wide expansion of electronic commerce, communications, research, development, and education." S. Rep. No. 105-190, at 1 (105th Congress, 2d Session 1998). Title II of the DMCA, set forth in 17 U.S.C. § 512, "protects qualifying Internet service providers from liability for all monetary relief for direct, vicarious and contributory infringement." Id. at 20. "Title II preserves strong incentives for service providers and copyright owners to cooperate to detect and deal with copyright infringements that take place in the digital networked environment." Id. at 40.

There is no dispute over whether eBay is an Internet "service provider" within the meaning of Section 512. eBay clearly meets the DMCA's broad definition of online "service provider." See *17 U.S.C. § 512(k)(1)(B)* ("the term 'service provider' means a provider of online services or network access, or the operator of facilities therefor").

To qualify for one of the safe harbor provisions, the service provider's activities at issue must involve functions described in one of four [*15] separate categories set forth in subsections (a) through (d) of Section 512. See *17 U.S.C. § 512(n)*. eBay argues that it qualifies for protection under the third and fourth categories. Because the record establishes that eBay qualifies for protection under Section 512(c), the Court need not address the applicability of Section 512(d).

3. Safe Harbor Under Section 512(c)

Subsection (c) limits liability for "infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider." *17 U.S.C. § 512(c)* (emphasis added). This section applies where a plaintiff seeks to hold an Internet service provider responsible for either (1) infringing "material" stored and displayed on the service provider's website or (2) infringing "activity using the material on the [service provider's computer] system." *17 U.S.C. § 512(c)(1)(A)(i)*. Here, because the focus of the copyright claims against eBay concerns infringing activity -- the sale and distribution of pirated copies of "Manson" -- using "materials" [*16] posted eBay's website, Section 512(c) would provide eBay a safe harbor from liability if eBay meets the conditions set forth therein.

Three requirements for safe harbor are delineated in Section 512(c)(1). First, the service provider must demonstrate that it does not have actual knowledge that an activity using the material stored on its website is infringing or an awareness of "facts or circumstances from which infringing activity is apparent." *17 U.S.C. § 512(c)(1)(A)(i)-(ii)*. Alternatively, the service provider must show that it expeditiously removed or disabled access to the problematic material upon obtaining knowledge or awareness of infringing activity. See *17 U.S.C. § 512(c)(1)(A)(iii)*. Second, the service provider must show it "does not receive a financial benefit directly attributable to the infringing activity" if the service provider has "the right and ability to control such

activity." *17 U.S.C. § 512(c)(1)(B)*. Third, the service provider must show that it responded expeditiously to remove the material that is the subject of infringing activity upon receiving notification of the claimed infringement [*17] in the manner described in Section 512(c)(3). *17 U.S.C. § 512(c)(1)(C)*.

a. The Third Prong of the Test: Notification of the Alleged Infringing Activity

Under the third prong of the test, the service provider's duty to act is triggered only upon receipt of proper notice. See *id.* Section 512(c)(3) sets forth the required elements for proper notification by copyright holders. First, rights holders must provide written notification to the service provider's designated agent. See *17 U.S.C. § 512(c)(3)*. In addition, the notification must include "substantially" the following six elements:

- (1) a physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
- (2) identification of the copyrighted work claimed to have been infringed;
- (3) identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled, and information reasonably sufficient to permit the service provider to locate the material;
- (4) information reasonably sufficient [*18] to permit the service provider to contact the complaining party;
- (5) a statement that the complaining party has a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
- (6) a statement that the information in the notification is accurate, and under penalty of perjury, that the complaining party is authorized to act on behalf of the copyright owner.

Id.

Preliminary, the Court rejects Plaintiff's argument that he need not submit written notification in the manner described above (i.e.,

provide the notification referenced in the third prong of the safe harbor test) as long as other facts show the service provider received actual or constructive knowledge of infringing activity. (See Opp. at 8.) Plaintiff refers to the first prong of the safe harbor test set forth in Section 512(c)(1)(ii) and (iii) in support of this argument. Plaintiff's argument has no merit.

The DMCA expressly provides that if the copyright holder's attempted notification fails to "comply substantially" with the elements of notification described in subsection (c)(3), that notification "shall not [*19] be considered" when evaluating whether the service provider had actual or constructive knowledge of the infringing activity under the first prong set forth in Section 512(c)(1). *17 U.S.C. § 512(c)(3)(B)(i)* (emphasis added). Here, Plaintiff does not dispute that he has not strictly complied with Section 512(c)(3). (See, e.g., Opp. at 8-9.) The question is whether Plaintiff's imperfect attempts to give notice satisfy Section 512(c)(3)'s "substantial[]" compliance requirement.

(1) No Statement Attesting to Good Faith And Accuracy of Claim

Plaintiff's pre-suit "cease and desist" letter and e-mails to eBay do not include several of the key elements for proper notice required by Section 513(c)(3). (See Richter Decl., Exs. C, E, F, H & I.) None of these writings includes a written statement under "penalty of perjury" attesting to the fact "that the information in the notification is accurate ... [and] the complaining party is authorized to act on behalf of the owner" of the copyright at issue. *17 U.S.C. § 512(c)(3)(A)(vi)*. Additionally, none of these writings includes a written statement that Plaintiff "has a good [*20] faith belief that use of the material in the manner complained of is not authorized." *17 U.S.C. § 512(c)(3)(A)(v)*. The complete failure to include these key elements in his written communications to eBay, even after eBay specifically asked for these items, renders Plaintiff's notification of claimed infringement deficient under Section 512(c)(3).

(2) Inadequate Identification of Material Claimed to be the Subject of Infringing Activity

Moreover, the record shows that Plaintiff failed to comply substantially with the requirement that he provide eBay with sufficient information to identify the various listings that purportedly offered pirated copies of "Manson" for sale. See *17*

U.S.C. § 512(c)(3)(A)(iii). It is true that Plaintiff has informed eBay in writing that counterfeit copies of "Manson" were being offered and sold on eBay's website. However, when eBay requested that Plaintiff identify the alleged problematic listings by the eBay item numbers, Plaintiff refused. (See, e.g., Kim Decl., Ex. P [Plaintiff's Response to First Request for Admissions], RFA Nos. 21 and 22.) Plaintiff contends that it is not his job to [*21] do so once he has notified eBay of the existence of infringing activity by eBay sellers. (See *id.* at 3.)

The Court recognizes that there may be instances where a copyright holder need not provide eBay with specific item numbers to satisfy the identification requirement. For example, if a movie studio advised eBay that all listings offering to sell a new movie (e.g., "Planet X") that has not yet been released in VHS or DVD format are unlawful, eBay could easily search its website using the title "Planet X" and identify the offensive listings. However, the record in this case indicates that specific item numbers were necessary to enable eBay to identify problematic listings.

Plaintiff has never explained what distinguishes an authorized copy of "Manson" from an unauthorized copy. Initially, in his December 2000 cease and desist letter, Plaintiff only complained about pirated copies of "Manson" in DVD format. (See Richter Decl., Ex. C.) Plaintiff did not inform eBay that all DVD copies were unauthorized copies; he merely asserted that pirated copies of "Manson" DVDs were being sold on eBay. (See *id.*) Subsequently, Plaintiff sent an e-mail to eBay complaining [*22] about a seller who was selling a pirated copy of "Manson" in VHS format. (See *id.* at P 24 & Ex. I.) n7 But Plaintiff's e-mail did not identify the basis for his claim that the seller was selling a pirated copy of "Manson."

n7 On January 4, 2001, Plaintiff sent eBay an e-mail complaining about a seller named "vidjointnyc@hotmail.com" who was "still selling pirated copies of my film MANSON in YOUR 'Thieves Market'." (See Richter Decl., Ex. I.) After receiving Plaintiff's e-mail, eBay discovered that this seller had one active listing on eBay's website; that listing offered "Charles Manson Family Footage VHS New!!" (See *id.* at P 24 & Ex. J.) Nowhere in the listing did the seller state he was offering a copy of a film entitled

"Manson." (See *id.*) eBay removed the listing at the risk of exposing itself to a lawsuit from the seller even though up until that time Plaintiff had only complained about pirated DVDs, the seller was clearly offering a VHS tape for sale, and the listing made no reference to the title "Manson." (See *id.* at P 24 & n.1.)

[*23]

During oral argument, Plaintiff stated that he notified eBay that all copies of "Manson" in DVD format are unauthorized. However, the undisputed record in this case shows that Plaintiff did not provide this notification in writing before filing suit. n8 A copyright holder must comply with the "written communication" requirement. See 17 U.S.C. § 512(3)(A). The writing requirement is not one of the elements listed under the substantial compliance category. See *id.* Therefore, the Court disregards all evidence that purports to show Plaintiff gave notice that all DVDs violate his copyright in "Manson." n9

n8 Plaintiff contends that during a January 2001 telephone conversation (shortly after he commenced suit), he told Richter that all copies of "Manson" in DVD format infringe on his copyright because he has never authorized the release of this movie on DVD. (Hendrickson Decl., P 11.) There is a dispute in the record as to when Plaintiff orally advised eBay that all copies of "Manson" in DVD format were unauthorized. (Compare *id.* with Kim Decl., P 7.) However, the dispute over the dates is immaterial. It is undisputed that Plaintiff has never provided this information in a written communication to eBay as required by Section 512(c)(3). [*24]

n9 The Court notes that even though Plaintiff failed to submit proper notice of his claim that all "Manson" in DVD format are unauthorized, since March 2001, eBay has voluntarily searched its website on a daily basis for all copies of "Manson" in DVD format, removed all such listings and suspended repeat offenders. (See April 13, 2001 Declaration of Michael Richter filed in support of the eBay Defendants' Opp. to

Motion for Prelim. Injunction, P 24.) eBay has represented to the Court that it plans to continue to take such action during the pendency of this lawsuit. (See *id.*)

With respect to "Manson" VHS tapes, Plaintiff has admitted that authorized copies of "Manson" have been released in VHS format. (See Hendrickson Decl., P 11 ("certain VHS tapes were infringing[] because some of those had been authorized"; Kim Decl., P 7.) Therefore, authorized copies of "Manson" in VHS format are available in the marketplace. Plaintiff has offered no explanation to eBay or this Court as to how eBay could determine which "Manson" VHS tapes being offered for sale are unauthorized copies. n10

n10 Plaintiff states that during a January 2001 telephone conversation, he informed Richter that all VHS tapes labeled "new" had to be counterfeit. (Hendrickson Decl., P 11.) Because Plaintiff did not provide this information to eBay in writing, the Court need not consider the deficient notice. Nevertheless, the Court notes that Plaintiff's contention that all "new" VHS tapes must be counterfeit is wholly unsubstantiated. Perhaps Plaintiff has not authorized the release of new VHS copies in recent years. However, it is certainly possible that a seller advertises a "Manson" VHS tape as "new" because the tape remains sealed in its original package. Such a VHS tape could be an authorized copy.

[*25]

Plaintiff raises two more arguments in support of his claim that he need not provide eBay with specific item numbers to satisfy the "identification" requirement under the DMCA. Neither argument has merit.

First, Plaintiff points out that he has sent an e-mail to eBay identifying the eBay user IDs of four alleged infringers. Plaintiff asserts that the identification of user names provides eBay with sufficient information to locate the listings that offer pirated copies of "Manson." (See Hendrickson Decl., P 9(b).) The e-mail in question, dated December 21, 2000, does not satisfy the DMCA's identification

requirement. (See *id.*, Ex. G.) n11 The e-mail does not identify the listings that are claimed to be the subject of infringing activity; it does not even describe the infringing activity. Moreover, it contains none of the other requisite elements of a proper notification under Section 512(c)(3)(A), e.g., a statement attesting to the good faith and accuracy of the allegations.

n11 The e-mail states:

Hi, Kai, this is Robert Hendrickson, the copyright owner of the motion picture MANSON. Because of the copyright infringement activity conducted by the following Ebay User Names: emailtales, luckyboyentertainment, stoonod and vidjointnyc via your website, please email me any and ALL information you have on these criminals. Thanks.
(Hendrickson Decl, Ex. G.)

[*26]

Second, Plaintiff contends that eBay can identify listings offering infringing copies of "Manson" for sale without particular item numbers because eBay previously removed two listings even though Plaintiff did not provide the item numbers. (See Hendrickson Decl., PP 7 & 10.) The first listing, item number 1401275408, was the one that offered a VHS for sale by the seller "vidjointnyc@hotmail.com." (See *id.*; Richter Decl., Ex. J.) As discussed above, eBay found and removed this listing after Plaintiff sent an email complaining about this seller; this seller only had one active advertisement at the time. (See Richter Decl., P 24.) At the time, eBay had no evidence that seller vidjointnyc@hotmail.com was engaging in infringing activity; eBay simply removed the listing out of an abundance of caution. (See *id.*) With respect to the second listing, item number 525181519, the record is not clear as to why eBay removed the listing. Plaintiff's only "evidence" concerning this listing is a single page printout from some unidentified Internet message board that contains a post submitted by an unknown user. (See Hendrickson Decl., P 10 & Ex. J.) Plaintiff's evidence is inadmissible [*27] and his conclusion is unsubstantiated.

In sum, the record in this case shows that proper identification under Section 512(c)(3)(A)(iii) should include the specific item numbers of the listings that are allegedly offering pirated copies of "Manson" for sale. It is undisputed that Plaintiff refused to provide specific item numbers of problematic listings before filing suit. n12 Accordingly, the Court holds that Plaintiff failed to comply substantially with Section 512(c)(3)'s identification requirement. n13

n12 Plaintiff provided eBay a list of specific eBay item numbers of allegedly problematic listings on one occasion -- he identified them in his March 5, 2001 written response to the eBay Defendants' request for production of documents. This discovery response pre-dates the filing of Case No. 3. To the extent Plaintiff contends this discovery response constitutes sufficient notice of claims alleged in Case No. 3, the Court rejects Plaintiff's contention. The response was not under oath, it does not attest to a good faith belief that the items identified in the list are pirated copies of "Manson," and it does not attest to the accuracy of the allegations. Such a writing, without more, does not constitute adequate notice under Section 512(c)(3)(A). [*28]

n13 In light of the above ruling, the Court need not address whether Plaintiff's notification satisfied the other elements set forth in Section 512(c)(3)(A), e.g., whether Plaintiff notified eBay's "designated agent." However, during the hearing on this motion, Plaintiff raised a new argument involving the "designated agent" requirement. Plaintiff argued, for the first time, that eBay should not be able to avail itself of the protections of the DMCA because its website failed to identify a "designated agent" until recently. Based on the comments made during oral argument, the Court surmises that Plaintiff's contention is premised on the belief that eBay cannot simply designate "VeRO Department" for the submission of notices of infringement; rather, eBay must identify on its website the name of an individual "agent." Because Plaintiff failed to raise this argument in his papers and failed to submit evidence in support of this argument, the

Court declines to consider it. Nevertheless, the Court notes that the record shows that at all relevant times, eBay advised Plaintiff that the notices of infringement should be submitted to the attention of eBay's "VeRO Program." In its emails to Plaintiff, eBay provided a hypertext link to the notice of infringement form on eBay's website. That form identifies the address and fax number for the VeRO Program. Nothing in the DMCA mandates that service providers must designate the name of a person as opposed to a specialized department to receive notifications of claimed infringement. See *17 U.S.C. § 512(c)(2)*.

[*29]

Consequently, eBay did not have a duty to act under the third prong of the safe harbor test. See *17 U.S.C. § 512(c)(1)(C)*. Thus, if eBay establishes that it meets the remaining prongs of the safe harbor test, eBay would be entitled to judgment in its favor on the copyright claims.

b. The First Prong of the Test: Actual or Constructive Knowledge

Under the DMCA, a notification from a copyright owner that fails to comply substantially with Sections 512(c)(3)(A)(ii), (iii) or (iv) "shall not be considered under [the first prong of the safe harbor test] in determining whether a service provider has actual knowledge or is aware of the facts or circumstances from which infringing activity is apparent." See *17 U.S.C. § 512(c)(3)(B)(i) & (ii)* (emphasis added). As discussed above, Plaintiff's written notifications do not comply substantially with Section (c)(3)(A)(ii)'s adequate identification requirement. Therefore, the Court does not consider those notices when evaluating the actual or constructive knowledge prong of the safe harbor test.

eBay's evidence shows that prior to this lawsuit, it did not have actual or constructive [*30] knowledge that particular listings were being used by particular sellers to sell pirated copies of "Manson." The limited information that Plaintiff provided to eBay cannot, as a matter of law, establish actual or constructive knowledge that particular listings were involved in infringing activity. Accordingly, the Court holds that eBay has

satisfied the first prong of the safe harbor test under Section 512(c). See *17 U.S.C. § 512(c)(1)(A)*.

c. The Second Prong of the Test: Right and Ability to Control Infringing Activity

To satisfy the second prong of the test, eBay must show that it "does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity." *17 U.S.C. § 512(c)(1)(B)* (emphasis added). Because the undisputed facts establish that eBay does not have the right and ability to control the infringing activity, the Court need not evaluate the financial benefit element of this prong.

Plaintiff's only argument on the "ability to control" issue centers on eBay's ability to remove infringing listings (1) after [*31] it receives proper notification of infringing activity and (2) upon detecting an "apparent" infringement on its own. n14 (See Opp. at 7.) Plaintiff argues that the record shows eBay has the right and ability to control the infringing activity because it has removed the listings for the sale of various items in the past, including the listings offering pirated copies of "Manson" (in response to Plaintiff's complaints). Plaintiff's argument has no merit.

n14 In December 2000, eBay voluntarily began searching its website daily, on a limited basis, for listings that appear on their faces to be infringing -- "apparent" infringements. (See Richter Decl., P 13.) eBay conducts these searches using generic key words such as "bootleg," "pirated," "counterfeit," and "taped off TV" that may indicate potentially infringing activity. If eBay's staff determines that a seller appears to be offering infringing goods for sale, eBay would remove the listing from its website, notify the seller that the listing has been removed, refund the fees paid for that listing and review the seller's account for possible suspension. (See id.)

[*32]

First, the "right and ability to control" the infringing activity, as the concept is used in the DMCA, cannot simply mean the ability of a service provider to remove or block access to materials

posted on its website or stored in its system. To hold otherwise would defeat the purpose of the DMCA and render the statute internally inconsistent. The DMCA specifically requires a service provider to remove or block access to materials posted on its system when it receives notice of claimed infringement. See *17 U.S.C. § 512(c)(1)(C)*. The DMCA also provides that the limitations on liability only apply to a service provider that has "adopted and reasonably implemented ... a policy that provides for the termination in appropriate circumstances of [users] of the service provider's system or network who are repeat infringers." See *17 U.S.C. § 512(i)(1)(A)*. Congress could not have intended for courts to hold that a service provider loses immunity under the safe harbor provision of the DMCA because it engages in acts that are specifically required by the DMCA.

Second, eBay's voluntary practice of engaging in limited monitoring of its [*33] website for "apparent" infringements under the VeRO program cannot, in and of itself, lead the Court to conclude that eBay has the right and ability to control infringing activity within the meaning of the DMCA. The legislative history shows that Congress did not intend for companies such as eBay to be penalized when they engage in voluntary efforts to combat piracy over the Internet:

This legislation is not intended to discourage the service provider from monitoring its service for infringing material. Courts should not conclude that the service provider loses eligibility for limitations on liability under section 512 solely because it engaged in a monitoring program.

House Report 105-796 at 73 (Oct. 8, 1998).

Moreover, as Plaintiff acknowledges, the infringing activities at issue are the sale and distribution of pirated copies of "Manson" by

various eBay sellers -- which are consummated "offline" -- and not the display of any infringing material on eBay's website. (Reply at 3.) Viewing the term "infringing activity" in this context, the undisputed facts demonstrate that eBay does not have the right and ability to control such activity.

Unlike a traditional auction [*34] house, eBay is not actively involved in the listing, bidding, sale and delivery of any item offered for sale on its website. eBay's evidence shows that it does not have any control over the allegedly infringing items -- the pirated films. (See Richter Decl., PP 7, 33 & 34.) The evidence also shows that eBay never has possession of, or opportunity to inspect, such items because such items are only in the possession of the seller. (See *id.*) When auctions end, eBay's system automatically sends an email to the high bidder and the seller identifying each other as such. (See *id.* at P 7.) After that, all arrangements to consummate the transaction are made directly between the buyer and seller. (See *id.*) eBay has no involvement in the final exchange and generally has no knowledge whether a sale is actually completed (i.e., whether payment exchanges hands and the goods are delivered). (See *id.*) If an item is sold, it passes directly from the seller to the buyer without eBay's involvement. (See *id.*) eBay makes money through the collection of an "insertion fee" for each listing and a "final value fee" based on a percentage of the highest bid amount at the end of the [*35] auction. (See *id.* at P 8.)

Plaintiff offers no evidence that establishes the existence of a triable issue of fact on the "ability to control the infringing activity" issue. Accordingly, the Court holds that the record shows that eBay does not have the right and ability to control the infringing activity at issue.

Because eBay has established that it meets the test for safe harbor under Section 512(c), eBay is entitled to summary judgment in its favor on the copyright claims.



[home](#) | [my eBay](#) | [site map](#) | [sign in](#)

[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)

[basics](#) | [buyer guide](#) | [seller guide](#) | [my info](#) | [billing](#) | [rules & safety](#)



Buy an Item

Smart
Search

Search titles **and** descriptions

eBay's Verified Rights Owner (VeRO) Program™: Protecting Intellectual Property

In keeping with its status as the internet's largest venue for person-to-person trading, eBay does not and cannot verify that sellers have the right or ability to sell or distribute their listed items. However, we are committed to removing infringing or unlicensed items once an authorized representative of the rights owner properly reports them to us. eBay's Verified Rights Owner (VeRO) Program works to ensure that items listed for auction do not infringe upon the copyright, trademark or other intellectual property rights of third parties. VeRO Program participants may identify and request removal of allegedly infringing auction listings.

Any person or company who holds intellectual property rights (such as a copyright, trademark or patent) which may be infringed by eBay auction listings is encouraged to become a VeRO Program Member. It's fast and it's simple to do so. Current Program Members include hundreds of individuals, local, state and federal law enforcement, and companies from a wide array of industries.

Program participation entitles you to the following benefits:

- Dedicated eBay staff to assist you in getting the most out of the Program
- Rapid response by eBay in ending auctions reported by you as allegedly infringing
- Dedicated priority email queues for reporting alleged infringements
- The ability to obtain identifying information about eBay users
- eBay member rights and privileges as described in the [eBay User Agreement](#) and [Privacy Policy](#)
- Automatic updates on new benefits available under the Program

How to Become a VeRO Program Member

It is fast and simple to join the VeRO Program. We require only that you fill out and fax to us a Notice of Infringement form specifying the allegedly infringing listings and infringed works, complete with an original authorized signature. The information requested by the Notice of Infringement is designed to ensure that parties reporting items are authorized by the rights owners, and to enable eBay to correctly identify the material or listing to be ended. After your first Notice of Infringement is received by us, you'll be able to transmit future notices to eBay by email. Click [here](#) to download the Notice of Infringement and explanatory materials. You will need Adobe® Reader to view and print these

documents. Free downloads are available at Adobe's web site by clicking on this button:



If you are unable to download a PDF file, please [click here](#) to view and print a copy of our Notice of Infringement.

Automated Searches

eBay offers to all users a feature called Favorite Searches. You can use our Favorite Searches feature to conduct automatic searches for potentially infringing items. Favorite Searches enables you to create up to fifteen automatic searches using search terms you provide. You can designate three of these searches to be automatically emailed to you. Our system will automatically notify you on a daily basis of any new

listings posted which contain any terms in your three selected searches. You can use sophisticated boolean logic searches just like our main search engine. The easiest way to set up this feature is to perform a search using eBay's main search engine [here](#), and then clicking "save this search" at the bottom of the search results. You'll need to be a member of eBay to use Favorite Searches. You can go directly to your Favorite Searches by clicking [here](#).

How to Report Items if You are Not an Intellectual Property Owner

If you are not an intellectual property owner, you will not be able to join our VeRO Program. However, you can still help by getting in touch with the relevant rights owner and encouraging them to contact us. Also, if you want to report suspected infringing items to eBay, [Contact Rules & Safety](#). We are happy to receive such information, but must advise that we may be limited in our ability to respond to your request absent formal notice from an authorized rights owner.

Please [click here](#) for a list of VeRO Program Member About Me Pages.

For More Information

- If you are an IP rights owner and have questions about the VeRO Program or our infringing items policies, please [Contact Rules & Safety](#).
- If you are a seller and had an auction ended, click [here](#) to learn more. You may also want to reread our [Privacy Policy](#) and [User Agreement](#).
- For additional information about prohibited, questionable, and infringing items on eBay, click [here](#).

Still have a question?

Search for help on:

(e.g., what is a Reserve Price Auction?)

[Announcements](#) | [Register](#) | [eBay Gear](#) | [SafeHarbor \(Rules & Safety\)](#) | [Feedback Forum](#) | [About eBay](#)
[Home](#) | [My eBay](#) | [Site Map](#)

[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)
[Basics](#) | [Buyer Guide](#) | [Seller Guide](#) | [My Info](#) | [Billing](#) | [Rules & Safety](#)

Copyright © 1995-2001 eBay Inc. All Rights Reserved.

Designated trademarks and brands are the property of their respective owners.

Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



US Copyright Law

17 U.S.C. § 1201 (Supp. 1999)

[NOTE: edited version - [click here](#) for full version]

§ 1201. Circumvention of copyright protection systems

(a) Violations Regarding Circumvention of Technological Measures.-(1)(A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title. The prohibition contained in the preceding sentence shall take effect at the end of the 2-year period beginning on the date of the enactment of this chapter.

(B) The prohibition contained in subparagraph (A) shall not apply to persons who are users of a copyrighted work which is in a particular class of works, if such persons are, or are likely to be in the succeeding 3-year period, adversely affected by virtue of such prohibition in their ability to make noninfringing uses of that particular class of works under this title, as determined under subparagraph (C).

(C) During the 2-year period described in subparagraph (A), and during each succeeding 3-year period, the Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rule-making, the Librarian shall examine-

- (i) the availability for use of copyrighted works;
- (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
- (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
- (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and
- (v) such other factors as the Librarian considers appropriate.

(D) The Librarian shall publish any class of copyrighted works for which the Librarian has determined, pursuant to the rulemaking conducted under subparagraph (C), that noninfringing uses by persons who are users of a copyrighted work are, or are likely to be, adversely affected, and the prohibition contained in subparagraph (A) shall not apply to such users with respect to such class of works for the ensuing 3-year period.

(E) Neither the exception under subparagraph (B) from the applicability

of the prohibition contained in subparagraph (A), nor any determination made in a rulemaking conducted under subparagraph (C), may be used as a defense in any action to enforce any provision of this title other than this paragraph.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any

technology, product, service, device, component, or part thereof, that-

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection-

(A) to "circumvent a technological measure" means 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; and

(B) a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

(b) Additional Violations.-(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that-

(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection-

(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" if the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.

(c) Other Rights, Etc., Not Affected.-(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(3) Nothing in this section shall require that the design of, or design and selection of parts and components for, a consumer electronics, telecommunications, or computing product provide for a response to any particular technological measure, so long as such part or component, or the product in which such part or component is integrated, does not otherwise fall within the prohibitions of subsection (a)(2) or (b)(1).

(4) Nothing in this section shall enlarge or diminish any rights of free speech or the press for activities using consumer electronics, telecommunications, or computing products.

(d) Exemption for Nonprofit Libraries, Archives, and Educational Institutions. . . .

(e) Law Enforcement, Intelligence, and Other Government Activities. . . .

(g) Encryption Research. . . .

(h) Exceptions Regarding Minors.-In applying subsection (a) to a component or part, the court may consider the necessity for its intended and actual incorporation in a technology, product, service, or device, which-

(1) does not itself violate the provisions of this title; and

(2) has the sole purpose to prevent the access of minors to material on the Internet.

(i) Protection of Personally Identifying Information.-

(1) Circumvention Permitted.-Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure that effectively controls access to a work protected under this title, if-

(A) the technological measure, or the work it protects, contains the capability of collecting or disseminating personally identifying information reflecting the online activities of a natural person who seeks to gain access to the work protected;

(B) in the normal course of its operation, the technological measure, or the work it protects, collects or disseminates personally identifying information about the person who seeks to gain access to the work protected, without providing conspicuous notice of such collection or dissemination to such person, and without providing such person with the capability to prevent or restrict such collection or dissemination;

(C) the act of circumvention has the sole effect of identifying and disabling the capability described in subparagraph (A), and has no other effect on the ability of any person to gain access to any work; and

(D) the act of circumvention is carried out solely for the purpose of preventing the collection or dissemination of personally identifying information about a natural person who seeks to gain access to the work protected, and is not in violation of any other law. . . .

(j) Security Testing. . . .

(k) Certain Analog Devices and Certain Technological Measures. . . .

US Copyright Law

17 U.S.C. § 1202 (Supp. 1999)

§ 1202. Integrity of copyright management information

(a) False Copyright Management Information.-No person shall knowingly and with the intent to induce, enable, facilitate, or conceal infringement-

- (1) provide copyright management information that is false, or
- (2) distribute or import for distribution copyright management information that is false.

(b) Removal or Alteration of Copyright Management Information.-

No person shall, without the authority of the copyright owner or the law-

- (1) intentionally remove or alter any copyright management information,
- (2) distribute or import for distribution copyright management information knowing that the copyright management information has been removed or altered without authority of the copyright owner or the law, or
- (3) distribute, import for distribution, or publicly perform works, copies of works, or phonorecords, knowing that copyright management information has been removed or altered without authority of the copyright owner or the law, knowing, or, with respect to civil remedies under section 1203, having reasonable grounds to know, that it will induce, enable, facilitate, or conceal an infringement of any right under this title.

(c) Definition.-As used in this section, the term "copyright management information" means any of the following information conveyed in connection with copies or phonorecords of a work or performances or displays of a work, including in digital form, except that such term does not include any personally identifying information about a user of a work or of a copy, phonorecord, performance, or display of a work:

- (1) The title and other information identifying the work, including the information set forth on a notice of copyright.
- (2) The name of, and other identifying information about, the author of a work.
- (3) The name of, and other identifying information about, the copyright owner of the work, including the information set forth in a notice of copyright.
- (4) With the exception of public performances of works by radio and television broadcast stations, the name of, and other identifying information about, a performer whose performance is fixed in a work other than an audiovisual work.
- (5) With the exception of public performances of works by radio and television broadcast stations, in the case of an audiovisual work, the name of, and other identifying information about, a writer, performer, or director who is credited in the audiovisual work.
- (6) Terms and conditions for use of the work.

(7) Identifying numbers or symbols referring to such information or links to such information.

(8) Such other information as the Register of Copyrights may prescribe by regulation, except that the Register of Copyrights may not require the provision of any information concerning the user of a copyrighted work.

(d) Law Enforcement, Intelligence, and Other Government Activities.-This section does not prohibit any lawfully authorized investigative, protective, information security, or intelligence activity of an officer, agent, or employee of the United States, a State, or a political subdivision of a State, or a person acting pursuant to a contract with the United States, a State, or a political subdivision of a State. For purposes of this subsection, the term "information security" means activities carried out in order to identify and address the vulnerabilities of a government computer, computer system, or computer network.

(e) Limitations on Liability.-

(1) Analog Transmissions.-In the case of an analog transmission, a person who is making transmissions in its capacity as a broadcast station, or as a cable system, or someone who provides programming to such station or system, shall not be liable for a violation of subsection (b) if-

(A) avoiding the activity that constitutes such violation is not technically feasible or would create an undue financial hardship on such person; and

(B) such person did not intend, by engaging in such activity, to induce, enable, facilitate, or conceal infringement of a right under this title.

(2) Digital Transmissions.-

(A) If a digital transmission standard for the placement of copyright management information for a category of works is set in a voluntary, consensus standard-setting process involving a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to the particular copyright management information addressed by such standard if-

(i) the placement of such information by someone other than such person is not in accordance with such standard; and

(ii) the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title.

(B) Until a digital transmission standard has been set pursuant to subparagraph (A) with respect to the placement of copyright management information for a category of works, a person identified in paragraph (1) shall not be liable for a violation of subsection (b) with respect to such copyright management information, if the activity that constitutes such violation is not intended to induce, enable, facilitate, or conceal infringement of a right under this title, and if-

(i) the transmission of such information by such person would result in a perceptible visual or aural degradation of the digital signal; or

(ii) the transmission of such information by such person would conflict with-

(I) an applicable government regulation relating to transmission of information in a digital signal;

(II) an applicable industry-wide standard relating to the transmission of information in a digital signal that was adopted by a voluntary consensus standards body prior to the effective date of this chapter; or

(III) an applicable industry-wide standard relating to the transmission of information in a digital signal

that was adopted in a voluntary, consensus standards-setting process open to participation by a representative cross-section of broadcast stations or cable systems and copyright owners of a category of works that are intended for public performance by such stations or systems.

(3) Definitions.-As used in this subsection-

(A) the term "broadcast station" has the meaning given that term in section 3 of the Communications Act of 1934 (47 U.S.C. 153); and

(B) the term "cable system" has the meaning given that term in section 602 of the Communications Act of 1934 (47 U.S.C. 522).

2000 U.S. Dist. LEXIS 11696, *; 55 U.S.P.Q.2D (BNA) 1873;
Copy. L. Rep. (CCH) P28,122

[note: edited version]

**UNIVERSAL CITY STUDIOS, INC, et al., Plaintiffs, -against- SHAWN C.
REIMERDES, et al., Defendants.**

00 Civ. 0277 (LAK)

**UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF
NEW YORK**

*2000 U.S. Dist. LEXIS 11696; 55 U.S.P.Q.2D (BNA) 1873; Copy. L. Rep. (CCH)
P28,122*

August 17, 2000, Decided

LEWIS A. KAPLAN, *District Judge.*

Plaintiffs, eight major United States motion picture studios, distribute many of their copyrighted motion pictures for home use on digital versatile disks ("DVDs"), which contain copies of the motion pictures in digital form. They protect those motion pictures from copying by using an encryption system called CSS. CSS-protected motion pictures on DVDs may be viewed only on players and computer drives equipped with licensed technology that permits the devices to decrypt and play--but not to copy--the films.

Late last year, computer hackers devised a computer program called DeCSS that circumvents the CSS protection system and allows CSS-protected motion pictures to be copied and played on devices that lack the licensed decryption technology. Defendants quickly posted [*2] DeCSS on their Internet web site, thus making it readily available to much of the world. Plaintiffs promptly brought this action under the Digital Millennium Copyright Act (the "DMCA") n1 to enjoin defendants from posting DeCSS and to prevent them from electronically "linking" their site to others that post DeCSS. Defendants responded with what they termed "electronic civil disobedience" --increasing their efforts to link their web site to a large number of others that continue to make DeCSS available.

n1 *17 U.S.C. § 1201 et seq.*

Defendants contend that their actions do not violate the DMCA and, in any case, that the DMCA, as applied to computer programs, or code, violates the First Amendment. n2 This is the Court's decision after trial, and the decision may be summarized in a nutshell.

[*3]

Defendants argue first that the DMCA should not be construed to reach their conduct, principally because the DMCA, so applied, could prevent those who wish to gain access to technologically protected copyrighted works in order to make fair--that is, non-infringing--use of them from doing so. They argue that those who would make fair use of technologically protected copyrighted works need means, such as DeCSS, of circumventing access control measures not for piracy, but to make lawful use of those works.

Technological access control measures have the capacity to prevent fair uses of copyrighted works as well as foul. Hence, there is a potential tension between the use of such access control measures and fair use. Defendants are not the first to recognize that possibility. As the DMCA made its way through the legislative process, Congress was preoccupied with precisely this issue. Proponents of strong restrictions on circumvention of access control measures argued that they were essential if copyright holders were to make their works available in digital form because digital works otherwise could be pirated too easily. Opponents contended that strong anticircumvention measures would [*4] extend the copyright monopoly inappropriately and prevent many fair uses of copyrighted material.

Congress struck a balance. The compromise it reached, depending upon future technological and commercial developments, may or may not prove ideal. n3 But the solution it enacted is clear. The potential tension to which defendants point does not absolve them of liability under the statute. There is no serious question that defendants' posting of DeCSS violates the DMCA.

* * *

5. *The Technology Here at Issue*

CSS, or Content Scramble System, is an access control and copy prevention system for DVDs developed by the motion picture companies, including plaintiffs. n27 It is an encryption-based system that requires the use of appropriately configured hardware such as a DVD player or a computer DVD drive to decrypt, unscramble and play back, but not copy, motion pictures on DVDs. n28 The technology necessary to configure DVD players and drives to play CSS-protected DVDs n29 has been licensed to hundreds of manufacturers in the United States and around the world.

DeCSS is a software utility, or computer program, that enables users to break the CSS copy protection system and hence to view DVDs on unlicensed players and make digital copies of DVD movies. n30 The quality of motion pictures decrypted by DeCSS is virtually identical to that of encrypted movies [*17] on DVD. n31

DivX is a compression program available for download over the Internet. n32 It compresses video files in order to minimize required storage space, often to facilitate transfer over the Internet or other networks. n33

B. *Parties*

Plaintiffs are eight major motion picture studios. Each is in the business of producing and distributing copyrighted material including motion pictures. Each distributes, either directly or through affiliates, copyrighted motion pictures on DVDs. n34 Plaintiffs produce and distribute a large majority of the motion pictures on DVDs on the market today. n35

Defendant Eric Corley is viewed as a leader of the computer hacker community and goes by the name Emmanuel Goldstein, after the leader of the underground in George Orwell's classic, *1984*. n36 He and his company, defendant 2600 Enterprises, Inc., together publish a magazine called *2600: The Hacker Quarterly*, which Corley founded in 1984, n37 and which is something of a bible to the hacker community. n38 The name "2600" was derived from the fact that hackers in the 1960's found that the transmission of a 2600 hertz tone over a long distance trunk connection gained access to "operator mode" and allowed the user to explore aspects of the telephone system that were not otherwise accessible. n39 Mr. Corley chose the name because he regarded it as a "mystical thing," n40 commemorating something that he evidently admired. Not surprisingly, *2600: The Hacker Quarterly* has included articles on such topics as how to steal an Internet domain name, n41 access other people's e-mail, n42 intercept cellular phone

calls, n43 and break into the computer systems at Costco stores n44 and Federal Express. n45 One issue contains a guide to the federal criminal justice system for readers charged [*19] with computer hacking. n46 In addition, defendants operate a web site located at <<http://www.2600.com>> ("2600.com"), which is managed primarily by Mr. Corley and has been in existence since 1995. n47

Prior to January 2000, when this action was commenced, defendants posted the source and object code for DeCSS on the 2600.com web site, from which they could be downloaded easily. n48 At that time, 2600.com contained also a list of links to other web sites purporting to post DeCSS. n49

* * *

[T]he technology for making compliant devices, i.e., devices with CSS keys, had to be licensed to consumer electronics manufacturers. n60 In order to ensure that the decryption technology did not become generally available and that compliant devices could not be used to copy as well as merely to play CSS-protected movies, the technology [*24] is licensed subject to strict security requirements. n61 Moreover, manufacturers may not, consistent with their licenses, make equipment that would supply digital output that could be used in copying protected DVDs. n62 Licenses to manufacture compliant devices are granted on a royalty-free basis subject only to an administrative fee. n63 At the time of trial, licenses had been issued to numerous hardware and software manufacturers, including two companies that plan to release DVD players for computers running the Linux operating system. n64

* * *

D. *The Appearance of DeCSS*

In late September 1999, Jon Johansen, a Norwegian subject then fifteen years of age, and two individuals he "met" under pseudonyms over the Internet, reverse engineered a licensed DVD player and discovered the CSS encryption algorithm and keys. n71 They used this information to create DeCSS, a program capable of decrypting or "ripping" encrypted DVDs, thereby allowing playback on non-compliant computers as well as the copying of decrypted files to computer hard drives. n72 Mr. Johansen then [*27] posted the executable code on his personal Internet web site and informed members of an Internet mailing list that he had done so. n73 Neither Mr. Johansen nor his collaborators obtained a license from the DVD CCA. n74

Although Mr. Johansen testified at trial that he created DeCSS in order to make a DVD player that would operate on a computer running the Linux operating system, n75 DeCSS is a Windows executable file; that is, it can be executed only on computers running the Windows operating system. n76 Mr. Johansen explained the fact that he created a Windows rather than a Linux program by asserting that Linux, at the time he created DeCSS, did not support [*28] the file system used on DVDs. n77 Hence, it was necessary, he said, to decrypt the DVD on a Windows computer in order subsequently to play the decrypted files on a Linux machine. n78 Assuming that to be true, n79 however, the fact remains that Mr. Johansen created DeCSS in the full knowledge that it could be used on computers running Windows rather than Linux. Moreover, he was well aware that the files, once decrypted, could be copied like any other computer files.

In January 1999, Norwegian prosecutors filed charges against Mr. Johansen stemming from the development of DeCSS. n80 The disposition of the Norwegian [*29] case does not appear of record.

E. The Distribution of DeCSS

In the months following its initial appearance on Mr. Johansen's web site, DeCSS has become widely available on the Internet, where hundreds of sites now purport to offer the software for download. n81 A few other applications said to decrypt CSS-encrypted DVDs also have appeared on the Internet. n82

In November 1999, defendants' web site began to offer DeCSS for download. n83 It established also a list of links to several web sites that purportedly "mirrored" or offered DeCSS for download. n84 The links on defendants' mirror list fall into one of three categories. By clicking the mouse on one of these links, the user may be brought to a page on the linked-to site on which there appears a further link to the DeCSS software. n85 If the user then clicks on the DeCSS link, download of the software begins. This page may or may not contain content other than the DeCSS link. n86 Alternatively, the user may be brought to a page on the linked-to site that does not itself purport to link to DeCSS, but that links, either directly or via a series of other pages on the site, to another page on the site on which there appears a link to the DeCSS software. n87 Finally, the user may be brought directly to the DeCSS link on the linked-to site such that download of DeCSS begins immediately

F. The Preliminary Injunction and Defendants' Response

The movie studios, through the Internet investigations division of the Motion Picture Association of America ("MPAA"), became aware of the availability

of DeCSS on the Internet in October 1999. n89 The industry responded by sending out a number of cease and desist letters to web site operators who posted the software, some of which removed it from their sites. n90 In January 2000, the studios filed this lawsuit against [*32] defendant Eric Corley and two others. n91

After a hearing at which defendants presented no affidavits or evidentiary material, the Court granted plaintiffs' motion for a preliminary injunction barring defendants from posting DeCSS. n92 At the conclusion of the hearing, plaintiffs sought also to enjoin defendants from linking to other sites that posted DeCSS, but the Court declined to entertain the application at that time in view of plaintiffs' failure to raise the issue in their motion papers. n93

Following the issuance of the preliminary injunction, defendants removed DeCSS from the 2600.com web site. n94 In what they termed an act of "electronic civil disobedience," n95 however, they continued to support links to other web sites purporting to offer DeCSS for download, a list which had grown to nearly five hundred by July 2000. n96 Indeed, they carried a banner saying "Stop the MPAA" and, in a reference to this lawsuit, proclaimed:

"We have to face the possibility that we could be forced into submission. For that reason it's especially important that as many of you as possible, all throughout the world, take a stand and mirror these files." n97

Thus, defendants obviously hoped to frustrate plaintiffs' recourse to the judicial system by making effective relief difficult or impossible.

At least some of the links currently [*34] on defendants' mirror list lead the user to copies of DeCSS that, when downloaded and executed, successfully decrypt a motion picture on a CSS-encrypted DVD. n98

* * *

II. The Digital Millennium Copyright Act

A. . . .

The DMCA contains two principal anticircumvention provisions. The first, Section

1201(a)(1), governs "the act of circumventing a technological protection measure put in place by a copyright owner to control access to a copyrighted work," an act described by Congress as "the electronic equivalent of breaking into a locked room in order to obtain a copy of a book." n131 The second, Section 1201(a)(2), which is the focus of this case, "supplements the prohibition against the act of circumvention in paragraph (a)(1) with prohibitions on creating and making available certain technologies ... developed or advertised to defeat technological protections against unauthorized access to a work." n132 As defendants are accused here only of posting and linking to [*46] other sites posting DeCSS, and not of using it themselves to bypass plaintiffs' access controls, it is principally the second of the anticircumvention provisions that is at issue in this case.

B. Posting of DeCSS

1. Violation of Anti-Trafficking [*47] Provision

Section 1201(a)(2) of the Copyright Act, part of the DMCA, provides that:

"No person shall ... offer to the public, provide or otherwise traffic in any technology ... that--

"(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act];

"(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under [the Copyright Act]; or

"(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under [the Copyright Act]."

In this case, defendants concededly offered and provided and, absent a court [*48] order, would continue to offer and provide DeCSS to the public by making it available for download on the 2600.com web site. DeCSS, a computer program, unquestionably is "technology" within the meaning of the statute. n135 "Circumvent a technological measure" is defined to mean descrambling a scrambled work, decrypting an encrypted work, or "otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without

the authority of the copyright owner," n136 so DeCSS clearly is a means of circumventing a technological access control measure. n137 In consequence, if CSS otherwise falls within paragraphs (A), (B) or (C) of Section 1201(a)(2), and if none of the statutory exceptions applies to their actions, defendants have violated and, unless enjoined, will continue to violate the DMCA by posting DeCSS.

[*50]

a. Section 1201(a)(2)(A)

(1) CSS Effectively Controls Access to Copyrighted Works

During pretrial proceedings and at trial, defendants attacked plaintiffs' Section 1201(a)(2)(A) claim, arguing that CSS, which is based on a 40-bit encryption key, is a weak cipher that does not "effectively control" access to plaintiffs' copyrighted works. They reasoned from this premise that CSS is not protected under this branch of the statute at all. Their post-trial memorandum appears to have abandoned this argument. In any case, however, the contention is indefensible as a matter of law.

First, the statute expressly provides that "a technological measure 'effectively controls access to a work' if the measure, in the ordinary course of its operation, requires the application of information or a process or a treatment, with the authority of the copyright owner, to gain access to a work." n138 One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player [*51] or drive containing the keys pursuant to such a license. In consequence, under the express terms of the statute, CSS "effectively controls access" to copyrighted DVD movies. It does so, within the meaning of the statute, whether or not it is a strong means of protection. n139

This view is confirmed by the legislative history, which deals with precisely this point. The House Judiciary Committee section-by-section analysis of the House bill, which in this respect was enacted into law, makes clear that a technological measure "effectively controls access" to a copyrighted work if its *function* is to control access:

"The bill does define the *functions* of the technological measures that are covered--that is, what it means for a technological measure to 'effectively control access to a work' ... and to 'effectively protect a right of a

copyright [*52] owner under this title' The practical, common-sense approach taken by H.R. 2281 is that if, in the ordinary course of its operation, a technology actually works in the defined ways to control access to a work ... then the 'effectiveness' test is met, and the prohibitions of the statute are applicable. This test, which focuses on the function performed by the technology, provides a sufficient basis for clear interpretation." n140

Further, the House Commerce Committee made clear that measures based on encryption or scrambling "effectively control" access to copyrighted works, n141 although it is well known that what may be encrypted or scrambled often may be decrypted or unscrambled. As CSS, in the ordinary course of its operation--that is, when DeCSS or some other decryption program is not employed-- "actually works" to prevent access to the protected work, it "effectively controls access" within the contemplation of the statute.

Finally, the interpretation of the phrase "effectively controls access" offered by defendants at trial--viz., that the use of the word "effectively" means that the statute protects only successful or efficacious technological means of controlling access--would gut the statute if it were adopted. If a technological means of access control is circumvented, it is, in common parlance, ineffective. Yet defendants' construction, if adopted, would limit the application of the statute to access control measures that thwart circumvention, but withhold protection for those measures that can be circumvented. In other words, defendants would have the Court construe the statute to offer protection where none is needed but to withhold protection precisely where protection is essential. The Court declines to do so. Accordingly, the Court holds that CSS effectively controls access to plaintiffs' copyrighted works. n142

(2) *DeCSS Was Designed Primarily to Circumvent CSS*

As CSS effectively controls access to plaintiffs' copyrighted works, the only remaining question under Section 1201(a)(2)(A) is whether DeCSS was designed primarily to circumvent CSS. The answer is perfectly obvious. By the admission of both Jon Johansen, the programmer who principally wrote DeCSS, and defendant Corley, DeCSS was created solely for the purpose of decrypting CSS--that is all it does. n143 Hence, absent satisfaction of a statutory exception, defendants clearly violated Section 1201(a)(2)(A) by posting DeCSS to their web site.

b. Section 1201(a)(2)(B)

As the only purpose or use of DeCSS is to circumvent CSS, the foregoing is sufficient to establish a *prima facie* violation of Section 1201(a)(2)(B) as well.

c. The Linux Argument

Perhaps the centerpiece of defendants' statutory position is the contention that DeCSS was not created for the purpose of pirating copyrighted motion pictures. [*55] Rather, they argue, it was written to further the development of a DVD player that would run under the Linux operating system, as there allegedly were no Linux compatible players on the market at the time. n144 The argument plays itself out in various ways as different elements of the DMCA come into focus. But it perhaps is useful to address the point at its most general level in order to place the preceding discussion in its fullest context.

As noted, Section 1201(a) of the DMCA contains two distinct prohibitions. Section 1201(a)(1), the so-called basic provision, "aims against those who engage in unauthorized circumvention of technological measures [It] focuses directly on wrongful conduct, rather than on those who facilitate wrongful conduct" n145 Section 1201(a)(2), the anti-trafficking provision at issue in this case, on the other hand, separately bans offering or providing technology that may be used to circumvent technological means of controlling access [*56] to copyrighted works. n146 If the means in question meets any of the three prongs of the standard set out in Section 1201(a)(2)(A), (B), or (C), it may not be offered or disseminated.

As the earlier discussion demonstrates, the question whether the development of a Linux DVD player motivated those who wrote DeCSS is immaterial to the question whether the defendants now before the Court violated the anti-trafficking provision of the DMCA. The inescapable facts are that (1) CSS is a technological means that effectively controls access to plaintiffs' copyrighted works, (2) the one and only function of DeCSS is to circumvent CSS, and (3) defendants offered and provided DeCSS by posting it on their web site. Whether defendants did so in order to infringe, or to permit or encourage others to infringe, copyrighted works in violation of other provisions of the Copyright Act simply does not matter for purposes [*57] of Section 1201(a)(2). The offering or provision of the program is the prohibited conduct--and it is prohibited irrespective of why the program was written, except to whatever extent motive may be germane to determining

whether their conduct falls within one of the statutory exceptions.

2. *Statutory Exceptions*

Earlier in the litigation, defendants contended that their activities came within several exceptions contained in the DMCA and the Copyright Act and constitute fair use under the Copyright Act. . . .

d. *Fair use*

[D]efendants rely on the doctrine of fair use. Stated in its most general terms, the doctrine, now codified in Section 107 of the Copyright Act, n158 limits the exclusive rights of a copyright holder by permitting others to make limited use of portions of the copyrighted work, for appropriate purposes, free of liability for copyright infringement. For example, it is permissible for one other than the copyright owner to reprint or quote a suitable part of a copyrighted book or article in certain circumstances. The doctrine traditionally has facilitated literary and artistic criticism, teaching and scholarship, and other socially useful forms of expression. It has been viewed by courts as a safety valve that accommodates the exclusive rights conferred by copyright with the freedom of expression guaranteed by the First Amendment.

The use of technological means of controlling access to a copyrighted work may affect the ability to make fair uses [*65] of the work. n159 Focusing specifically on the facts of this case, the application of CSS to encrypt a copyrighted motion picture requires the use of a compliant DVD player to view or listen to the movie. Perhaps more significantly, it prevents exact copying of either the video or the audio portion of all or any part of the film. n160 This latter point means that certain uses that might qualify as "fair" for purposes of copyright infringement--for example, the preparation by a film studies professor of a single CD-ROM or tape containing two scenes from different movies in order to illustrate a point in a lecture on cinematography, as opposed to showing relevant parts of two different DVDs--would be difficult or impossible absent circumvention of the CSS encryption. Defendants therefore argue that the DMCA cannot properly be construed to make it difficult or impossible to make any fair use of plaintiffs' copyrighted works and that the statute therefore does not reach their activities, which are simply a means to enable users of DeCSS to make such fair uses.

Defendants have focused on a significant point. Access control measures such as CSS do involve some risk of preventing lawful as well as unlawful uses of copyrighted material. Congress, however, clearly faced up to and dealt with this question in enacting the DMCA.

The Court begins its statutory analysis, as it must, with the language of the statute. Section 107 of the Copyright Act provides in critical part that certain uses of copyrighted works that otherwise would be wrongful are "not ... infringement[s] of copyright." n161 Defendants, however, are not here sued for copyright infringement. They are sued for offering and providing technology designed to circumvent technological measures that control access to copyrighted works and otherwise violating Section 1201(a)(2) of the Act. If Congress had meant the fair use defense to apply to such actions, [*67] it would have said so. Indeed, as the legislative history demonstrates, the decision not to make fair use a defense to a claim under Section 1201(a) was quite deliberate.

Congress was well aware during the consideration of the DMCA of the traditional role of the fair use defense in accommodating the exclusive rights of copyright owners with the legitimate interests of noninfringing users of portions of copyrighted works. It recognized the contention, voiced by a range of constituencies concerned with the legislation, that technological controls on access to copyrighted works might erode fair use by preventing access even for uses that would be deemed "fair" if only access might be gained. n162 And it struck a balance among the competing interests.

The first element of the balance was the careful limitation of Section 1201(a)(1)'s prohibition of the act of circumvention to the act itself so as not to "apply to subsequent actions of a person once he or she has obtained authorized access to a copy of a [copyrighted] work. ..." n163 By doing so, it left "the traditional defenses to copyright infringement, including fair use, ... fully applicable" provided "the access is authorized." n164

Second, Congress delayed the effective date of Section 1201(a)(1)'s prohibition of the act of circumvention for two years pending further investigation about how best to reconcile Section 1201(a)(1) with fair use concerns. Following that investigation, which is being carried out in the form of a rule-making by the Register of Copyright, the prohibition will not apply to users of particular classes of copyrighted works who demonstrate that their ability to make noninfringing uses of those classes of works would be affected [*69] adversely by Section 1201(a)(1). n165

Third, it created a series of exceptions to aspects of Section 1201(a) for certain uses that Congress thought "fair," including reverse engineering, security testing, good faith encryption research, and certain uses by

nonprofit libraries, archives and educational institutions.
n166

Defendants claim also that the possibility that DeCSS might be used for the purpose of gaining access to copyrighted works in order to make fair use of those works saves them under *Sony Corp. v. Universal City Studios, Inc.* [*70] n167 But they are mistaken. *Sony* does not apply to the activities with which defendants here are charged. Even if it did, it would not govern here. *Sony* involved a construction of the Copyright Act that has been overruled by the later enactment of the DMCA to the extent of any inconsistency between *Sony* and the new statute.

Sony was a suit for contributory infringement brought against manufacturers of video cassette recorders on the theory that the manufacturers were contributing to infringing home taping of copyrighted television broadcasts. The Supreme Court held that the manufacturers were not liable in view of the substantial numbers of copyright holders who either had authorized or did not object to such taping by viewers. n168 But *Sony* has no application here.

When *Sony* was decided, the only question was whether the manufacturers could be held liable for infringement by those who purchased equipment from them in circumstances in which there were many noninfringing uses for their equipment. But that is not the question now before this Court. The question here is whether the possibility of noninfringing fair use by someone who gains access to a protected copyrighted work through a circumvention technology distributed by the defendants saves the defendants from liability under Section 1201. But nothing in Section 1201 so suggests. By prohibiting the provision of circumvention technology, the DMCA fundamentally altered the landscape. A given device or piece of technology might have "a substantial noninfringing use, and hence be immune from attack under *Sony's* construction of the Copyright Act--but nonetheless still be subject to suppression under Section 1201." n169 Indeed, Congress explicitly noted that Section 1201 does not incorporate

The policy concerns raised by defendants were considered by Congress. Having considered them, Congress crafted a statute that, so far as the applicability of the fair use defense to Section 1201(a) claims is concerned, is crystal clear. In such circumstances, courts may not undo what Congress so plainly has done by

"construing" the words of a statute to accomplish a result that Congress rejected. The fact that Congress elected to leave technologically unsophisticated persons who wish to make fair use of encrypted copyrighted works without the technical means of doing so is a matter for Congress unless Congress' decision contravenes the Constitution, a matter to which the Court turns below. Defendants' statutory fair use argument therefore is entirely without merit.

* * *

VI. Conclusion

In the final analysis, the dispute between these parties is simply put if not necessarily simply resolved.

Plaintiffs have invested huge sums over the years in producing motion pictures in reliance upon a legal framework that, through the law of copyright, has ensured that they will have the exclusive right to copy and distribute those motion pictures for economic gain. They contend that the advent of new technology should not alter this long established structure.

Defendants, on the other hand, are adherents of a movement that believes that information should be available without charge to anyone clever enough to break into the computer systems or data storage media in which it is located. Less radically, they have raised a legitimate concern about the possible impact on traditional fair use of access control measures in the digital era.

Each side is entitled to its views. In our society, however, clashes of competing interests like this are resolved by Congress. For now, at least, Congress has resolved this clash in the DMCA and in plaintiffs' favor. Given the peculiar characteristics of computer programs for circumventing encryption and other access control [*148] measures, the DMCA as applied to posting and linking here does not contravene the First Amendment. Accordingly, plaintiffs are entitled to appropriate injunctive and declaratory relief.

SO ORDERED.

Dated: August 17, 2000

Lewis A. Kaplan

United States District Judge

Anticircumvention Rules: Threat to Science

Pamela Samuelson

Scientists who study encryption or computer security or otherwise reverse engineer technical measures, who make tools enabling them to do this work, and who report the results of their research face new risks of legal liability because of recently adopted rules prohibiting the circumvention of technical measures and manufacture or distribution of circumvention tools. Because all data in digital form can be technically protected, the impact of these rules goes far beyond encryption and computer security research. The scientific community must recognize the harms these rules pose and provide guidance about how to improve the anticircumvention rules.

Recent legislation in the United States and Europe whose ostensible purpose is to protect copyrighted works from pirates is being used to inhibit science and stifle academic research and scholarly communication. The threat to science is illustrated by strong-arm efforts of the Recording Industry Association of America (RIAA) and the Secure Digital Music Initiative (SDMI) Foundation to use the anticircumvention provisions of the Digital Millennium Copyright Act (DMCA) to suppress publication of a paper by Edward Felten of Princeton University's Computer Science Department and several coauthors (1). Felten's paper described weaknesses in digital watermarking technologies that RIAA and SDMI hoped to use to protect commercially distributed digital music (2). RIAA and SDMI asserted that the researchers could not publicly disclose details of their research without violating the DMCA (3). Unfortunately, such an assertion must be taken seriously because all too often in recent years, when courts have perceived a conflict between intellectual property rights and free speech rights, property has trumped speech (4).

Computer security and encryption researchers are far from the only scientists who have reason to fear the DMCA. Any data in digital form can be protected by encryption and other technical measures, and those who distribute digital data in this manner can use the DMCA to restrict what scientists or other researchers can do with the data.

The DMCA establishes several new rules to protect copyright owners. First, the DMCA bans the bypassing of technical measures used by copyright owners to protect access to their works (5). Second, it outlaws the manufacture or distribution of technologies primarily designed or produced to circumvent technical measures used by copyright owners to protect their works (6). Third, it makes

removal or alteration of copyright management information (CMI) from digital copies of copyrighted works illegal (7). Copyright industry lobbyists persuaded Congress to adopt these rules to reassure rights-holders that when they used technology to identify their ownership rights (e.g., by digital watermarks) or to protect digital copies of their works (e.g., by encryption), pirates could not simply strip the CMI from those copies or use countermeasures to undo the encryption to facilitate copyright infringements (8).

The major recording industry firms who belong to RIAA plan to implant watermarks in digital recordings not only to identify their ownership rights but also to ensure that the music can only be played or copied if the watermarks authorize it (9). For this plan to work, the consumer electronics industry and makers of music-player software for PCs must build systems designed to read and conform to these watermarks. SDMI is the multi-industry consortium formed largely at the instigation of RIAA to develop technical standards for watermarks and compliant devices and player software. In September 2000, SDMI announced its selection of certain technologies as candidate standards and issued a public challenge encouraging skilled technologists to try to defeat these technical protection measures (10). SDMI even offered to pay \$10,000 per broken watermark to anyone who demonstrated to SDMI's satisfaction that his or her attack had been successful.

Felten and his collaborators decided to accept the challenge, although they decided against seeking the prize money because SDMI was only willing to award it to those who agreed not to reveal how they defeated the watermarks to anyone but SDMI (11). Felten and his collaborators made no secret of the fact that they were writing a paper on the results of their research about the SDMI watermarks (12). When an executive from the developer of one of the candidate watermarks asked to see the paper, Felten sent him a draft. This executive and RIAA then tried to persuade Felten to omit from the paper cer-

tain details about the weaknesses of the SDMI technologies. Felten and his coauthors decided that these details were necessary to support their scientific conclusions. There ensued numerous conversations between representatives of SDMI and RIAA, on the one hand, and Felten, his coauthors, members of the conference organizing and program committees, and lawyers from institutions with which these persons were affiliated, on the other hand. SDMI and RIAA asserted that any presentation of the paper at a conference or subsequent publication of the paper in the conference proceedings would subject these persons and their institutions to liability under the DMCA and made clear their intent to take action against the researchers unless they withdrew the paper (13).

Although convinced that they would be vindicated if the matter went to court, Felten and his coauthors reluctantly withdrew the paper from the April conference out of concern about the high costs of litigation (14). This decision was widely reported in the press and has had a chilling effect on the willingness of cryptographers to publish the results of their research (15). Since then, the Electronic Frontier Foundation has agreed to represent Felten and his coauthors in an affirmative challenge to the RIAA and SDMI claim that seeks a judicial declaration that presenting or publishing this paper does not violate the DMCA (16).

The idea that Felten's paper violates the DMCA initially seems absurd on its face. Whatever plausibility it has is due to a broad interpretation given to the DMCA rules in a trial court decision in *Universal City Studios, Inc. v. Reimerdes* in August 2000 (17). Universal sued *2600* Magazine and its publisher Eric Corley (a.k.a. Emmanuel Goldstein) because *2600* posted a copy of a computer program, known as DeCSS, as part of its story about a young Norwegian hacker Jon Johanssen who figured out how to bypass the Content Scrambling System (CSS) used to protect commercially distributed DVD movies. Johanssen wrote DeCSS and posted it on the Web so that others could benefit from what he had learned. Universal convinced the trial judge that DeCSS was an illegal circumvention technology, the public availability of which threatened the viability of the motion picture industry (even though Universal did not produce any evidence that DeCSS had ever actually been used to make an infringing copy of the plaintiffs' movies; it was enough, in Universal's view, that the program could be used for this purpose).

School of Information Management and Law, University of California, Berkeley, CA 94720, USA. E-mail: pam@sims.berkeley.edu

After being ordered in January 2000 to take down DeCSS from the 2600 site, Corley decided to link to sites where DeCSS could be found. In August 2000, the trial judge ruled that linking also violated the DMCA and forbade posting or linking to source or object code forms of DeCSS. The judge rejected Corley's First Amendment defense because of the functionality of DeCSS and the danger that the program posed to Universal's market for copyrighted movies. Under this judge's reasoning, even an English-language version of DeCSS might violate the DMCA.

SDMI and RIAA regard Felten's paper as providing a functional recipe for circumventing the SDMI watermarks that posed dangers to the recording industry akin to those that DeCSS posed for the motion picture industry. SDMI and RIAA have not been willing to concede that writing and distributing a paper describing the results of reverse engineering of a technical protection measure are different from writing and distributing an executable program capable of defeating that measure [but for the fact that SDMI issued a public challenge to the technical community to try to break the technical protections they had devised, SDMI and RIAA would undoubtedly argue that the reverse engineering of publicly disseminated watermarking technologies, whether for academic research or for piratical purposes, violates the DMCA rule against alteration or removal of copyright management information (18)].

The ruling against Corley is on appeal. One can always hope that the appeals court will give the DMCA a narrower interpretation than the trial judge did and that this narrower interpretation will propagate in other cases. In the meantime, the DMCA is a cloud on the horizon for all computer security and encryption researchers, whether they operate in an academic or commercial setting, if their work has any potential application to protecting digital content.

Although the DMCA rules contain narrow exceptions for computer security and encryption research, practitioners in these fields take little comfort in them (19). Several prominent cryptographers submitted an amicus (friend of the court) brief in the Corley case in which they characterized the encryption research exception as "so parsimonious as to be of little practical value" as well as being based on a "fundamentally mistaken conception of cryptographic science" (20, 21). It applies, for example, only if the researcher is employed or has been trained as a cryptographer, even though some brilliant breakthroughs in this field have come from amateurs (22). The researcher must also seek permission from affected rights-holders before trying to reverse engineer encryption technology (23). The exception further requires the researcher to prove that his or her research was neces-

sary to advance the state of the art when the researcher may just be trying to understand how a technology works (24). In addition, the exception may be unavailable if the researcher publishes his or her results on the Internet because this will make them accessible to potential pirates (25). But the most fundamental point is that "the science of cryptography depends on cryptographers' ability to exchange ideas in code, to test and refine those ideas, and to challenge them with their own code. By communicating with other researchers and testing one another's work, cryptographers can improve the technologies they work with, discard those that fail, and gain confidence in technologies that have withstood repeated testing" (20). Encryption and computer security cannot get stronger if researchers in these fields are at risk of liability from the DMCA for merely working in their chosen field and communicating with one another about it.

The implications of the DMCA for science are not limited to computer security and encryption researchers. Virtually all computer scientists, as well as many other scientists with some programming skills, find it necessary on occasion to reverse engineer computer programs. Sometimes they have to bypass an authentication procedure or some other technical measure in order to find out how the program works, how to fix it, or how to adapt it in some way. The act of bypassing the authentication procedure or other technical measure, as well as the making of a tool to aid the reverse engineering process, may violate the DMCA.

Although the DMCA also has an exception for reverse engineering of a program (26), it too is narrow. It only applies if the sole purpose of the reverse engineering is to achieve program-to-program interoperability and if reverse engineering is necessary to do so (27). Trying to fix a bug or understand the underlying algorithm does not qualify. Information even incidentally learned in the course of a privileged reverse engineering process cannot be divulged to any other person except for the sole purposes of enabling program-to-program interoperability (28). Under a strict interpretation of the DMCA, a reverse engineer could not, for example, publish lawfully obtained interface information or details of the program's authentication technique in an academic or research paper.

Other evidence of the narrowness of the reverse engineering exception can be seen in the trial judge's response to Corley's interoperability defense (29). Jon Johanssen testified at Corley's trial that he developed DeCSS to help the Linux programmers develop a Linux-based DVD player. The judge rejected this defense for several reasons: First, DeCSS did not have as its sole purpose the achieving of interoperability because it could also be used to bypass CSS on a Windows-based

system. Second, DeCSS might help achieve data-to-program interoperability, but the statutory exception only permits program-to-program interoperability. Third, even if Johanssen had been eligible for the interoperability privilege, Corley—a mere journalist—was not because he was not trying to develop an interoperable program.

Of course, any data in digital form—not just sound recordings and motion pictures—can be protected by technical measures. Those who disseminate digital data may want to restrict what researchers can do with the data. Imagine, for example, that a pharmaceutical company produces data to prove that a new drug is safe but technically protects it so that only certain tests can be performed on the data, all of which support the safety claim. A scientist who doubted the safety claim and tried to process the data by additional tests would violate the DMCA if he or she bypassed the access control system restricting use of the data (30).

Or imagine that this pharmaceutical firm put the data on an access-controlled Web site available only to those who agreed to licensing terms forbidding use or disclosure of the data or test results except as authorized in the license. A scientist who tried to access the data without agreeing to the license might also run afoul of the DMCA. Microsoft once posted a certain technical specification on a Web site, access to which was designed to be available to researchers only if they clicked "I agree" to a license that forbade disclosing details of the specification (31). A smart technologist figured out how to bypass the click-through license and posted instructions about it on slashdot.org, after which there was a heated debate about the specification on slashdot. Microsoft learned about the slashdot postings and demanded that slashdot delete these messages on the theory that they violated the DMCA's anticircumvention rules. Microsoft is surely not the only entity in the world that wants to control a wider community's use of its information and will find the DMCA a useful tool for achieving this objective.

Advances in technology now permit very fine-grained control over access to and use of information. This control has been powerfully reinforced by the DMCA, and it enables firms and individuals to engage in "privication" (i.e., "the mass distribution of information to 'authorized' users with tight control over its use") (32, p. 1218). This disturbing practice may well creep from one subdiscipline of science to another unless the scientific community recognizes the potential threat that privication and the DMCA pose for preservation of the norms and practices of science.

The question, then, is whether science can do something about it. I am optimistic that the scientific community can make a differ-

ence because it has been able to mobilize and make an effective case for policy change when expansions of intellectual property rights, actual or proposed, were about to have serious repercussions for science (33). The scientific community has played an important role in holding back a vast expansion of intellectual property rights to the contents of databases.

Back in 1996, the European Commission realized that many commercially valuable databases did not qualify for copyright protection because they exhibited insufficient creativity in selection and arrangement of data and that when databases did qualify for protection, the copyright in them did not protect the data themselves from being reselected and rearranged. So the Commission proposed a new form of intellectual property protection for the contents of databases, and in 1996, this new legal regime was mandated in the European Union. Now any person or firm that expends substantial resources in compiling data in the European Union has a legal right to prevent anyone else from extracting or reusing all or a substantial part (whatever that means) of the contents of the database for 15 years (34). Additional expenditures in maintaining the database will renew the term of protection, which arguably gives European data compilers perpetual rights in the data in their databases (35).

Although scientists in Europe seem not to have been consulted when this law was wending its way through the European Commission and Parliamentary approval process, scientists in the United States recognized that such a law posed serious problems for traditional norms and practices of science (36). They did not object to giving databases some legal protection but argued that the European Union database right went too far. So they organized a successful effort in late 1996 to persuade the Clinton Administration to back away from support for an international treaty to universalize the European database rules that a senior U.S. official had previously endorsed (37). These organizations also helped to persuade the Clinton Administration to moderate its stance on several digital copyright issues, including whether fair use would survive in the digital age, scheduled for consideration at a diplomatic conference in December 1996 (38). Thanks in no small part to these efforts, the treaty eventually adopted was balanced and sound.

Since 1996, the American Association for the Advancement of Science and the National Academies of Science and Engineering have been among the scientific organizations that have worked together to oppose European Union-style database legislation in Congress and in the international arena (39). So far they have been successful, but database bills will be back, and victory in future rounds will depend on continued vigilance.

The scientific community has not been as active about the DMCA anticircumvention rules, perhaps because the threat they posed seemed too abstract and diffuse. But now that the threat that these overbroad rules pose for science is more evident and immediate, it may be the right time to focus on the DMCA. There are at least two ways to do this. One is to submit amicus briefs in pending cases to urge courts to give narrow interpretations to these rules to mitigate the harm to science. Another is to make suggestions to Congress about how the DMCA could be modified to provide a better balance between protection for copyrighted works and protection for scientific research and communications.

One thing is certain: Better anticircumvention rules will not come about just because it is the right thing to do. This will only happen if the scientific community and others harmed by these overbroad rules are able to articulate why the DMCA rules are harmful and how legal decision makers can fix the problems with this legislation.

References and Notes

- See, e.g., C. C. Mann, "Secure-Music Group Threatens Researchers Who Plan to Publish on Hacking Success," *Inside Magazine*, 22 April 2001, available at www.inside.com.
- The paper was entitled "Reading Between the Lines: Lessons from the SDMI Challenge" and was scheduled for presentation at the Fourth International Information Hiding Workshop in Pittsburgh, PA, on 26 April 2001. For further details, see SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
- A copy of the RIAA letter to Felten asserting that presentation or publication of the researchers' paper would violate the DMCA is available at cryptome.org/sdmi-attack.htm.
- See, e.g., M. A. Lemley, E. Volokh, *Duke Law J.* **48**, 147 (1999) (giving examples).
- 17 U.S.C. sec. 1201(a)(1)(A). This provision is subject to seven exceptions, three of which are discussed in this viewpoint. For a critical commentary on the DMCA anticircumvention regulations, see, e.g., P. Samuelson, *Berkeley Technol. Law J.* **14**, 519 (1999).
- 17 U.S.C. sec. 1201(a)(2), 1201(b)(1). Subsection (a)(2) pertains to technologies that bypass access controls and (b)(1) to technologies that bypass other technical measures (e.g., copy controls) used by copyright owners to protect their works.
- 17 U.S.C. sec. 1202. Unlike section 1201, this rule has no exceptions for research or other legitimate purposes.
- See WIPO Copyright Treaties Implementation Act and Online Copyright Liability Limitation Act: Hearings on H.R. 2281 and H.R. 2280 Before the Subcommittee on the Courts and Intellectual Property of the House Committee on the Judiciary, 105th Congress (1997) (statements of Jack Valenti, Robert Holleyman, and Allan R. Adler in support of the anticircumvention rules).
- For a concise description of the intended role of watermarks in protecting digital music in compliant devices, see the SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
- See "An Open Letter to the Digital Community" available at www.sdmi.org/pr/OL_Sept_28_2000.htm.
- This is explained in the SDMI challenge FAQ at www.cs.princeton.edu/sip/sdmi/faq.html.
- The facts in this paragraph are set forth in the complaint filed by the Electronic Frontier Foundation on behalf of Felten and his coauthors against RIAA and SDMI, which is available at www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_complaint.html.
- Also challenged was a chapter of a Princeton Ph.D. student's dissertation that discussed the SDMI challenge. This student successfully defended her dissertation and, in keeping with standard practice in her field, posted the dissertation on the Internet. Out of an abundance of caution after withdrawal of the Felten paper (of which she was a coauthor) from the April conference, she removed the SDMI chapter from the Internet.
- Felten's statement when he announced withdrawal of the paper from the April conference is available at cryptome.org/sdmi-attack.htm.
- See, e.g., (7); K. Dawson, "Watermarks...or Freedom?," *Industry Standard*, 7 May 2001. One Dutch cryptographer, Niels Ferguson, has explained the chilling effects that the DMCA has had on his willingness to publish the results of his research at macfergus.com/niels/dmca/index.html.
- The complaint is available at www.eff.org/Legal/Cases/Felten_v_RIAA/20010606_eff_complaint.html. Felten finally presented the paper at a USENIX conference on 15 August 2001. However, he and his coauthors continue to be concerned about DMCA liability for reasons set forth in court papers filed in response to RIAA's motion to dismiss the Felten lawsuit (also available on the www.eff.org). These concerns have been amplified by the recent arrest of a Russian programmer, Dmitri Sklyarov, for criminal violation of the DMCA rules because he wrote a program capable of bypassing an Adobe e-book program.
- Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294 (S.D.N.Y. 2000).
- The *Felton v. RIAA* complaint in (12) reflects concerns that the defendants claim that the researchers violated 1202 as well as 1201.
- 17 U.S.C. sec. 1201(g), 1201(j). Felten may not be eligible for either privilege because the SDMI watermarks are not encryption and because the computer security exception does not apply to 1201(b), but only to 1201(a)(2). Neither privilege applies to 1202 claims.
- Brief of Amici Curiae of S. Bellovin, M. Blaze, D. Boneh, D. Del Torto, I. Goldberg, B. Schneier, F. A. Stevenson, D. Wagner, in *Universal City Studios, Inc. v. Reimerdes*, to the Second Circuit Court of Appeals, 26 January 2001, available at eon.law.harvard.edu/openlaw/DVD/NY/appeal/000126-cryptographers-amicus.html.
- Problems with the overly narrow and ambiguous encryption and computer security exceptions to the DMCA are discussed by the National Research Council [*The Digital Dilemma: Intellectual Property in the Information Age 174-75, Appendix G* (National Academies of Sciences Press, Washington, DC, 2000)].
- 17 U.S.C. sec. 1201(g)(3)(B).
- 17 U.S.C. sec. 1201(g)(2)(C). The computer security exception requires that the researcher actually get, and not just ask for, permission to defeat the technical protection measure. 17 U.S.C. sec. 1201(j)(1).
- 17 U.S.C. sec. 1201(g)(1), (g)(2)(B).
- 17 U.S.C. sec. 1201(g)(3)(A). The encryption researcher must also provide affected copyright owners with the results of his or her research in a timely manner. 17 U.S.C. sec. 1201(g)(3)(D).
- 17 U.S.C. sec. 1201(f).
- 17 U.S.C. sec. 1201(f)(1).
- 17 U.S.C. sec. 1201(f)(3).
- The interoperability defense is discussed in *Universal City Studios, Inc. v. Reimerdes*, 82 F. Supp. 211 (S.D.N.Y. 2000) (ruling on the preliminary injunction motion), 111 F. Supp. 2d 294 (S.D.N.Y. 2000) (ruling after trial).
- See A. W. Appel, E. W. Felten, *Comm. ACM* **43**, 21 (September 2000) (giving examples of academic research that might be illegal under a strict interpretation of the DMCA rules).
- See J. E. Cohen, "Unfair Use," *The New Republic*, 23 May 2000 (available at www.tnr.com/online/cohen052300.html).
- J. Zittrun, *Stanford Law Rev.* **52**, 1201 (2000).
- The scientific community expressed doubts, for example, about the patenting of expressed sequence tags (ESTs) of DNA of unknown functionality. The U.S. Patent and Trademark Office thereafter issued new guidelines to require a known utility for patent-

- ing of ESTs that substantially alleviated, even if they did not totally resolve, this threat to science from overbroad patent rights.
34. Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases, 1996 O.J (L 77) 20.
35. For a critical commentary on the EU database directive

- and kindred U.S. legislation, see, e.g., J. H. Reichman, P. Samuelson, *Vanderbilt Law Rev.* 50, 51 (1997).
36. See, e.g., National Research Council, *Bits of Power: Issues in Global Access to Scientific Data* (National Academy of Sciences Press, Washington, DC, 1997) (expressing concern about European Union-style database protection).

37. The role of scientific organizations in facilitating changes in U.S. policy is recounted in (38).
38. P. Samuelson, *Va. J. Intl. Law* 37, 369 (1997).
39. These efforts are recounted by J. H. Reichman and P. F. Uhlir [*Berkeley Technol. Law J.* 14, 793 (1999)].
40. I gratefully acknowledge research support from NSF grant SEC-9979852.

VIEWPOINT

Computer Networks As Social Networks

Barry Wellman

Computer networks are inherently social networks, linking people, organizations, and knowledge. They are social institutions that should not be studied in isolation but as integrated into everyday lives. The proliferation of computer networks has facilitated a deemphasis on group solidarities at work and in the community and afforded a turn to networked societies that are loosely bounded and sparsely knit. The Internet increases people's social capital, increasing contact with friends and relatives who live nearby and far away. New tools must be developed to help people navigate and find knowledge in complex, fragmented, networked societies.

Once upon a time, computers were not social beings. Most stood alone, be they mainframe, mini, or personal computer. Each person who used a computer sat alone in front of a keyboard and screen. To help people deal with their computers, the field of human-computer interaction (HCI) developed, providing such things as more accessible interfaces and user-friendly software. But as the HCI name says, the model was person-computer.

Computers have increasingly reached out to each other. Starting in the 1960s, people began piggybacking on machine-machine data transfers to send each other messages. Communication soon spilled over organizational boundaries. The proliferation of electronic mail (e-mail) in the 1980s and its expansion into the Internet in the 1990s (based on e-mail and the Web) have so tied things together that to many, being at a computer is synonymous with being connected to the Internet.

As a result, HCI has become socialized. Much of the discussion at current HCI conferences is about how people use computers to relate to each other (1). Some participants build "groupware" to support such interactions; others do ethnographic, laboratory, and survey studies to ascertain how people actually relate to each other. This work has slowly moved from the lone computer user to dealing with (i) how two people relate to each other online, (ii) how small groups interact, and (iii) how large unbounded systems operate—the ultimate being the worldwide Internet, the largest and most fully connected so-

cial network of them all. Just one small portion of the Internet—Usenet members—participated in more than 80,000 topic-oriented collective discussion groups in 2000. 8.1 million unique participants posted 151 million messages (2–4). This is more than three times the number identified on 27 January 1996 (5)

Computer scientists and developers have come to realize that when computer systems connect people and organizations, they are inherently social. They are also coming to realize that the popular term "groupware" is misleading, because computer networks principally support social networks, not groups. A group is only one special type of a social network; one that is heavily interconnected and clearly bounded. Much social organization no longer fits the group model. Work, community, and domestic life have largely moved from hierarchically arranged, densely knit, bounded groups to social networks.

In networked societies, boundaries are more permeable, interactions are with diverse others, linkages switch between multiple networks, and hierarchies are flatter and more recursive (6–8). Hence, many people and organizations communicate with others in ways that ramify across group boundaries. Rather than relating to one group, they cycle through interactions with a variety of others, at work or in the community. Their work and community networks are diffuse and sparsely knit, with vague overlapping social and spatial boundaries. Their computer-mediated communication has become part of their everyday lives, rather than being a separate set of relationships.

When computer-mediated communication networks link people, institutions, and knowledge, they are computer-supported social networks. Indeed, if Novell had not gotten there

first, computer scientists would be saying "netware" instead of "groupware" for systems that enable people to interact with each other online. Often computer networks and social networks work conjointly, with computer networks linking people in social networks and with people bringing their offline situations to bear when they use computer networks to interact.

The intersection of computer networks with the emerging networked society has fostered several exciting developments. I report here on two developing areas: (i) community networks on- and offline and (ii) knowledge access.

Community Networks On- and Offline

Community, like computers, has become networked. Although community was once synonymous with densely knit, bounded neighborhood groups, it is now seen as a less bounded social network of relationships that provide sociability support, information, and a sense of belonging. These communities are partial (people cycle through interactions with multiple sets of others) and ramify through space [a low proportion of community members in the developed world are neighbors (7)]. Where once people interacted door-to-door in villages (subject to public support and social control), they now interact household-to-household and person-to-person (9).

Although the support of collaborative work was the initial purpose of the Internet (both e-mail and the Web), it is an excellent medium for supporting far-flung, intermittent, networked communities. E-mail transcends physical propinquity and mutual availability; e-mail lists enable broadcasts to multiple community members; attachments and Web sites allow documents, pictures, and videos to be passed along; buddy lists and other awareness tools show who might be available for communication at any one time; and instant messaging means that simultaneous communication can happen online as well as face-to-face and by telephone.

Systematic research on what people actually do on the Internet has lagged behind the Internet's development. After a long

FREE DMITRY? SPARE ME.:
WHY THE FBI WAS RIGHT TO ARREST THE INTERNET'S LATEST MARTYR

Roger Parloff
INSIDE.COM
August 1, 2001

Civil liberties advocates, programmers and cryptographers are up in arms about the arrest of a Russian programmer for distributing software that strips Adobe eBook Reader of its copy-protection. They shouldn't be, Inside's legal editor argues

A hacker has allegedly violated the Digital Millennium Copyright Act -- so you know the drill. It's time for extremely smart people to espouse extremely unpersuasive arguments for why the hacker must swiftly be exonerated and the law struck down as unconstitutional.

This time around the hacker (and I'm trying to use that term in the positive sense) is Dmitry Sklyarov, a 27-year-old Russian computer programmer who was arrested in Las Vegas on July 16. If you get your news from any of the numerous news sources that cater to computer programmers and software enthusiasts -- the online wire services or listserv e-mails from digital civil liberties advocates or cryptographers -- you are doubtless familiar with the outlines of the case, or at least think you are. You have read how Sklyarov was arrested the day after he delivered a lecture at the Def Con 9 convention in Las Vegas -- the ninth annual gathering of what is described on the group's official Web site as "computer underground party for hackers" -- about the flaws in the copy-protection system for the Adobe eBook Reader.

Maybe you have been alerted to the message posted on the Web by Bruce Schneier, the chief technology officer of Counterpane Internet Security and one of the nation's foremost experts on cryptography and computer systems security, who has expressed his outrage that "the FBI arrested (Sklyarov) because he presented a paper on the strengths and weaknesses of software used to protect electronic books." You have probably been told how Alan Cox, an eminent British open-source programmer, resigned his membership in an American-based society of computer engineers as a result of Sklyarov's arrest, explaining: "With the arrest of Dmitry Sklyarov, it has become apparent that it is not safe for non-U.S. software engineers to visit the United States." You may also agree with Sklyarov's defenders that it is deeply ironic that federal

prosecutors are trying to punish Sklyarov at Adobe's behest, when Adobe should really be thanking Sklyarov for having -- in the long and fine tradition of hackers (again in the positive sense of that term) -- pointed out flaws in its copy-control system, which might have done far greater damage had they first been discovered by someone malevolent.

Then again, if you've learned about the case from more mainstream news sources, you probably already realize that Sklyarov's arrest doesn't really have anything to do with the presentation he gave in Las Vegas. (The conference, which listed Sklyarov as a scheduled speaker, was just the event that alerted authorities to the fact that he would be in the United States, enabling them to seize him.) It relates to some software that Sklyarov wrote and that his employer distributed.

But even so, you may still be outraged by his arrest. As Stanford Law School professor Lawrence Lessig recently pointed out in his New York Times op-ed piece urging Sklyarov's release, Sklyarov's software was perfectly lawful in Russia, where he wrote it. Adobe just downloaded it off the Internet, and then asked our government to punish Sklyarov for violating U.S. law. That poses all sorts of very troubling, international jurisdictional issues, doesn't it?

In addition, Professor Lessig stresses, neither Sklyarov nor his employer have even been charged with infringing anyone's copyrights! Sklyarov simply made software that removes certain security protections from the Adobe eBook Reader, enabling people to engage in numberless, marvelous, invaluable, noninfringing uses. "A blind person," for instance, could use it to activate Adobe's "read-aloud function" in order "to listen to a book," even if Adobe had, at a publisher's instructions, disabled that function for a particular title. Alas, has helping the blind to read become a crime in our country? Sklyarov's wonderful creation also enables people to make back-up copies of e-books, explains the Electronic Frontier Foundation's Web site. It also enables them to transfer an e-book from an old computer to a new one. Best of all, Sklyarov's software only works on lawfully purchased e-books. So what in the world could the prosecutors and Adobe and the Association of American Publishers -- which has applauded the prosecution -- possibly be so upset about?

ON THE WEB, IT ONLY TAKES A SINGLE UNPROTECTED COPY ...

Now let's visit Planet Earth. Dmitry Sklyarov works for ElcomSoft Co. Ltd., a Moscow-based company that sells, among other things, the Advanced eBook Processor. That product converts e-books formatted for viewing through the Adobe eBook Reader into

ordinary, unsecured PDF files. Once in that form, the file is in the free and clear, and can be distributed by anyone to anyone throughout the globe via numerous file-sharing programs like Gnutella, KaZaA, iMesh or Freenet, not to mention by e-mail attachment, or by Aimster-style instant-messaging attachment, or by posting on evanescent pirate Web sites, and probably via several other mechanisms that were invented so recently that you and I haven't heard of them yet.

The point is: it only takes a single unprotected copy to have the material spread. The cat is then out of the bag and any attempt to bring a copyright infringement charge against the individual who originally uploaded it becomes laughably futile, even assuming it were possible to identify that individual, which it usually isn't. Accordingly, Congress has tried to protect copyrights in the digital world by prohibiting the distribution of "devices" -- like Elcomsoft's Advanced eBook Processor -- that are "primarily designed" to circumvent copy-control technologies that copyright holders have implemented in an effort to protect their intellectual property. (The DMCA is designed to effectuate two World Intellectual Property Organization copyright treaties that were signed in Geneva in December 1996.)

Most of the people coming to Sklyarov's defense fully appreciate that some sort of anti-circumvention legislation like the DMCA is crucial to maintaining meaningful copyright protection in the digital world. But they simply don't want such protection maintained. They believe that the digital world is fundamentally hostile to copyright law as we have known it and that the copyright laws have grown too protective in any event (which might be true), and they are therefore eager to enter a brave new world in which creators of intellectual property will be effectively forced to turn to unspecified "new business models" in an effort to get paid for their creations. Most of the new business models that have been proposed so far, however -- like having consumers voluntarily donate fees to creators whose works they have downloaded for free -- very closely resemble begging.

In any event, there is little question that ElcomSoft has been knowingly and intentionally violating U.S. law and that the FBI has ample jurisdiction over Sklyarov. Until Sklyarov's arrest -- when ElcomSoft finally discontinued distributing these circumvention products -- ElcomSoft made a demonstration model of its Adobe-targeted circumvention software available on its (English-language) Web site for free. But that demo tantalizingly unlocked only the first 10 percent of an Adobe e-book, according to the ElcomSoft site (which was quoted in the July 10 affidavit of an FBI agent filed in support of the criminal complaint against Sklyarov). If a customer wanted to unlock the whole Adobe e-book, ElcomSoft directed that person to send \$99 -- that's U.S. dollars -- to ElcomSoft's U.S.-

based billing agent, Register Now, which is based in Issaquah, Wash. Upon verifying that payment had been made, ElcomSoft would then e-mail the customer -- including U.S. customers -- a key that would fully activate the software, enabling the customer to unlock and copy entire Adobe-formatted e-books. (By the way, if Sklyarov's or ElcomSoft's goal had been to alert Adobe to potential flaws in its software, the demo version would have fully accomplished that purpose. Evidently, that wasn't the goal.)

Nor should Sklyarov's July 16 arrest have come as a surprise to either ElcomSoft or Sklyarov, unless ElcomSoft was cruelly keeping Sklyarov in the dark about Adobe's dissatisfaction with ElcomSoft's business operations. On June 25, Adobe's anti-piracy unit warned ElcomSoft that its product was illegal and demanded that the product be removed from its Web site. ElcomSoft refused. On June 25, Adobe also demanded that ElcomSoft's Internet Service Provider, Verio Inc., terminate ElcomSoft's service if ElcomSoft did not take down the Adobe circumvention software. After Verio told ElcomSoft of the demand, ElcomSoft switched ISPs, managing to keep its site afloat, though Verio cut off service by June 27. On June 28, Adobe demanded that Register Now stop serving as ElcomSoft's billing agent, prompting ElcomSoft to advise Register Now that it had better protect itself by honoring Adobe's demand. It is unclear whether ElcomSoft planned to arrange a substitute method of payment.

WHY CHARGE DMITRY, AND NOT THE COMPANY?

In sum, then, the FBI alleges that ElcomSoft had been marketing software to Americans from an English-language Web site, soliciting payment in American money through an American billing agent, and then sending Americans a key that would enable Americans to defeat the security protections built into an American-made product. So while some may be outraged that the U.S. government would attempt to impose its laws upon a Russian company under these circumstances, I am unmoved.

In fairness, however, the government hasn't charged ElcomSoft with a crime, it has charged its employee, Sklyarov. Why him? An FBI agent noticed that when he called up Elcomsoft's circumvention software on a computer, the software displayed a title page indicating that the software had been copyrighted in the name of Dmitry Sklyarov. (Yes, ElcomSoft's officials evidently believe in protections for some intellectual property -- their own.) That led the agent to conclude that Sklyarov had created the circumvention software that his employer was distributing in the United States. Though the Electronic Frontier Foundation and ElcomSoft's president and owner, Alexander Katalov, are now both suggesting that maybe Sklyarov played only a bit role in creating the Advanced

eBook Processor, Sklyarov in a post-arrest interview with a local television new reporter acknowledged having written it. (A video clip of this interview is still available on the Electronic Frontier Foundation's Web site.) Similarly, an explanatory Web page about the case provided by ElcomSoft asserts that Sklyarov "wrote" the program.

On July 2, the same FBI agent who made the Sklyarov connection visited the Def Con 9 Web site and saw that Sklyarov was scheduled to appear at the convention in Las Vegas on July 13-15. When Sklyarov in fact appeared, he was arrested on a criminal complaint from the Northern District of California, the district that includes San Jose, where Adobe Systems is headquartered. If ElcomSoft president Katalov is now willing to subject himself to U.S. jurisdiction, it would certainly seem preferable to arrest him and release Sklyarov, but in the meantime the FBI seems to have an ample basis for exercising jurisdiction over Sklyarov, and for accusing him of helping to distribute illegal circumvention software in the United States. Whether prosecutors can ultimately prove beyond a reasonable doubt that Sklyarov -- as opposed to ElcomSoft -- "manufactured, imported, offered to the public, provided, or otherwise trafficked" in that software is a question that depends on facts and evidence which neither I nor any other commentator is currently in a position to evaluate.

But what about the fate of all those blind people who now won't be able to read e-books because Adobe will have disabled the read-aloud feature at some publisher's request? Typically, publishers ask Adobe to disable that feature when they fear it might violate their contracts relating to an existing audio version of the same book. But when you think about it, in those circumstances it might actually make more sense for a blind person to pay \$15 to buy the audio book -- a tape of a professional actor or the author of the work reading the book aloud -- rather than pay \$8 for an e-book and \$99 for circumvention software, in order to hear voice-simulation software articulating the words in a robotic monotone.

THE EFFECT OF BOYCOTT THREATS

But what will everyone now do when they need to make backup copies? Well, again, since most e-books cost somewhere between nothing and \$8, it might be more sensible to buy a new copy of the book than the \$99 circumvention software required to make a backup. If you save some proof of purchase, you might even be able to talk Amazon.com or the publisher into sending you a new e-book for free. It's a brand new industry, and if it is not yet possible to insure yourself against loss from a crashed system, the exigencies of the market guarantee that it soon will be. It would be surprising if the only possible

solution to this minor inconvenience was to legalize the distribution of circumvention software, thereby guaranteeing the demise of copyright protection as we know it.

On July 23, after meeting with representatives of the Electronic Frontier Foundation -- and faced with imminent protests and commercial boycotts organized by geek activists - - Adobe issued a carefully worded statement recommending release of Sklyarov and withdrawing its support for the government's complaint. "We strongly support the DMCA and the enforcement of the copyright protection of digital content," said Colleen Pouliot, Adobe's senior vice president and general counsel, in the statement. "However, the prosecution of this individual in this particular case is not conducive to the best interests of any of the parties involved or the industry. ElcomSoft's Advanced eBook Processor software is no longer available in the United States, and from that perspective the DMCA worked."

The government has so far declined to drop the case, however. Given that the government's interest in enforcing the nation's laws are always broader than any individual complainant's -- and given the circumstances under which this particular complainant was mau-maued into backing away from a case it had initiated -- the government is probably doing the right thing.

While we can all applaud the Electronic Frontier Society and its allies for their dogged and vigilant commitment to free speech, every once in awhile it would be refreshing to see those advocates show a comparable commitment to candid speech.