

1 SCOTT P. COOPER (Cal. Bar No. 96905)
2 PROSKAUER ROSE LLP
2049 Century Park East, Suite 3200
Los Angeles, CA 90067
3 Telephone: (310) 557-2900
Facsimile: (310) 557-2193
4 *Attorneys for the MGM, Fox, Universal, Viacom,*
5 *Disney & NBC Plaintiffs*

6 ROBERT M. SCHWARTZ (Cal. Bar No. 117166)
O'MELVENY & MYERS LLP
7 1999 Avenue of the Stars, Seventh Floor
Los Angeles, California 90067-6035
8 Telephone: (310) 553-6700
Facsimile: (310) 246-6779
9 *Attorneys for the Time Warner Plaintiffs*

10 ROBERT H. ROTSTEIN (Cal. Bar No. 72452)
McDERMOTT, WILL & EMERY
11 2049 Century Park East, 34th Floor
Los Angeles, CA 90067
12 Telephone: (310) 277-4110
Facsimile: (310) 277-4730
13 *Attorneys for the Columbia Plaintiffs*

14
15 **UNITED STATES DISTRICT COURT**
16 **CENTRAL DISTRICT OF CALIFORNIA**
17

18 PARAMOUNT PICTURES
19 CORPORATION *et al.*,
20 Plaintiffs,

21 v.

22 REPLAYTV, INC. *et al.*,
23 Defendants.

CASE NO. CV 01-9358 FMC (Ex)
Hon. Florence-Marie Cooper
DECLARATION OF MICHAEL H.
WEISS IN SUPPORT OF THE
COPYRIGHT OWNER PLAINTIFFS'
MOTION FOR PROTECTIVE ORDER

24 AND CONSOLIDATED ACTIONS.
25
26
27
28

1 Discussion Subgroup to the Copy Protection Technical Working Group – June 3,
2 2002,” and is what it purports to be. This subgroup is commonly referred to as
3 “BPDG.”

4 7. Attached as Exhibit J is a true and correct copy of a published article
5 titled “Industry Groups See Limited Consensus on Broadcast Flag Standard,” from
6 a publication titled “Public Broadcasting Report,” published by Warren Publishing,
7 Inc. This article was located through a LEXIS search, and quotes EFF “staff
8 technologist” Seth Schoen on the second page.

9 8. Attached as Exhibit K is a true and correct copy of the “Featured
10 News” as presented on EFF’s website. I obtained Exhibit K from EFF’s website
11 and cite it for its reference to a headline that appears on the second page, which
12 starts, “FCC to Announce . . .”

13 9. Attached as Exhibit L is a true and correct copy of one of many so-
14 called “Action Alerts” that are posted on EFF’s website. This particular posting,
15 titled: “ALERT: Congress Call for Public Participation on Digital Music Issues,”
16 shows an “Issued” date of March 22, 2002. I obtained Exhibit L from EFF’s
17 website.

18 10. Attached as Exhibit M is a true and correct copy of a document titled
19 “Testimony of Electronic Frontier Foundation (EFF) Before Copyright Office –
20 Public Hearings on Digital Millennium Copyright Act (DMCA), May 19, 2002.”
21 This document is maintained on a website called “Virtual Recordings.” One of the
22 four links on the website is titled “Hot Topics in High Tech Law: Articles on
23 Cyberspace Law and Intellectual Property Law by Robin D. Gross, Esq.” I
24 obtained Exhibit M from this link.

25 11. Attached as Exhibit N is a true and correct copy of a posting from
26 EFF’s website, titled “Active EFF Legal Cases and Efforts.” The three cases in
27 which EFF is involved, as mentioned in Separate Statement ,are identified and
28 discussed in Exhibit N.

EXHIBIT A

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ENTERED
CLERK U.S. DISTRICT COURT
AUG 16 2002
CENTRAL DISTRICT OF CALIFORNIA
BY [Signature]

FILED
CLERK US DISTRICT COURT
AUG 15 2002
CENTRAL DISTRICT OF CALIFORNIA
DEPUTY
[Signature] [Signature]

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

CRAIG NEWMARK, et al.,

Plaintiffs,

vs.

**TURNER BROADCASTING
NETWORK, et al.,**

Defendants.

CV 02-04445 FMC (Ex)

**ORDER DENYING MOTION TO
DISMISS; ORDER DENYING
MOTION TO STAY; ORDER
GRANTING MOTION TO
CONSOLIDATE**

This matter is before the Court on Defendants' Motion to Dismiss or, Alternatively, to Stay Proceedings, and Plaintiffs' Motion to Consolidate. These matters were heard on August 12, 2002, at which time the parties were in receipt of the Court's tentative order. For the reasons set forth below, the Court hereby denies the Motion to Dismiss (docket #43-1), hereby denies the Motion to Stay (docket #43-2), and hereby grants the Motion to Consolidate (docket #45).

1 **I. Background**

2 The parties are well-acquainted with the nature of the present action and
3 *Paramount Pictures Corporation v. RePlayTV, Inc.*, No. 02-04445 FMC (Ex) (“the
4 *RePlayTV* action”), which are only briefly described below.

5 **A. The *RePlayTV* Action**

6 Plaintiffs in the *RePlayTV* action are a number of television and film
7 companies in the entertainment industry.¹ Defendants in the *RePlayTV* action
8 are SONICblue, Inc. (“SONICblue”), and its wholly owned subsidiary,
9 RePlayTV, Inc (“RePlayTV”).²

10 The factual allegations in the *RePlayTV* action center on the development
11 and sale by RePlayTV of a digital video recorder: the RePlayTV 4000 series.
12 The digital video recorder, or DVR, enables television viewers to make digital
13 copies of copyrighted television programs. The DVRs are equipped with
14 commercial-skipping features, and they may be used to send copies of televised
15 programs (or “content”) to other RePlayTV owners via high-speed internet
16 connections.

17
18 ¹ Specifically, the Plaintiffs in the *RePlayTV* action are Paramount Pictures Corp.
19 (“Paramount”); Disney Enterprises, Inc. (“Disney”); National Broadcasting Company
20 (“NBC”); NBC Studios, Inc. (“NBC Studios”); Showtime Networks, Inc. (“Showtime”); The
21 United Paramount Network (“UPN”); ABC, Inc. (“ABC”); Viacom International, Inc.
22 (“Viacom”); CBS Worldwide, Inc. (“CBS Worldwide”); CBS Broadcasting, Inc. (“CBS”); Time
23 Warner Entertainment Company, L.P. (“TWE”); Home Box Office (“HBO”); Warner Brothers
24 (“Warner Brothers”); Warner Brothers Television (“WBT”); Time Warner, Inc. (“TWI”);
25 Turner Broadcasting System, Inc. (“Turner Broadcasting”); New Line Cinema Corp. (“New
26 Line”); Castle Rock Entertainment (“Castle Rock”); The WB Television Network Partners,
27 L.P (“WBT Network”); Metro-Goldwyn-Mayer Studios, Inc. (“MGM”); Orion Pictures Corp.
28 (“Orion”); Twentieth Century Fox Film Corp. (“Fox”); Universal City Studios Productions,
Inc. (“Universal”); Fox Broadcasting Co. (“FBC”); Columbia Pictures Industries, Inc.
 (“Columbia Industries”); Columbia Pictures Television (“Columbia Television”); Columbia
Tristar Television (“CTTV”); and TriStar Television, Inc. (“TriStar Television”).

² Throughout this Order, the Court will refer to SONICblue, Inc., and RePlayTV, Inc.,
collectively as “RePlayTV.”

1 The Plaintiffs in the *RePlayTV* action have asserted claims against
2 SONICblue and RePlayTV based on, *inter alia*, contributory and vicarious
3 copyright infringement. These claims are based on the alleged direct copyright
4 infringement committed by the owners of the RePlayTV DVRs. (*See, e.g.,*
5 *Paramount Compl.*, No. 01-09358, ¶ 64 (regarding contributory infringement);
6 ¶ 71 (regarding vicarious infringement)).
7

8 **B. The *Newmark* Action**

9 Five owners of RePlayTV DVRs have filed the present declaratory relief
10 action in this Court.

11 All the twenty-eight plaintiffs in the *RePlayTV* action are defendants in
12 the present action, which the Court refers to as the *Newmark* action.
13 Throughout this Order, the Court refers to these defendants as “the
14 Entertainment Defendants.” SONICblue and RePlayTV are defendants in the
15 present action as well.

16 The factual allegations in the Complaint reveal that the *Newmark*
17 Plaintiffs use the units to record content for later viewing;³ some of the
18 Plaintiffs transfer content to laptop computers for viewing while traveling.
19 Plaintiffs use the commercial-skipping features of the RePlayTV DVRs; at least
20 one Plaintiff uses the commercial-skipping features to control the advertising
21 to which his children are exposed.

22 The *Newmark* Plaintiffs seek a declaration as to whether their activities
23 constitute copyright infringement.
24
25
26
27

28 ³ This use is referred to as “time-shifting.”

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

II. Motion to Dismiss

The Entertainment Defendants move to dismiss the *Newmark* Plaintiffs' claims, arguing that the claims do not present an actual "case or controversy" as required by the Declaratory Judgment Act, 28 U.S.C. § 2201, and Article III of the United States Constitution. If the *Newmark* Plaintiffs' claims do not present an actual "case or controversy", the Court lacks subject matter jurisdiction over the matter, and the claims must be dismissed. *See Mason v. Genisco Technology Corp.*, 960 F.2d 849, 853 (9th Cir. 1991).

A motion to dismiss an action for lack of subject matter jurisdiction is properly brought under Fed. R. Civ. P. 12(b)(1). The objection presented by this motion is that the court has no authority to hear and decide the case. When considering a Rule 12(b)(1) motion challenging the substance of jurisdictional allegations, the Court is not restricted to the face of the pleadings, but may review any evidence, such as declarations and testimony, to resolve any factual disputes concerning the existence of jurisdiction. *See McCarthy v. United States*, 850 F.2d 558, 560 (9th Cir. 1988), *cert. denied*, 489 U.S. 1052, 109 S. Ct. 1312 (1989). The burden of proof on a Rule 12(b)(1) motion is on the party asserting jurisdiction. *See Sopcak v. Northern Mountain Helicopter Serv.*, 52 F.3d 817, 818 (9th Cir. 1995).

The present motion presents a novel issue: Does a plaintiff present an actual "case or controversy" under the Declaratory Judgment Act and Article III where the plaintiff's conduct is alleged, in a separate action against a third party for contributory and/or vicarious copyright infringement, to be direct copyright infringement? The parties have cited no authority that discusses the actual "case or controversy" requirement in the context of this unique factual scenario, and the Court, in its own research, has found none.

Nevertheless, both the Entertainment Defendants and the *Newmark* Plaintiffs cite a number of cases that are instructive on this issue, from which

1 the Court concludes that the *Newmark* Plaintiffs have presented an actual “case
2 or controversy.”

3 The Declaratory Judgment Act permits a federal court to “declare the
4 rights and other legal relations” of parties to “a case of actual controversy.” 28
5 U.S.C. § 2201. This “actual controversy” requirement is the same as the “case
6 or controversy” requirement of Article III of the United States Constitution.
7 *See Aetna Life Ins. Co. v. Haworth*, 300 U.S. 227, 239-40, 57 S. Ct. 461, 463 (1937).
8 Therefore, the question of justiciability, and therefore of subject matter
9 jurisdiction, is the same under § 2201 as it is under Article III.

10 The United States Supreme Court has given guidance as to when “an
11 abstract” question becomes a “controversy” under the Declaratory Judgment
12 Act:

13 The difference between an abstract question and a “controversy”
14 contemplated by the Declaratory Judgment Act is necessarily one
15 of degree, and it would be difficult, if it would be possible, to
16 fashion a precise test for determining in every case whether there
17 is such a controversy. Basically, the question in each case is
18 whether the facts alleged, under all the circumstances, show that
19 there is a substantial controversy, between parties having adverse
20 legal interests, of sufficient immediacy and reality to warrant the
21 issuance of a declaratory judgment.

22 *Maryland Casualty Co. v. Pacific Coal & Oil Co.*, 312 U.S. 270, 273, 61 S. Ct. 510,
23 512 (1941).

24 Applying this standard, the Ninth Circuit has held that something less
25 than an “actual threat” of litigation is required to meet the “case or controversy”
26 requirement; instead, courts must focus on whether a declaratory plaintiff has
27 a “reasonable apprehension” that he or she will be subjected to liability. *Societe
28 de Conditionnement en Aluminium v. Hunter Engineering Co., Inc.*, 655 F.2d 938,

1 944 (9th Cir. 1981). In *Societe*, the court first noted that the parties' assumption
2 that a declaratory plaintiff must be subject to an "actual threat" was incorrect:

3 We infer from the arguments of the parties that they agree that an
4 actual threat of litigation must be made by the [declaratory
5 defendant] for a case or controversy to exist. We assume that the
6 district court applied this standard in reaching its decision. We
7 conclude that the Constitution has a much lower threshold than
8 this standard would suggest.

9 *Id.* The Ninth Circuit then went on to hold that the determination of whether
10 a case or controversy exists must focus on the reasonable apprehension of the
11 declaratory plaintiff:

12 A better way to conceptualize the case or controversy
13 standard is to focus on the declaratory judgment plaintiff. An
14 action for a declaratory judgment that a patent is invalid, or that
15 the plaintiff is not infringing, is a case or controversy if the plaintiff
16 has a real and reasonable apprehension that he will be subject to
17 liability if he continues to manufacture his product.

18 *Id.*

19 Other cases make it clear that no explicit threat of litigation is required
20 to meet the "case or controversy" requirement. *See also K-Lath v. Davis Wire*
21 *Corp.*, 15 F. Supp. 2d 952 (C.D. Cal. 1998) (noting that a plaintiff seeking
22 declaratory judgment must show "an explicit threat or *other action*" that creates
23 a reasonable apprehension that the plaintiff will face an infringement suit)
24 (emphasis added); *Intellectual Property Development v. TCI Cablevision of*
25 *California, Inc.*, 248 F.3d 1333, 1340 (Fed. Cir. 2001) ("other action" is
26 sufficient), *cert. denied*, ___ U.S. ___, 122 S. Ct. 216 (2001); *Guthy-Renker Fitness v.*
27 *Icon Health & Fitness, Inc.*, 179 F.R.D. 264 (C.D. Cal. 1998) (same).

28 The Entertainment Defendants argue that the *Newmark* Plaintiffs cannot

1 have a reasonable apprehension that they will face liability based on their use
2 of their RePlayTV DVRs. The Entertainment Defendants contend that did not
3 even know about the *Newmark* Plaintiffs until they filed this action, and that
4 they did not name any individual Doe defendants in the *RePlayTV* action and
5 point out that they make these allegations only because these allegations are
6 necessary to state a claim against RePlayTV for contributory and vicarious
7 copyright infringement.

8 However, the *Newmark* Plaintiffs argue persuasively that a victory by the
9 Entertainment Defendants in the *RePlayTV* action will necessarily require a
10 determination that the activities of the owners constitute direct copyright
11 infringement, thereby instilling in them a reasonable apprehension that they
12 will be subject to liability.

13 When viewed from the perspective of the *Newmark* Plaintiffs, the
14 Entertainment Defendants' allegations in the *RePlayTV* action are sufficient to
15 raise a reasonable apprehension that they will be subject to liability. The
16 Complaints in the *RePlayTV* action allege that the actions of the *Newmark*
17 Plaintiffs (and other RePlayTV DVR owners) constitute direct copyright
18 infringement. Of course, the Entertainment Defendants must allege these facts
19 to support their claims of contributory and vicarious copyright infringement
20 against RePlayTV. But the fact remains that the Entertainment Defendants
21 have, with a great deal of specificity, accused the *Newmark* Plaintiffs (and other
22 RePlayTV DVR owners) of infringing the Entertainment Defendants'
23 copyrights, and have demonstrated the will to protect copyrights through
24 litigation. These facts raise a reasonable apprehension on the part of the
25 *Newmark* Plaintiffs. This is especially so because that it appears from the
26 Complaint in the *Newmark* action that the *Newmark* Plaintiffs are continuing
27 to use their RePlayTV DVRs in a manner that the Entertainment Defendants
28 allege constitutes infringing activity.

1 federal courts competence to make a declaration of rights; it did not impose a
2 duty to do so." *Public Affairs Associates, Inc. v. Rickover*, 369 U.S. 111, 112, 82 S.
3 Ct. 580 (1962). "A declaratory judgment, like other forms of equitable relief,
4 should be granted only as a matter of judicial discretion, exercised in the public
5 interest." *Id.*

6 The Supreme Court not surprisingly has noted, however, that the refusal
7 to exercise its discretion must be principled and reasonable, and should be
8 articulated: "Of course a District Court cannot decline to entertain such an
9 action as a matter of whim or personal disinclination." *Id.*

10 This Court considers a number of factors in determining whether a stay
11 should be granted. The factors enunciated in *Brillhart v. Excess Insurance*
12 *Company of America*, 316 U.S. 491, 62 S. Ct. 1173 (1942), are meaningful when
13 the underlying action is a state action, rather than where, as here, the
14 underlying action is proceeding in the same forum. *Brillhart* requires federal
15 courts to 1) avoid needless determinations of state law issues, 2) discourage
16 forum shopping, and 2) avoid duplicative litigation. These factors are not
17 particularly helpful to the Court's analysis in this case. *Id.*

18 The Ninth Circuit has noted, however, that the *Brillhart* factors are not
19 exhaustive. *See Government Employees Insurance Co. v. Dizol*, 133 F.3d 1220,
20 1225 n.5 (9th Cir. 1998). Other factors to be considered by the Court are
21 1) whether the declaratory action will settle all aspects of the controversy;
22 2) whether the declaratory action will serve a useful purpose in clarifying the
23 legal relations at issue; 3) whether the declaratory action is being sought merely
24 for the purposes of procedural fencing or to obtain a "res judicata" advantage;
25 and 4) whether the use of a declaratory action will result in entanglements
26 between the federal and state court systems. *Id.*

27 The fourth factor, like the *Brillhart* factors, is inapplicable here.

28 The first and second factor appear to the Court to be interrelated, and to

1 weigh in favor of denying a stay. The argument in favor of a stay is that all the
2 issues presented in the *Newmark* action will necessarily be resolved by the
3 *RePlayTV* action. However, the Court is persuaded that the *Newmark* Plaintiffs
4 may be correct that the *RePlayTV* action will not necessarily resolve what
5 specific uses, if any,⁴ of the RePlayTV DVR constitute fair use.⁵ Denying the
6 stay furthers the purpose of the first and second factors — to resolve the
7 uncertainties in the relations between the parties. The rationale behind these
8 factors are better served by permitting the *RePlayTV* action and the *Newmark*
9 action to proceed simultaneously.

10 Despite the Entertainment Defendants' argument, the Court is
11 unconvinced that the *Newmark* action constitutes "procedural fencing." The
12 Entertainment Defendants contend that the *Newmark* Plaintiffs' true intent is
13 to circumvent the intervention requirements of Fed. R. Civ. P. 24 and to, in
14 effect, intervene in the *RePlayTV* action. The Court is persuaded, however, that
15 the *Newmark* Plaintiffs could well meet the intervention requirements of Fed.
16 R. Civ. P. 24(a).⁶ The *Newmark* Plaintiffs claim an interest in the transaction
17 at issue, and are so situated that the resolution of the *RePlayTV* action may as
18

19 ⁴ The *RePlayTV* action is in its early stages. At this time, the Court expresses no
20 opinion as to the merits of the claims advanced in the *RePlayTV* action.

21 ⁵ The Court recognizes that resolution of the *RePlayTV* action may significantly narrow
22 the issues presented in the *Newmark* action.

23 ⁶ Rule 24(a) of the Federal Rules of Civil Procedure provides:

24 Upon timely application anyone shall be permitted to intervene in an action: . . .
25 (2) when the applicant claims an interest relating to the property or transaction
26 which is the subject of the action and the applicant is so situated that the
27 disposition of the action may as a practical matter impair or impede the
applicant's ability to protect that interest, unless the applicant's interest is
adequately represented by existing parties.

28 *Id.*

1 a practical matter impair or impede their ability to protect that interest.⁷ The
2 Court is persuaded that although RePlayTV's interests and the interests of the
3 *Newmark* Plaintiffs overlap significantly, those interests are not perfectly
4 aligned. The *Newmark* Plaintiffs' interests are focused on whether specific
5 uses constitute "fair use" under copyright law; RePlayTV's interests (and legal
6 defenses) are likely to venture beyond the fair use doctrine. Therefore, the
7 Court rejects the Entertainment Defendants' argument that the *Newmark*
8 Plaintiffs' true intent is to circumvent the intervention requirements of Fed. R.
9 Civ. P. 24, and that their actions constitute mere "procedural fencing".

10 The Court concludes that the factors set forth in *Dizol* favor a denial of
11 a stay.

12 The Court has also considered whether a stay will serve the public
13 interest. *See Rickover*, 369 U.S. at 112. The Court recognizes that any
14 unnecessary delay in adjudicating the rights of the *Newmark* Plaintiffs may chill
15 their use of their RePlayTV DVRs. Similarly, any unnecessary delay may also
16 lead to increased liability for statutory damages under federal copyright law.
17 *See* 17 U.S.C. § 504(c)(1) (authorizing statutory damages for each non-willful
18 violation of no less than \$750 and no more than \$30,000). Additionally, the
19 Court is persuaded that denying the stay may result in a more fully developed
20 factual record regarding the consumers' uses of the RePlayTV DVR and, as a
21 result, the Court may be better able to fashion an appropriate equitable relief.
22 The Court agrees that the public interest would not be served by the granting
23 of a stay.

24 Accordingly, the Court hereby denies the Motion to Stay.

25
26
27 ⁷ For instance, the *Newmark* Plaintiffs' ability to protect their interest in using their
28 RePlayTV DVRs would be impaired if the Court were to order that RePlayTV disable the
send-show and commercial skipping features of the DVRs.

1 **IV. Motion to Consolidate**

2 The Federal Rules of Civil Procedure authorize consolidation of cases in
3 appropriate circumstances:

4 When actions involving a common question of law or fact are
5 pending before the court, it may order a joint hearing or trial of any
6 or all the matters in issue in the actions; it may order all the actions
7 consolidated; and it may make such orders concerning proceedings
8 therein as may tend to avoid unnecessary costs or delay.

9 Fed. R. Civ. P. 42(a).

10 Under this standard, it is clear to the Court that the *Newmark* action
11 should be consolidated with the *RePlayTV* action. The actions involve
12 common questions of law and fact. Both actions involve a determination of
13 whether the use of certain features of the RePlayTV DVR constitutes copyright
14 infringement. Both cases are at the early stage of litigation, which facilitates
15 consolidation, at least for discovery and pretrial purposes.⁸

16 The Entertainment Defendants argue that the actions should not be
17 consolidated. They correctly contend that the issues presented in the *Newmark*
18 action — whether the specific uses of the *Newmark* Plaintiffs constitute fair use
19 — is narrower than the issues presented in the *RePlayTV* action. From this
20 fact, the Entertainment Defendants conclude that the *Newmark* action will be
21 more quickly and efficiently resolved if it is not consolidated with the
22 *RePlayTV* action. Nevertheless, there is no question that the issue of whether
23 the *Newmark* Plaintiffs' use of the RePlayTV DVRs' send-show and
24 commercial-skipping features constitutes fair use will most likely figure
25 prominently in both the *RePlayTV* action and the *Newmark* action. The Court
26

27
28

* The Court reserves for another day the issue of whether these actions should be consolidated for trial.

1 is unconvinced that the Entertainment Defendants' are correct in
2 characterizing the *Newmark* action as a case that will require little discovery and
3 that will be resolved quickly if not consolidated. The issue of fair use has
4 yielded a great deal of discovery in the *RePlayTV* action, and promises to do the
5 same in this action.⁹

6 The Entertainment Defendants also claim that the *Newmark* Plaintiffs,
7 in seeking consolidation, are merely attempting to gain unfettered access to
8 discovery documents, and to widen the scope of discovery in *RePlayTV* action.
9 That a party may seek discovery of irrelevant documents is a danger in any
10 litigation; this concern is not unique to consolidated cases. There are
11 procedural protections in place that assist parties in guarding against a party
12 obtaining that irrelevant discovery. The Entertainment Defendants are well
13 versed in seeking such protection. The Court does not at this time resolve
14 issues regarding the scope of discovery; rather, the Court merely notes that the
15 Entertainment Defendants' concerns regarding access to discovery do not
16 persuade the Court that consolidation is inappropriate.

17 In reaching this conclusion, the Court is guided by the agreement of the
18 *Newmark* Plaintiffs' counsel to abide by the terms of the multi-tiered protective
19 order to which the parties stipulated in the *RePlayTV* action.

20
21 ⁹ Part of the Entertainment Defendants' Opposition to the Motion for Consolidation
22 addresses the scope of discovery to which the *Newmark* Plaintiffs would be entitled. They
23 contend that consolidation will unnecessarily complicate the *RePlayTV* action because the
24 *Newmark* Plaintiffs will not be entitled to as broad a range of discovery as *RePlayTV* was found
25 to be entitled to. The Entertainment Defendants similarly argue that the depositions of the
26 Entertainment Defendant representatives would be unnecessarily complicated as *RePlayTV*
27 would attempt to question these representatives using documents obtained in discovery in the
28 *RePlayTV* action. This would cause the Entertainment Defendants to halt the depositions
every few moments to discuss whether the *Newmark* Plaintiffs should be entitled to access to
discovery provided in the *RePlayTV* action.

The Court leaves the determination of the precise scope of discovery to the Magistrate
Judge. At this stage of the proceeding, the Court is satisfied that the issue of fair use is present
in both actions, and therefore finds the Entertainment Defendant's arguments unpersuasive.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

V. Conclusion

For the reasons set forth above, the Court hereby denies the Motion to Dismiss (docket #43-1), hereby denies the Motion to Stay (docket #43-2), and hereby grants the Motion to Consolidate (docket #45). For ease of recordkeeping, the Court orders that all further documents be filed under Case No. CV 01-09358, and that Case No. CV 02-04445 be closed.

Dated: August 15, 2002



FLORENCE-MARIE COOPER, JUDGE
UNITED STATES DISTRICT COURT

EXHIBIT B

O'MELVENY & MYERS LLP

LOS ANGELES
IRVINE
MENLO PARK
NEWPORT BEACH
NEW YORK
SAN FRANCISCO

1999 Avenue of the Stars
Los Angeles, California 90067-6035

TELEPHONE (310) 553-6700
FACSIMILE (310) 246-6779
INTERNET: www.omm.com

TYSONS CORNER
WASHINGTON, D.C.
HONG KONG
LONDON
SHANGHAI
TOKYO

September 3, 2002

OUR FILE NUMBER
019,019-20

VIA FACSIMILE (415) 924-2905

WRITER'S DIRECT DIAL
310-246-6747

Ira P. Rothken, Esq.
ROTHKEN LAW FIRM
1050 Northgate Drive, Suite 520
San Rafael, California 94903

WRITER'S E-MAIL ADDRESS
arader@omm.com

Re: **Paramount Pictures Corp., et al. v. ReplayTV, Inc., et al.**

Dear Ira:

As we discussed a few minutes ago, here is a draft stipulation to effectuate the arrangements we have discussed. As I told you when we spoke, all of the plaintiffs have not yet signed off.

Sincerely,



Alan Rader
of O'MELVENY & MYERS LLP

AR:bss

cc: Plaintiffs' Counsel
Emmett Stanton, Esq.

Enclosure

1 SCOTT P. COOPER (Cal. Bar No. 96905)
PROSKAUER ROSE LLP
2 2049 Century Park East, 32nd Floor
Los Angeles, California 90067
3 Telephone: (310) 557-2900 / Facsimile: (310) 557-2193
Attorneys for the MGM, Fox, Universal,
4 *Disney, Viacom & NBC Plaintiffs*

5 ROBERT M. SCHWARTZ (Cal. Bar No. 117166)
O'MELVENY & MYERS LLP
6 1999 Avenue of the Stars, Seventh Floor
Los Angeles, California 90067-6035
7 Telephone: (310) 553-6700 / Facsimile: (310) 246-6779
8 *Attorneys for the Time Warner Plaintiffs*

9 ROBERT H. ROTSTEIN (Cal. Bar No. 72452)
McDERMOTT, WILL & EMERY
10 2049 Century Park East, 34th Floor
Los Angeles, California 90067
11 Telephone: (310) 284-6101 / Facsimile: (310) 277-4730
Attorneys for the Columbia Plaintiffs

12 IRA P. ROTHKEN (Cal. Bar No. 160029)
ROTHKEN LAW FIRM
13 1050 Northgate Drive, Suite 520
San Rafael, California 94903
14 Telephone: (415) 924-4250 / Facsimile: (415) 924-2905
15 *Attorneys for the Newmark Plaintiffs*

16 LAURENCE F. PULGRAM (Cal. Bar No. 115163)
FENWICK & WEST LLP
17 275 Battery Street, Suite 1500
San Francisco, California 94111
18 Telephone: (415) 875-2300 / Facsimile: (415) 281-1417
19 *Attorneys for Defendants ReplayTV, Inc. and SONICblue Incorporated*

20 [Full counsel appearances on signature page]

21 **UNITED STATES DISTRICT COURT**
22 **CENTRAL DISTRICT OF CALIFORNIA**

1 PARAMOUNT PICTURES
CORPORATION, *et al.*,

2 Plaintiffs,

3 v.

4 REPLAYTV, INC., *et al.*,

5 Defendants.
6
7

) Case No.: CV 01-09358 FMC (Ex)

Hon. Florence-Marie Cooper

STIPULATION AND [PROPOSED]
ORDER REGARDING THE
NEWMARK PLAINTIFFS' ACCESS
TO CONFIDENTIAL
INFORMATION

8
9 AND CONSOLIDATED ACTIONS.
10

11
12 WHEREAS, on August 15, 2002, the Court granted the Newmark Plaintiffs'
13 motion to consolidate the action entitled Newmark, et al. v. Turner Broadcasting
14 System, Inc., et al. (former Case No CV 02-04445 FMC (Ex) (the "Newmark
15 Action") with the above-captioned consolidated actions (the "Action"), the parties
16 to the Action, through their respective counsel of record, HEREBY STIPULATE
17 AND AGREE as follows:

18 1. The plaintiffs in the Newmark Action (the "Newmark Plaintiffs"),
19 through their counsel of record, shall execute the Stipulation and Protective Order
20 entered by this Court on May 29, 2002 (the "Protective Order");

21 2. Upon their execution of the Protective Order and subject to its terms,
22 the Newmark Plaintiffs shall, to the same extent as all other parties in the Action,
23 be allowed to obtain and to review all discovery in the Action to date, including
24 but not limited to all documents, interrogatory responses and responses to requests
25 for admissions produced or served in the Action, subject to the following
26 limitations and restrictions:
27
28

1 (a) Neither the Newmark Plaintiffs nor their attorneys shall be
2 given access to, or be allowed to obtain or review, documents or interrogatory
3 responses that were produced or served by Plaintiffs in the Action in response to
4 any of the following discovery requests: SONICblue Document Request Nos. 12,
5 14, 15, 16, and 17 (the "Movies.com/Movielink Discovery"); and ReplayTV
6 Document Request No. 53 through 56, and ReplayTV Interrogatory Nos. 11(f) and
7 14 (the "Lobbying Discovery").¹ Plaintiffs in the Action shall promptly identify by
8 Bates number all documents produced in response to the Movies.com/Movielink
9 Discovery and the Lobbying Discovery.
10
11
12

13 (b) The Electronic Frontier Foundation, and its attorneys,
14 employees and agents (including but not limited to Cindy A. Cohn, Esq., Fred von
15 Lohmann, Esq., and Robin D. Gross, Esq.) (collectively, the "EFF") shall not be
16 given access to, nor be allowed to obtain or review, any discovery produced by any
17 of the parties in the Action designated as "Restricted" Information or "Highly
18 Restricted" Information (as those terms are defined in the Protective Order).
19
20
21

22 3. Nothing in this Stipulation and Order shall prevent the Newmark
23 Plaintiffs from applying to the Court for an order allowing (i) the Newmark
24 Plaintiffs to obtain access to, or to obtain or review, the Movies.com/Movielink
25

26 ¹ Defendants ReplayTV, Inc. and SONICblue Inc. used different numbering for the written discovery they served
27 on the various groups of Plaintiffs in the Action. The ReplayTV Document Requests and Interrogatories referenced
28 above refer to the requests and interrogatories identified in Magistrate Judge Eick's April 26, 2002 orders.

1 Discovery and/or the Lobbying Discovery and/or (ii) the EFF to obtain access to
2 discovery produced by any of the parties in the Action designated as "Restricted"
3
4 Information or "Highly Restricted" Information (as those terms are defined in the
5 Protective Order); nor shall anything in this Stipulation and Order prevent any
6
7 other party to this Action from opposing such an application. All such rights are
8 expressly reserved.
9

10 DATED: September __, 2002

11
12 PROSKAUER ROSE LLP

O'MELVENY & MYERS LLP

13
14 By: _____
15 Scott P. Cooper

By: _____
Robert M. Schwartz

16 Attorneys for Plaintiffs Metro-
17 Goldwyn-Mayer Studios Inc., Orion
18 Pictures Corporation, Twentieth
19 Century Fox Film Corporation,
20 Universal City Studios Productions, Inc.
21 (formerly, Universal City Studios
22 Productions LLLP), Fox Broadcasting
23 Company, Plaintiffs Paramount Pictures
24 Corporation, Disney Enterprises, Inc.,
25 National Broadcasting Company, Inc.,
26 NBC Studios, Inc., Showtime Networks
27 Inc., UPN (formerly, The United
28 Paramount Network), ABC, Inc.,
Viacom International Inc., CBS
Worldwide Inc., and CBS Broadcasting
Inc.

Attorneys for Plaintiffs Time Warner
Entertainment Company, L.P., Home
Box Office, Warner Bros., Warner Bros.
Television, Time Warner Inc., Turner
Broadcasting System, Inc., New Line
Cinema Corporation, Castle Rock
Entertainment, and The WB Television
Network Partners, L.P.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

MCDERMOTT, WILL & EMERY

FENWICK & WEST LLP

By: _____
Robert H. Rotstein

By: _____
Laurence F. Pulgram

Attorneys for Plaintiffs Columbia Pictures Industries, Inc., Columbia Pictures Television, Inc., Columbia TriStar Television, Inc., and TriStar Television, Inc.

Attorneys for Defendants ReplayTV, Inc. and SONICblue Incorporated

ROTHKEN LAW FIRM

By: _____
Ira P. Rothken

Attorneys for Plaintiffs Craig Newmark, Shawn Hughes, Keith Ogden, Glenn Fleishman and Phil Wright

Good cause appearing therefore, the preceding stipulation of the parties in the above-captioned action, as evidenced by the signatures of counsel of record appearing above, is hereby ordered.

DATED: September __, 2002

HONORABLE CHARLES F. EICK
United States Magistrate Judge

EXHIBIT C

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

SCOTT P. COOPER (Cal. Bar No. 96905)
PROSKAUER ROSE LLP
2049 Century Park East, Suite 3200
Los Angeles, CA 90067
Telephone: (310) 557-2900
Facsimile: (310) 557-2193
*Attorneys for the MGM, Fox, Universal, Viacom,
Disney & NBC Plaintiffs*

Priority _____
Send X
Enter _____
Closed _____
JS-5/JS-6 _____
JS-2/JS-3 _____
Scan Only _____

ROBERT M. SCHWARTZ (Cal. Bar No. 117166)
O'MELVENY & MYERS LLP
1999 Avenue of the Stars, Seventh Floor
Los Angeles, California 90067-6035
Telephone: (310) 553-6700
Facsimile: (310) 246-6779
Attorneys for the Time Warner Plaintiffs

ROBERT H. ROTSTEIN (Cal. Bar No. 72452)
McDERMOTT, WILL & EMERY
2049 Century Park East, 34th Floor
Los Angeles, CA 90067
Telephone: (310) 277-4110
Facsimile: (310) 277-4730
Attorneys for the Columbia Plaintiffs

FILED FILED
CLERK, U.S. DISTRICT COURT
C9-20-02
JUL 20 2002
CENTRAL DISTRICT OF CALIFORNIA

*locked
#1111*

[Full counsel appearances on signature page]

SEP 11 10 55

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

PARAMOUNT PICTURES
CORPORATION *et al.*,

Plaintiffs,

v.

REPLAYTV, INC. *et al.*,

Defendants.

CASE NO. CV 01-9358 FMC (Ex) ✓

Hon. Florence-Marie Cooper

**STIPULATION AND [PROPOSED]
ORDER REGARDING THE
NEWMARK PLAINTIFFS' ACCESS
TO CONFIDENTIAL
INFORMATION**

AND CONSOLIDATED ACTIONS.

EN 9:00 AM CMS
CV [Signature]

1 On August 15, 2002, the Court granted a motion to consolidate the action
2 entitled Newmark, et al. v. Turner Broadcasting System, Inc., et al. (former Case No
3 CV 02-04445 FMC (Ex)) with the previously pending Paramount Pictures
4 Corporation, et al. v. ReplayTV, Inc., et al. action. The Plaintiffs in the Newmark
5 action (the "Newmark Plaintiffs") and the Plaintiffs in the original action (the
6 "Copyright Owner Plaintiffs") disagree concerning the extent to which the Electronic
7 Frontier Foundation and its attorneys, employees and agents (including but not
8 limited to Cindy A. Cohn, Esq., Fred von Lohmann, Esq., and Robin D. Gross, Esq.
9 (collectively, the "EFF") are entitled to access to information and documents already
10 produced during discovery in this action. To obtain a judicial resolution of this
11 disagreement while allowing this litigation to progress, the parties to this action
12 through their respective counsel of record, HEREBY STIPULATE AND AGREE as
13 follows:

14 1. Pursuant to Local Rule 37-2, the Copyright Owner Plaintiffs will file a
15 motion for protective order seeking certain restrictions on the types of discovery
16 available to EFF. The Copyright Owner Plaintiffs shall provide the opening portion
17 of the Joint Stipulation called for by Local Rule 37-2.1 to the Newmark Plaintiffs on
18 September 23, 2002. The Newmark Plaintiffs shall provide their portion of the Joint
19 Stipulation on September 30, 2002, and the motion shall be filed promptly thereafter.
20 Supplemental Memoranda, pursuant to Local Rule 37-2.3, shall be filed on October 7,
21 2002. The motion shall be noticed for hearing on October 15, 2002.

22 2. The Newmark Plaintiffs, through their counsel of record, shall execute the
23 Stipulation and Protective Order entered in this action by this Court on May 29, 2002
24 (the "Protective Order"). Upon their execution of the Protective Order, and subject to
25 its terms and the terms of this Stipulation, counsel for the Newmark Plaintiffs, Ira
26 Rothken and EFF, shall be allowed to obtain and to review all discovery in the action
27 to date, including but not limited to all documents, deposition transcripts,
28 interrogatory responses and responses to requests for admissions produced or served

1 in the action, *except that* -- unless and until altered or adjusted by the Court's ruling
2 on the motion for protective order referred to above -- the following additional
3 limitations and procedures shall apply:

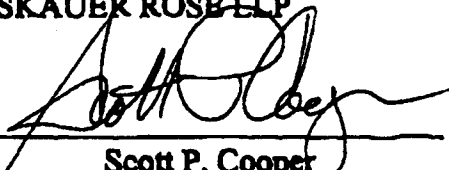
4 (a) The EFF shall not have or be given access to, nor be allowed to
5 obtain or review: (i) documents produced in this action that were originally produced
6 or prepared by the Copyright Owner Plaintiffs in connection with the Department of
7 Justice investigation regarding Movies.com and/or Movielink; and (ii) documents,
8 interrogatory responses or responses to requests for admission that were produced or
9 served by Copyright Owner Plaintiffs in response to any written discovery
10 concerning lobbying activity by the Copyright Owner Plaintiffs. The Copyright
11 Owner Plaintiffs shall promptly identify, by Bates number or otherwise, all such
12 produced documents, interrogatory responses and responses to requests for
13 admission, and the EFF will not be allowed to have, and will not accept, access to any
14 such information.

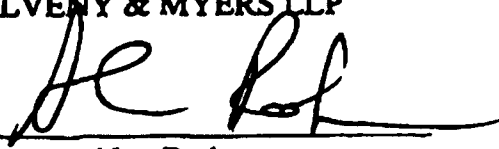
15 (b) The EFF also shall not have or be given access to, nor be allowed
16 to obtain or review, any other discovery produced by the Copyright Owner Plaintiffs
17 designated as "Restricted" Information or "Highly Restricted" Information (as those
18 terms are defined in the Protective Order) to the extent that that Information will be
19 the subject of the Copyright Owner Plaintiffs' motion for protective order referred to
20 above. The Copyright Owner Plaintiffs will, on a rolling basis, identify, by Bates
21 number or otherwise, any discovery responses and produced documents designated
22 under the Protective Order as "Restricted" or "Highly Restricted" Information that
23 are not subject to their motion for protective order. Thereafter, the EFF may have
24 immediate access to those materials that are not subject to such motion.

25 (c) The Copyright Owner Plaintiffs shall promptly identify, by Bates
26 number or otherwise, the other discovery responses and produced documents that are
27
28

1 designated under the Protective Order as "Confidential" or "Highly Confidential"
2 Information or were produced without any designation under the Protective Order
3 and EFF shall be entitled to have access to such responses and documents, subject to
4 the provisions of the Protective Order (as applicable).

5
6 DATED: September 17, 2002

7 PROSKAUER ROSE LLP
8
9 By: 
10 Scott P. Cooper
11 Attorneys for Plaintiffs Metro-
12 Goldwyn-Mayer Studios Inc., Orion
13 Pictures Corporation, Twentieth
14 Century Fox Film Corporation,
15 Universal City Studios Productions
16 LLLP (formerly, Universal City Studios
17 Productions, Inc.), Fox Broadcasting
18 Company, Plaintiffs Paramount Pictures
19 Corporation, Disney Enterprises, Inc.,
20 National Broadcasting Company, Inc.,
21 NBC Studios, Inc., Showtime Networks
22 Inc., UPN (formerly, The United
23 Paramount Network), ABC, Inc.,
24 Viacom International Inc., CBS
25 Worldwide Inc., and CBS Broadcasting
26 Inc.

O'MELVENY & MYERS LLP
By: 
Alan Rader
Attorneys for Plaintiffs Time Warner
Entertainment Company, L.P., Home
Box Office, Warner Bros., Warner Bros.
Television, Time Warner Inc., Turner
Broadcasting System, Inc., New Line
Cinema Corporation, Castle Rock -
Entertainment, and The WB Television
Network Partners L.P.

22 MCDERMOTT, WILL & EMERY
23 By: _____
24 Robert H. Rotstein
25 Attorneys for Plaintiffs Columbia
26 Pictures Industries, Inc., Columbia
27 Pictures Television, Inc., Columbia
28 TriStar Television, Inc., and TriStar
Television, Inc.

FENWICK & WEST LLP
By: _____
Laurence F. Pulgram
Attorneys for Defendants ReplayTV,
Inc. and SONICblue Incorporated

CCI-585468.1

1 designated under the Protective Order as "Confidential" or "Highly Confidential"
2 Information or were produced without any designation under the Protective Order
3 and EFF shall be entitled to have access to such responses and documents, subject to
4 the provisions of the Protective Order (as applicable).

5
6 DATED: September 17 2002

7 PROSKAUER ROSE LLP

O'MELVENY & MYERS LLP

8
9 By: _____

By: _____

10 Scott P. Cooper
11 Attorneys for Plaintiffs Metro-
12 Goldwyn-Mayer Studios Inc., Orion
13 Pictures Corporation, Twentieth
14 Century Fox Film Corporation,
15 Universal City Studios Productions
16 LLLP (formerly, Universal City Studios
17 Productions, Inc.), Fox Broadcasting
18 Company, Plaintiffs Paramount Pictures
19 Corporation, Disney Enterprises, Inc.,
20 National Broadcasting Company, Inc.,
21 NBC Studios, Inc., Showtime Networks
22 Inc., UPN (formerly, The United
23 Paramount Network), ABC, Inc.,
24 Viacom International Inc., CBS
25 Worldwide Inc., and CBS Broadcasting
26 Inc.

Alan Rader
Attorneys for Plaintiffs Time Warner
Entertainment Company, L.P., Home
Box Office, Warner Bros., Warner Bros.
Television, Time Warner Inc., Turner
Broadcasting System, Inc., New Line
Cinema Corporation, Castle Rock
Entertainment, and The WB Television
Network Partners L.P.

22 MCDERMOTT, WILL & EMERY

FENWICK & WEST LLP

23 By: Robert H. Rotstein
24 Robert H. Rotstein

By: _____
Laurence F. Pulgram

25 Attorneys for Plaintiffs Columbia
26 Pictures Industries, Inc., Columbia
27 Pictures Television, Inc., Columbia
28 TriStar Television, Inc., and TriStar
Television, Inc.

Attorneys for Defendants ReplayTV,
Inc. and SONICblue Incorporated

CC1-585468.1

1 designated under the Protective Order as "Confidential" or "Highly Confidential"
 2 Information or were produced without any designation under the Protective Order
 3 and EFF shall be entitled to have access to such responses and documents, subject to
 4 the provisions of the Protective Order (as applicable).

5
 6 DATED: September __, 2002

7 PROSKAUER ROSE LLP

O'MELVENY & MYERS LLP

8
 9 By: _____

By: _____

10 Scott P. Cooper
 11 Attorneys for Plaintiffs Metro-
 12 Goldwyn-Mayer Studios Inc., Orion
 13 Pictures Corporation, Twentieth
 14 Century Fox Film Corporation,
 15 Universal City Studios Productions
 16 LLLP (formerly, Universal City Studios
 17 Productions, Inc.), Fox Broadcasting
 18 Company, Plaintiffs Paramount Pictures
 19 Corporation, Disney Enterprises, Inc.,
 20 National Broadcasting Company, Inc.,
 21 NBC Studios, Inc., Showtime Networks
 22 Inc., UPN (formerly, The United
 23 Paramount Network), ABC, Inc.,
 24 Viacom International Inc., CBS
 25 Worldwide Inc., and CBS Broadcasting
 26 Inc.

Attorneys for Plaintiffs Time Warner
 Entertainment Company, L.P., Home
 Box Office, Warner Bros., Warner Bros.
 Television, Time Warner Inc., Turner
 Broadcasting System, Inc., New Line
 Cinema Corporation, Castle Rock
 Entertainment, and The WB Television
 Network Partners L.P.

22 MCDERMOTT, WILL & EMERY

FENWICK & WEST LLP

23 By: _____

By: 

24 Robert H. Rotstein

Laurence F. Pulgram

25 Attorneys for Plaintiffs Columbia
 26 Pictures Industries, Inc., Columbia
 27 Pictures Television, Inc., Columbia
 28 TriStar Television, Inc., and TriStar
 Television, Inc.

Attorneys for Defendants ReplayTV,
 Inc. and SONICblue Incorporated

CC1:585468.1

4

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

ROTHKEN LAW FIRM

By:



Ira P. Rothken

Attorneys for Plaintiffs Craig Newmark,
Shawn Hughes, Keith Ogden, Glenn
Fleishman and Phil Wright

ELECTRONIC FRONTIER
FOUNDATION

By:




Cindy A. Cohn

Attorneys for Plaintiffs Craig Newmark,
Shawn Hughes, Keith Ogden, Glenn
Fleishman and Phil Wright

ORDER

Good cause appearing therefore, the preceding stipulation of the parties in the above-captioned action, as evidenced by the signatures of counsel of record appearing above, is hereby ordered.

DATED: September 19, 2002



HONORABLE CHARLES F. EICK
United States Magistrate Judge

CC: 585468.1

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

PROOF OF SERVICE

I, Cora Moncrief, declare:

I am a resident of the State of California and over the age of eighteen years, and not a party to the within action; my business address is 1999 Avenue of the Stars, Seventh Floor, Los Angeles, CA 90067-6035. On September 18, 2002, I served the within document(s):

STIPULATION AND [PROPOSED] ORDER REGARDING THE NEWMARK PLAINTIFFS' ACCESS TO CONFIDENTIAL INFORMATION

by placing the document(s) listed above in a sealed envelope with postage thereon fully prepaid, in the United States mail at Los Angeles, California addressed as set forth below. I am readily familiar with the firm's practice of collecting and processing correspondence for mailing. Under that practice it would be deposited with the U.S. Postal Service on that same day with postage thereon fully prepaid in the ordinary course of business. I am aware that on motion of the party served, service is presumed invalid if the postal cancellation date or postage meter date is more than one day after date of deposit for mailing in affidavit.

Emmett C. Stanton, Esq.
Fenwick & West LLP
Two Palo Alto Square
Palo Alto, California 94306

Laurence F. Pulgram, Esq.
Fenwick & West LLP
275 Battery Street
San Francisco, CA 94111

Ira P. Rothken, Esq.
Rothken Law Firm
1050 Northgate Drive, Suite 520
San Rafael, CA 94903

Scott P. Cooper, Esq.
Proskauer Rose LLP
2049 Century Park East
Suite 3200
Los Angeles, California 90067

Robert H. Rotstein, Esq.
McDermott, Will & Emery
2049 Century Park East
34th Floor
Los Angeles, California 90067

Cindy Cohn, Esq.
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110

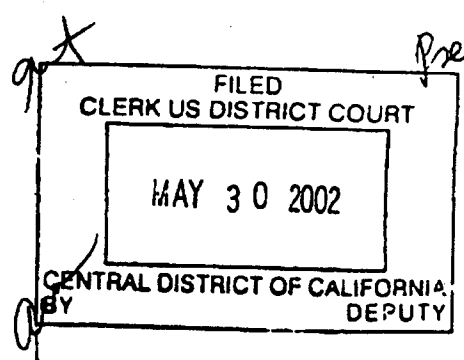
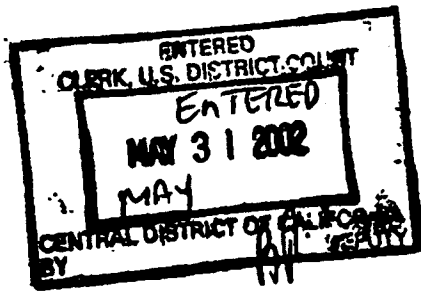
I declare under penalty of perjury under the laws of the United States that the above is true and correct.

Executed on September 18, 2002, at Los Angeles, California.



Cora Moncrief

EXHIBIT D



1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

PARAMOUNT PICTURES)
CORPORATION, et al.,

CV 01-9358 FMC (Ex)

Plaintiff,

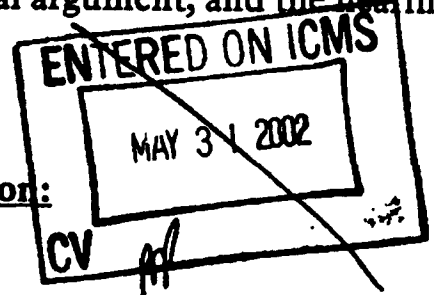
ORDER ON PARTIES' MOTIONS
FOR REVIEW OF MAGISTRATE
JUDGE'S DISCOVERY ORDER OF
APRIL 26, 2002

vs.

REPLAY TV, et al.,

Defendants.

This case is before the Court on the parties' requests for review of the Magistrate Judge's Discovery Order of April 26, 2002. The Court deems these matters suitable for resolution without oral argument, and the hearing set for June 3, 2002, is off calendar.



I. Order re Customer Use Data Collection:

A. Documents Considered:

In connection with this motion, the Court has read and considered the following documents:

- *Defendants' memorandum in support of objections and motion for review
- *Declaration of Laurence F. Pulgrum
- *Defendants' objections to Declaration of Craig O. Thomas
- *Plaintiffs' memorandum in opposition
- *Declaration of Simon Block in opposition
- *Defendants' reply memorandum
- *Brief of Technology Industry, *Amici Curiae*, in support of defendant's motion

1 *Plaintiffs' response to the brief of Technology Industry
2 *Brief of Liberties and Consumer Groups, *Amici Curiae*, in support of
3 defendants' motion.
4 *Transcript of oral argument conducted April 23, 2002.

5 ***B. Standard of Review:***

6 The Court has not considered the declaration of Craig O. Thomas in
7 opposition to defendants' motion, because that declaration was not considered
8 by, nor even presented to, the Magistrate Judge. This Court's function, on a
9 motion for review of a magistrate judge's discovery orders, is not to decide what
10 decision this Court would have reached on its own, nor to determine what is the
11 best possible result considering all available evidence. It is to decide whether
12 the Magistrate Judge, based on the evidence and information before him,
13 rendered a decision that was clearly erroneous or contrary to law. *Bhan v.*
14 *Hospitals, Inc.*, (9th Cir. 1991) 929 F.2d. 1404, 1414; F.R.C.P. 72(a); 28 USC
15 §636(b)(1)(A). Therefore, parties objecting to a magistrate judge's order may
16 not present affidavits containing evidence not presented below. *Paddington*
17 *Partners v. Bouchard*, (2nd Cir. 1994) 34 F.3d. 1132, 1137-8.

18 The Court sustains the defendants' objection to the Thomas declaration,
19 because it was not part of the record before the Magistrate Judge. The Court
20 has, for the same reason, not considered the Supplemental and Reply
21 declarations of Philippe Pignon.

22 ***C. Order Reviewed:***

23 The Magistrate Judge ordered defendants, within 60 days, to "do that
24 which Plaintiffs sought to be ordered at page 43, line 7 through page 44, line 10
25 of the Joint Stipulation..." By the terms of that order, therefore, defendants are
26 required to:

27 (1) take the steps necessary to use their broadband connections with
28 ReplayTV 4000 customers to gather all available information about how
 users of the ReplayTV employ the devices, including all available

1 information about what works are copied, stored, viewed with
2 commercials omitted, or distributed to third parties with the ReplayTV
3 4000, when each of those events took place, and the like;

4 (2) implement Defendants' offer to collect available data from a second
5 source – the MyReplayTV.com web site – about how users of the
6 ReplayTV employ the devices, but for all time periods for which that data
7 can be collected, rather than just for a short period;

8 (3) provide the foregoing data to Plaintiffs in a readily understandable
9 electronic format and provide any technical assistance that may be
10 necessary for Plaintiffs to review the data;

11 (4) provide Plaintiffs with all documents about Defendants' consideration
12 of what data to gather or not to gather about their customers' uses of the
13 ReplayTV 4000; and

14 (5) provide Plaintiffs with any other documents (such as emails or logs)
15 reflecting what works have been copied with the ReplayTV 4000 and how
16 those works have been stored, viewed, or distributed.

17 *D. Discussion:*

18 Defendants and *amici* raise numerous objections to this Order. Generally,
19 they contend that the order requires not that they produce material in discovery
20 but that they create new data; that the order is, therefore, not a discovery order
21 but an impermissible mandatory injunction; that the burdens on defendants
22 and their customers outweigh any benefit to the plaintiffs, and that the order
23 constitutes a serious and unnecessary invasion of ReplayTV4000 users' privacy
24 rights.

25 Although each of the issues raises serious questions, which have been very
26 well briefed on all sides, the Court is persuaded to reverse the Magistrate
27 Judge's Order on the grounds that it impermissibly requires defendants to
28 create new data which does not now exist. A party cannot be compelled to

1 create, or cause to be created, new documents solely for their production.
2 Federal Rule of Civil Procedure Rule 34 requires only that a party produce
3 documents that are already in existence. *Alexander v. FBI* (D.D.C. 2000) 194
4 F.R.D. 305, 310.

5 The only evidence before the Magistrate Judge on this issue was the
6 uncontroverted declaration of Philippe Pignon, Ph.D., Vice President of
7 Engineering Operations at defendant SONICblue, Inc. According to that
8 declaration, defendants were able to collect some customer-use data from earlier
9 versions of the ReplayTV. In May 2001, following negative publicity about the
10 data collection practices of defendants' competitor, TiVo, defendants stopped
11 all customer data-collection, except for technical information such as error
12 messages. Defendants have never collected customer data (other than limited
13 technical information) from ReplayTV4000 customers. Further, when
14 customer-use data was being gathered from ReplayTV customers, it did not
15 include information concerning Send Show or Commercial Advance, which
16 were not then in existence.¹

17 In order to gather information from customers about "what works are
18 copied, stored, viewed with commercials omitted, or distributed to third parties
19 with the ReplayTV4000 [and] when each of those events took place," defendants
20 would be required to undertake a major software development effort, incur
21 substantial expense, and spend approximately four months doing so.

22 It is evident to the Court, based on Pignon's declaration, that the
23 information sought by plaintiffs is not now and never has been in existence.
24 The Order requiring its production is, therefore, contrary to law. See *National*
25 *Union Elect. Corp. v. Matsushita Elec. Indust. Co.*, 494 F.Supp. 1257, 1261 (E.D.

26
27 ¹These two features are the most significant and relevant in connection
28 with the issues raised in this lawsuit.

1 Pa. 1980)²

2 The Court does not question the relevance of information concerning
3 how customers of ReplayTV4000 use their units. However, this information
4 can be obtained by plaintiffs by conducting surveys, a traditional method of
5 gleaning customer data in copyright-infringement cases.

6 That portion of the Magistrate Judge's Discovery Order of April 26, found
7 at page 3, paragraph 2, is hereby reversed.

8

9 **II. Defendants' Motion for Review of Order re Responses to Document**
10 **Requests No. 35 and 44:**

11 *A. Documents Reviewed:*

12 In connection with this motion, the Court has read and considered the
13 following documents:

- 14 *Defendants' Amended notice of motion for review of the order
- 15 *Defendant's points and authorities in support of the motion
- 16 *Corrected declaration of Emmett C. Stanton in support
- 17 *Plaintiff's opposition
- 18 *Defendant's Reply memorandum
- 19 *Declaration of Jennifer M. Lloyd in support of reply.
- 20 *Transcript of April 23, 2002, oral argument

21 *B. Standard of Review:*

22 A magistrate judge's nondispositive order may be set aside or modified
23 by a district court only if it is found to be clearly erroneous or contrary to law.
24 28 USC §636(b)(a)(A); Federal Rules of Civil Procedure, Rule 72(a).

25 *C. Order Reviewed:*

26 The Magistrate Judge denied defendant's motion to compel the
27 production of the following two items:

28

29 ²This Order does not affect the defendants' obligation to provide to
30 plaintiffs customer-use information presently being collected from the
31 approximately 10% of customers who are subscribers to MyReplayTV.com.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Request #35:

All Documents relating to plans for utilizing and/or actual or potential revenues available to Plaintiff by, Set Top Boxes, Interactive Television, and/or direct targeted advertising, including but not limited to Documents relating to Plaintiff's knowledge, evaluation, analysis, or communications concerning these subjects from 1984 to the present, including but not limited to compilations and evaluations of such information.

Request #44:

Documents sufficient to show Plaintiff's business plans, marketing strategies and forecasts from 1984 to the present relating to commercial advertising and/or alternative advertising methods.

D. Discussion:

Defendants first contend that the Magistrate Judge's failure to include these two production requests in his Order was clearly the result of a mistake. This argument is based on the fact that these items were not discussed in the Joint Statement in connection with similar requests (e.g., items 43, 45, 46, 47, and 48, which were compelled) but were handled separately in a different section of the Joint Statement. Defendants also argue that because production of similar items was compelled, the Magistrate Judge must have intended to include items 35 and 44 as well, but inadvertently failed to do so.

It does not appear to the Court that the denial of these requests was inadvertent. The transcript of the hearing on these motions reveals that the Magistrate Judge had carefully and thoroughly reviewed all of the parties' documents, acquainted himself with their positions and contentions, and was familiar with the relevant case law. The record does not lead the Court to

1 believe that the Magistrate made a mistake.³

2 Defendants next argue that the order is inconsistent with the Magistrate
3 Judge's ruling on similar requests and therefore erroneous. The Court
4 disagrees. The Magistrate Judge may well have concluded that his Order
5 compelling the production of other similar information provided the
6 defendants with all the relevant evidence they needed, and that anything
7 further would be excessive and burdensome.

8 The request to reverse this portion of the Magistrate Judge's Order is
9 denied.

10

11 **III. Plaintiff's Objections and Request for Review:**

12 *A. Documents Considered:*

13 In connection with this motion for review, the Court has read and
14 considered the following documents:

- 15 *Plaintiff's notice of motion for review and reconsideration
- 16 *Declaration of Robert H. Rotstein in support of motion
- 17 *Defendants' objections to declarations
- 18 *Plaintiffs' motion to strike portions of defendants' objections
- 19 *Defendants' Opposition
- 20 *Declaration of Emmett Stanton in support of opposition
- 21 *Plaintiffs' Reply

22 The Court has not considered the proffered declarations of Mike Cruz,
23 Frederick A. F. Cooke, Jr., Richard A. Frankie, Michelle Stratton, Del
24 Mayberry, Jane Waxman, Steve Rath, Michael Doodan or David C. Vigilante,
25 because these declarations were not presented to the Magistrate Judge for his
26 consideration. See discussion at section I.B, *supra*.

27

28 ³It appears to the Court that it would not be inappropriate for counsel to
inquire of the Magistrate Judge whether this portion of his ruling was intentional
or inadvertent.

1 *B. Standard of Review:*

2 A magistrate judge's nondispositive order may be set aside or modified
3 by a district court only if it is found to be clearly erroneous or contrary to law.
4 *Bhan v. Hospitals, Inc.* (9th Cir. 1991) 929 F.2d. 1404, 1414.

5 *C. Order Reviewed:*

6 Plaintiffs seek review of five categories of compelled discovery.⁴ These
7 are: (1) confidential financial documents; (2) confidential business plans;
8 (3) documents relating to MovieFly/MovieLink and Movies.com;
9 (4) documents and information in various categories concerning plaintiffs'
10 businesses dating from 1984 to 1996; and (5) documents relating to lobbying.

11 *D. Discussion:*

12 The Court has carefully reviewed all of plaintiffs' objections and
13 arguments concerning the Magistrate Judge's rulings in each of these categories.
14 Although the arguments made concerning the breadth and scope of the orders
15 are not unreasonable, and certainly different orders could have been issued, the
16 unfailing conclusion reached by this Court with respect to each issue is that the
17 Magistrate Judge's orders are not clearly wrong or contrary to law. No legal
18 basis exists for this Court to reverse any of the discovery orders of which
19 plaintiffs complain.

20 Dated this 30th day of May 2002.

21
22 
23 FLORENCE-MARIE COOPER, Judge
24 United States District Judge

25
26
27 ⁴In their Notice of Motion, plaintiffs set out three categories; however, in
28 the body of their motion, they identify five categories of discovery as to which
they seek review and reconsideration.

EXHIBIT E

In the 210th Issue of EFFector:

- [ALERT: Act Now to Stop BPDG From Hobbling Digital TV \[global\]](#)
- [ALERT: Further Update on House Digital Music Alert \[US\]](#)
- [ALERT: ICANN Seeks Comments on Reform \[global\]](#)
- [Court Hears Argument on Constitutionality of DMCA](#)
- [EFF's "Consensus at Lawyerpoint" Blog and Alphabet Soup Contest](#)
- [Exchange Ideas with EFF Founders Kapor & Barlow](#)

For more information on EFF activities & alerts: <http://www.eff.org/>

To join EFF or make an additional donation:

<http://www.eff.org/support/>

EFF is a member-supported nonprofit. Please sign up as a member today!

ALERT: Act Now to Stop BPDG From Hobbling Digital TV

Hollywood Threatens Your Rights (Again)

Electronic Frontier Foundation ACTION ALERT

(Issued: April 5, 2002 / Deadline: April 17, 2002)

Introduction:

Well, Hollywood's at it again. This time, the entertainment giants are meeting behind closed doors with key consumer electronics and computer companies. Using the rubric of eliminating "piracy," this semi-secret group will set the standards for over-the-air broadcast signals of digital television (DTV), the new TV format that will replace current broadcasts by the year 2006.

While the broadcasts will remain unencrypted, Hollywood is determined to cripple the equipment that can actually receive the broadcasts. Through the Broadcast Protection Discussion Group (BPDG), an industry forum meeting in Los Angeles, Hollywood is writing a "technical standard" that will restrict digital television equipment -- TVs, VCRs, personal video recorders, and computer "tuner cards" -- capable of receiving digital TV broadcasts.

The BPDG is determined to exclude the public from its discussions. Members of the press are not permitted in BPDG and CPTWG (Content Protection Technology Working Group--BPDG's mother organization) meetings. In order to attend BPDG meetings, one has to come (in person) to Los Angeles and pay a \$100 fee -- per meeting. There are no call-in numbers and no public minutes or records of what takes place. In fact, in order to find out that BPDG existed, you had to be a member of one of a handful of trade associations, or be present in person at one of a handful of industry conferences. There was no press release and there is still no public web site run by BPDG or any participating organization (except EFF). BPDG had been meeting for months

before references to it were made in recent Congressional testimony regarding the SSSCA and CBDTPA legislation.

Let Hollywood's self-appointed technology cops know what you think of restricting broadcast television!

What YOU Can Do Now:

- EFF encourages you to write to the Drafting Committee working on these rules to let them know what you think. To date, the Drafting Committee has received only the opinions of major companies -- not of small businesses or of users. You can read the drafts of the rules they've promulgated (see below) and respond specifically to the technical details. Feel free to use the EFF's sample letter below as a starting point for your comments. You should also feel free to write your own letter about general issues related to BPDG's work.

Let the BPDG Drafting Committee know that you are concerned about their efforts to control your use of free over-the-air television broadcasts, and the long-term effects of government mandates on innovation. Please be polite and concise, but firm.

- Contact your legislators about this issue. For information on how to contact your legislators and other government officials, see EFF's "Contacting Congress and Other Policymakers" guide at:
<http://www.eff.org/congress.html>
- Join EFF! For membership information see:
<http://www.eff.org/support/>

Sample Letter:

Use this sample letter as a model (please do not send it verbatim), and send your own letter to:
BPDG Drafting Committee
bpdg-draft@list.lmicp.com

Dear BPDG Drafting Committee:

I'm writing to object to what the BPDG is doing -- meeting in private to bargain away my rights as a consumer and the rights of engineers to create the best possible products for me.

You're creating a future where innovation and consumers' choices will take a back seat to copyright holders' fears. You're setting a precedent for government involvement in technology where open competition is set aside and winners and losers are chosen, not by competition or by giving the public a choice, but by a bureaucrat or by an "industry consensus".

This precedent sets the stage for other mandates on the design of PCs, software, and computer networks, with implications far beyond television broadcast. Jack Valenti is already talking about the "analog hole" and looking for a new mandate to prevent digitizing-without-a-license. We need to draw the line where it was drawn in 1984: if a

device -- like a VCR or something as-yet uninvented -- serves a legitimate consumer use then its manufacture, sale and improvement is legal, even if it frightens Mr. Valenti.

I have the right to time-shift television programs, to space-shift them, to format-shift them, and to use technology to help me make the most of free over-the-air TV programming. I should have my choice of any technology that helps me make a legitimate use -- and plenty of manufacturers are prepared to give it to me.

When technology companies want to build products that enable my legitimate use, it's not your business to get in their way. If the electronics companies represented at CPTWG don't care to sell me the best possible products, I want the right to turn to other companies who will continue to put my interests first. Equipment subject to a mandate is going to be less capable, more expensive, take longer to invent, and prevent user-serviceability. New devices under such a mandate will lack even the features of currently available digital TV equipment -- so you're arranging for technology to get worse, not better.

The standards you're creating have no conceivable technical purpose except as raw material for legislation or regulation; there isn't even the faintest pretense that they're "purely technical" and free of policy implications.

BPDG is working closely with people whose job is to get what you come up with enacted into law. You're creating legislation in private to spring upon us in the hope we won't notice.

I should not be punished in advance for the possibility that someone else will commit a crime. That's exactly what technology mandates do; they undermine my rights even though there's no indication that I've done, or will do, anything wrong. They take away my choices. They impose costs on me. They slow down innovation and give the entertainment industry veto power over technologists. They treat me like a criminal.

I don't want to be treated like a criminal.

Sincerely,

[Your name;
include full address for maximum effectiveness]

Tips:

Please remember to be polite but firm. Ranting, swearing, or lack of clear focus and resolve will not make a good impression. Try to make it brief (1 page or less written, or a few sentences spoken) and clear, without getting into nitpicky details. Re-casting the letter in your own words will be more effective than copy-pasting our sample.

Activists Around the World

This alert is mostly for U.S. residents, but the technology policy issue and its effects will be felt globally, so non-U.S. activists should send in letters as well.

Background:

Since the FCC has mandated that broadcasts will remain unencrypted, Hollywood is determined to seal any device capable of touching digital video in layers of tamper-proof laws and innovation-dampening "standards." They call themselves the Broadcast Protection Discussion Group (BPDG), and they're writing a "technical standard" that will restrict digital television equipment -- TVs, VCRs, personal video recorders, and computer tuner cards -- capable of receiving digital TV broadcasts.

The standard BPDG is developing is a dense technical document called the "BPDG Compliance and Robustness Rules". Here "compliance" means that a device will do what Hollywood wants (as opposed to what its owner wants); "robustness" means that it will be difficult (and illegal!) for the owner to modify the device. The result is that you'll get equipment which is less functional, less flexible, more expensive, less interoperable, and harder to fix, modify, or upgrade.

Links:

New brief EFF introduction to BPDG:

<http://bpdg.blogs.eff.org/archives/000008.html>

"Consensus At Lawyerpoint" -- EFF news site with regular BPDG updates, docs:

<http://bpdg.blogs.eff.org/>

Copy Protection Technical Working Group, the parent organization of the BPDG:

<http://www.cptwg.org/>

Charter of Broadcast Protection Discussion Group:

http://www.eff.org/IP/Video/HDTV/20011214_bpdg_draft_charter.html

5C consortium introduction/proposal/rationale for BPDG's work:

http://www.eff.org/IP/Video/HDTV/20011128_5c_bpdg_introduction.html

Current discussion draft of BPDG Compliance and Robustness Rules:

http://www.eff.org/IP/Video/HDTV/20020326_bpdg_compliance_rules.pdf

Current drafts of language to ban all "non-compliant" devices and software:

http://www.eff.org/IP/Video/HDTV/20020215_bpdg_mpa_rider.html

http://www.eff.org/IP/Video/HDTV/20020215_bpdg_ce_it_rider.html

CAFE Campaign:

This drive to contact BPDG Drafting Committee with your objections to Hollywood control of digital media technology is part of a larger campaign to highlight intellectual property industry assaults against the public's fair use rights, and what you can do about it.

Check the EFF *Campaign for Audivisual Free Expression* (CAFE) website regularly for additional alerts and news:

<http://www.eff.org/cafe/>

About EFF:

The Electronic Frontier Foundation is the leading civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. EFF is a member-supported organization and maintains one of the most linked-to websites in the

EXHIBIT F

Copyright 2002 Informa Publishing Group Plc.
Broadband Media

March 25, 2002

SECTION: Broadband Media

LENGTH: 2527 words

HEADLINE: Rights-protection issues block way to broadband content flow

BYLINE: Joseph Smithies, joseph.smithies@informa.com

BODY:

"There will be no property in cyberspace," predicted John Perry Barlow in 2000. Speaking less as a former lyricist for the Grateful Dead than as a co-founder of internet civil-rights group the Electronic Frontier Foundation, Barlow heralded a post-Napster era of "dotcommunism". In this new world, digital copyright would become an irrelevance as the content industry realised it could actually benefit from the free publicity of pirate distribution.

Two years on, that vision looks decidedly utopian, as an understandable corporate paranoia continues to swirl around all aspects of digital piracy.

Witness this month's astonishing claim and counterclaim between smart-card manufacturers NDS and Canal+ Technologies, the latter alleging codebreaking and industrial sabotage. While arguments over digital-protection standards rumble on, the content "majors" are growing increasingly restive, eager to have an unbreakable rights-management solution in place before household broadband takes off and mass-media downloading becomes ubiquitous.

"There is no better example of the content community's potential, as well as its vulnerability, than the rollout of broadband access," News Corp. president Peter Chernin told a recent US congressional hearing.

"Without adequate technological and legal protections for intellectual property, content producers and legitimate content distributors will find themselves vulnerable to theft by anyone who has broadband access."

Such protections have proved hard to implement. Technological solutions are not standardised, while legislative measures are criticised for curtailing consumer rights. With proposals to enforce standardisation now on the table in the US, the argument has moved to Capitol Hill, where copyright holders clamour for government intervention to secure content, and consumer rights groups join with electronics manufacturers to resist the changes.

Meanwhile, the first of two global treaties intended to safeguard the rights of copyright owners on the internet came into force this month.

Showing some degree of foresight, the UN's World Intellectual Property Organisation (WIPO) proposed two treaties to address the issue of digital-media distribution back in 1996, three years before Napster made it urgent.

WIPO's Copyright Treaty finally gained sufficient signatories to become law on March 6. A related pact, the WIPO Phonograms and Performances Treaty (WPPT), will take effect on May 20. The two documents give performing artists and producers exclusive rights to reproduce and distribute their

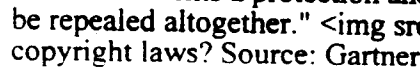
work over the internet, and provide a basis for them to challenge any distortions caused by digital manipulation. They also prohibit unauthorised distribution of hacked media files.

The treaties themselves have aroused no great controversy, being brief documents with little technical detail. **But the US legislation that incorporated them, the Digital Millennium Copyright Act (DMCA), has attracted fierce criticism since its enactment in 1998.**

At the request of content-industry lobbyists, the DMCA outlawed the circumvention of digital-rights-management (DRM) controls to gain access to electronic media. The act also banned any device or service whose primary purpose was to facilitate copyright infringement. In return, content providers at the time promised a flood of compelling broadband content to drive network construction and consumer demand.

But bodies such as Barlow's Electronic Frontier Foundation are furious at what they see as the DMCA's violation of the long-standing "fair use" principle, which allows consumers to make personal copies of copyright material for noncommercial purposes.

Chief among the "chilling effects" of the DMCA, according to the EFF's Fred von Lohmann, is that it stifles technological innovation in several areas, including DRM. Von Lohmann points to the case of a Princeton professor who answered a challenge to defeat watermarking technologies proposed for digital audio files. When he attempted to publish his findings demonstrating flaws in current watermarking techniques, he was threatened with civil action under the DMCA by the organisers of the challenge.

"That's exactly the kind of wrong-headed abuse that we warned would occur," says von Lohmann, "because there's no obvious end-point. What's the difference between a device or a broadband service that circumvents a protection and a professor who tells you how to do it? Ideally, the DMCA should be repealed altogether."  <caption>Does free music file sharing violate copyright laws? Source: Gartner

The fair-use issue does not only affect consumers. Voices as diverse as the Canadian Copyright Forum and the UK Patent Office have warned of the damaging effect of digital-rights legislation on e-learning, already an established broadband application thanks to high-speed academic networks.

They argue that libraries and academics are not being given clear dispensation to skip copy protection for nonprofit purposes.

US critics claim that the DMCA, a law intended to prevent DRM circumvention, has ironically succeeded more in allowing litigious parties to circumvent a defendant's right to free speech under the First Amendment. Either way, the promised flood of content has not materialised, while the major labels' MusicNet and pressplay services have taken a maximally cautious approach to licensing.

"Until industry can resolve concerns over digital-rights management and copyright protection for movies, music and games, the biggest drivers of commercial broadband adoption will remain on the sidelines," said Bruce Mehlman of the US Commerce Department in October. Weeks later, Federal Communications Commission chairman Michael Powell advanced the same argument, as did Disney and News Corp. representatives last month. It seems the DMCA has failed to ease copyright-holders' concerns after all.

Many observers believe the only way to resolve the issue is to establish industry-standard protection techniques that work across all devices, platforms and legal jurisdictions. So far the electronics industry has instead employed a range of proprietary measures. Enter Democrat Senator Ernest Hollings, whose Security Systems Standards and Certification Act (SSSCA) is still at bill stage, but stands every chance of being passed next month. Von Lohmann describes the proposals, which would extend the scope of the DMCA's powers, as "the next step in the wrong direction".

The SSSCA would require every "interactive digital device" sold in the US, from PCs to camcorders,

to incorporate a standardised copy-protection technology. Individuals who violate the protection face heavy fines or imprisonment. And if industry cannot devise such a standard within 18 months of the legislation's passage, the government would intervene to impose one. Unsurprisingly, the bill is opposed by electronics firms, who express little appetite to become copyright enforcers on behalf of the entertainment industry.

"The pressure of a timeline for eventual government action is critical to yield the desired standards in a reasonable time frame." Disney's Eisner warned Congress. He and News Corp.'s Chernin controversially implied that some electronics firms were resisting standardisation because they profited from piracy. "At least one high-tech executive has described illegal pirate content as a 'killer application' that will drive demand for broadband," Eisner claimed.

While it is wrong to caricature the debate as between content players and hardware firms - AOL Time Warner, for example, has strong reservations about the Hollings bill - it is not the first time the two industries have clashed on copyright issues. The Secure Digital Music Initiative, a private-sector attempt to establish security standards, collapsed because of disagreement between content and hardware parties.

But others argue that piracy is not what is really holding back broadband content; rather, it is copyright-holders' fear of new distribution channels, and their determination to stifle innovation. In his evidence to last month's commerce committee, Mitsubishi's Robert Perry invoked the well-worn example of home video recorders - the so-called "Betamax defence".

When early VCR technology emerged in the late 1970s, the US film industry feared a negative impact on revenues. The Court of Appeals eventually banned Sony's Betamax VCR, but the decision was overturned by the Supreme Court. It then became apparent that the movie industry would actually benefit from the technology through video sales and rental revenue, while the hardware firms were left to develop and improve the technology.

Perry also argued that studios and cable operators were ultimately seeking the power to turn off individual elements within future home networks if they believed a copyright violation was taking place.

These home networks, based on multimedia entertainment centres, are a real area of concern for major content providers, who fear multiple copies of their titles existing on wirelessly linked devices in the home. The Copy Protection Technical Working Group, a consortium of Hollywood studios, TV networks and consumer electronics firms, is now calling for all digital broadcasts to be tagged so that duplication in the home can be controlled.

Herein lies another potential dispute, should the electronics manufacturers break rank. The home network's raison d'être is to offer convenience, yet wireless watermarking would require a whole new set of DRM techniques that could inhibit the transfer of data between devices. The process of encryption and decryption could, at the least, slow the networks down.

And recent history suggests industry may struggle to establish a wireless DRM standard in the three years before wireless LAN is expected to take off in the home.

Five leading hardware manufacturers - Intel, Hitachi, Sony, Toshiba and Matsushita - have formed a body, known as 5C, to agree a common specification for wireless encryption. But talks between the group and content owners such as News Corp. are at an impasse, with 5C arguing that broadcasters would not be willing to have a copyright "flag" embedded in their output.

Meanwhile, Forrester Research warns that home gateways could even be outlawed under the DMCA - a credible outcome, given the current litigation surrounding PVRs, including a case between manufacturer SONICblue and the Motion Picture Association of America. Such is the ongoing nature of these disputes that many fear they will become a permanent eyesore on the future digital landscape. As long as new technology is developed, content owners will always seek to close new

avenues for piracy, according to Tony Ghee, head of film and media practices at law firm Ashurst Morris Crisp.

"They're just never going to allow the release of their material in digital form unless they have complete control over it," says Ghee. "So I'm never going to be able to use a VoD service from outside the US to access a new Hollywood movie ahead of the release in Europe. They just won't allow it."

Ghee also questions whether the very concept of copyright can ever be effectively enforced on the internet community, which extends across countless legal jurisdictions. "If I'm sitting in London," he asks, "do I really care whether I've broken the law in the United States?"

But Simon Halberstam, of London law firm Sprecher Grier Halberstam, disagrees.

"The concept of copyright has been recognised all over the world, and it's wide enough a concept to adapt to what happens on the internet, including multimedia." But without failsafe DRM technology, the law itself is useless.

"A lot of users don't care about the law, because it's an ass as far as the internet is concerned. As long as people can infringe copyright, because the technology allows them to do so, they will do so - whatever the legal rights or wrongs."

Lawyers and technologists concur that most consumers will lose interest in overcoming copyright controls once they are sufficiently advanced and widespread to make circumvention a laborious process. If so, the current and proposed legislation in the US may indeed be unnecessarily heavy-handed.

Now the debate is set to move to Europe, where EU member states are aiming to bring their domestic law into line with the WIPO treaties by the end of this year. According to the EFF's von Lohmann, the legislation used to do this may commit the same mistakes as the DMCA. A body in the UK, the Campaign for Digital Rights, part of the Europe-wide group Eurorights.org, is already resisting DMCA-like controls in the forthcoming European copyright directive.

In the meantime, all eyes are on Washington, where the future of the Hollings bill will soon be decided. Mitsubishi's Perry has argued for a calm, retrospective approach to copy protection, with "balanced licence agreements" implemented over an "appropriate time scale". If that is a call for private-sector solutions, implemented retrospectively once broadband access is widespread, it is echoed by Laurence Kaye, head of technology at Andersen Legal, who urges copyright holders to take a risk.

"Let's get the content and the services up there," he suggests. "If we then find that there are legal problems, we can address them with an understanding of how consumers use the technology. Clearly a balance needs to be struck, but I don't think we're heading for a tsarist copyright state."

Consumer groups and hardware firms in the US are less sure. The novelty of the high-speed internet means there is little precedent to call upon in a legal field that is evolving almost daily.

It says much for the uncertainty surrounding the broadband-copyright debate that no one is keen to predict the imminent outcome of the ongoing case between BT and a little known US ISP, Prodigy. The telco is seeking to claim a 1989 patent for hyperlinking, a simple but fundamental technology on which the entire internet relies. CONTACTS Andersen Legal Garretts

4 Brindleyplace

Birmingham B1 2JZ

UK

T: (44) 121 644 2001

F: (44) 121 644 2101

www.andersenlegal.com Ashurst Morris Crisp

Broadwalk House

5 Appold Street

London EC2A 2HA

UK

T: (44) 20 7638 1111

F: (44) 20 7638 1112

www.ashursts.com Copy Protection Technical Working Group

c/o **MPAA**

15503 Ventura Boulevard

Encino

CA 91436

US

T: (1) 818 995 6600

www.cptwg.org **Electronic Frontier Foundation**

454 Shotwell Street

San Francisco

CA 94110-1914

US

T: (1) 415 436 9333

F: (1) 415 436 9993

www.eff.org The Patent Office

Concept House

Cardiff Road

Newport

South Wales

NP10 8QQ

UK

T: (44) 1633 813930

F: (44) 1633 813600

www.patent.gov.uk Sprecher Grier Halberstam

Lincoln House

300 High Holborn

London WC1V 7JH

UK

T: (44) 20 7544 5555

F: (44) 20 7544 5565

www.weblaw.co.uk World Intellectual Property Organization

PO Box 18

CH-1211 Geneva 20

Switzerland

T: (41) 22 3389 111

F: (41) 22 7335 428

www.wipo.int

LOAD-DATE: May 14, 2002

EXHIBIT G



Electronic Frontier Foundation

- [EFF Home](#)
- [Join EFF/Donate!](#)
- [About EFF](#)
- [Free Speech Online](#)
- [Audiovisual Freedom](#)
- [Online Privacy](#)
- [Active Legal Cases](#)
- [Recent News](#)
- [EFF BPDG Blog](#)
- [EFF Newsletter](#)
- [Internships](#)
- [EFF Topics](#)
- [Radio EFF](#)
- [Contact Us](#)
- [Calendar](#)
- [Media Resources](#)

[Subscribe to the
EFF Action Alert!](#)

Got a domain
name (UDRP)
problem? [Click
here.](#)

[EFF Privacy Policy](#)

Search:

[Site
Map](#)

[Most Popular EFF Pages
Today](#)

[Français: Au sujet de l'EFF](#)
[Italiano: Informazioni riguardo la EFF](#)

About EFF

General Information About the Electronic Frontier Foundation

- [Introduction](#)
- [Who We Are](#)
- [A History of Protecting Freedom Where Law and Technology Collide](#)
- [Today's Issues](#)
- [Representing the Rights of People](#)
- [Related Sites and Other Rights](#)
- [Contact Us](#)
- [Staff/Board List](#)
- [How to Support the Electronic Frontier Foundation](#)

Imagine a world where technology can empower us all to share knowledge, ideas, thoughts, humor, music, words and art with friends, strangers and future generations.

That world is here and now, made possible with the electronic network -- the Internet -- with the power to connect us all. And future developments in technology will enable us to access information and communicate with others in even more powerful ways.

But governments and corporate interests worldwide are trying to prevent us from communicating freely through new technologies, just as when those in positions of power controlled the production and distribution of -- or even burned -- books they did not want people to read in the Middle Ages. But only by fighting for our rights to speak freely whatever the medium -- whether books, telephones, or computers -- can we protect and enhance the human condition.

The Electronic Frontier Foundation (EFF) was created to defend our rights to think, speak, and share our ideas, thoughts, and needs using new technologies, such as the Internet and the World Wide Web. EFF is the first to identify threats to our basic rights online and to advocate on behalf of free expression in the digital age.

Who We Are

Based in San Francisco, EFF is a donor-supported membership

organization working to protect our fundamental rights regardless of technology; to educate the press, policymakers and the general public about civil liberties issues related to technology; and to act as a defender of those liberties. Among our various activities, EFF opposes misguided legislation, initiates and defends court cases preserving individuals' rights, launches global public campaigns, introduces leading edge proposals and papers, hosts frequent educational events, engages the press regularly, and publishes a comprehensive archive of digital civil liberties information at one of the most linked-to websites in the world: <http://www.eff.org>.

A History of Protecting Freedom Where Law and Technology Collide

The Electronic Frontier Foundation was founded in July of 1990 in response to a basic threat to speech. The United States Secret Service conducted series of raids tracking the distribution of a document illegally copied from a BellSouth computer that described how the emergency 911 system worked, referred to as the E911 document. The Secret Service believed that if "hackers" knew how to use the telephone lines set aside for receiving emergency phone calls, the lines would become overloaded and people facing true emergencies would be unable to get through.

One of the alleged recipients of the E911 document was the systems operator at a small games book publisher out of Austin, Texas, named Steve Jackson Games. The Secret Service executed a warrant against the innocent Jackson and took all electronic equipment and copies of an upcoming game book from Steve Jackson Games's premises. Steve Jackson panicked as he watched the deadline come and go for his latest release and still hadn't received his computers back. He was forced to lay off nearly half of his staff. In the end, the Secret Service returned all of Steve Jackson's computers and decided not to press charges against the company, since they were unable to find any copies of the E911 document on any of the computers.

In the meantime, Steve Jackson's business was nearly ruined. And when he and his employees had the opportunity to investigate the returned computers, they noticed that all of the electronic mail that had been stored on the company's electronic bulletin board computer, where non-employee users had dialed in and sent personal messages to one another, had been individually accessed and deleted. Steve Jackson was furious, as he believed his rights as a publisher had been violated and the free speech and privacy rights of his users had been violated. Steve Jackson tried desperately to find a civil liberties group to help him, to no avail. Unfortunately, none of the existing groups understood the technology well enough to understand the import of the issues.

In an electronic community called the Whole Earth 'Lectronic Link (now WELL.com) several informed technologists understood exactly what civil liberties issues were involved. Mitch Kapor, former president of Lotus Development Corporation, John Perry Barlow, Wyoming cattle rancher and lyricist for the Grateful Dead, and John Gilmore, an early employee of Sun Microsystems, decided to do something about it. They

formed an organization to work on civil liberties issues raised by new technologies. And on the day they formally announced the organization, they announced that they were representing Steve Jackson Games and several of the company's bulletin board users in a lawsuit they were bringing against the United States Secret Service. The Electronic Frontier Foundation was born!

The Steve Jackson Games case turned out to be an extremely important one in the development of a proper legal framework for cyberspace. For the first time, a court held that electronic mail deserves at least as much protection as telephone calls. We take for granted today that law enforcement must have a warrant that particularly describes all electronic mail messages before seizing and reading them. The Steve Jackson Games case established that principle.

The Electronic Frontier Foundation continues to take on cases that set important precedents for the treatment of rights in cyberspace. In our second big case, *Bernstein v. U.S. Dept. of Justice*, the United States government prohibited a University of California mathematics Ph.D. student from publishing on the Internet an encryption computer program he had created. Years before, the government had placed encryption, a method for scrambling messages so they can only be understood by their intended recipients, on the United States Munitions List, alongside bombs and flamethrowers, as a weapon to be regulated for national security purposes. Companies and individuals exporting items on the munitions list, including software with encryption capabilities, had to obtain prior State Department approval.

Encryption export restrictions crippled American businesses and damaged the free speech rights of individuals. Critical for e-commerce, companies use encryption to safeguard sensitive information, such as credit card numbers, which they send or receive over electronic networks. Companies also secure access to software programs and provide system security using encryption. By limiting the export of encryption, technologies and methods, the U.S. government drove development of security software overseas, where American companies were unable to compete.

The State Department was unsympathetic to Bernstein's situation and told Bernstein he would need a license to be an arms dealer before he could simply post the text of his encryption program on the Internet. They also told him that they would deny him an export license if he actually applied for one, because his technology was too secure.

The Electronic Frontier Foundation pulled together a top-notch legal team and sued the United States government on behalf of Dan Bernstein. The court ruled, for the first time ever, that written software code is speech protected by the First Amendment. The court further ruled that the export control laws on encryption violated Bernstein's First Amendment rights by prohibiting his constitutionally protected speech. As a result, the government changed its export regulations. Now everyone has the right to "export" encryption software -- by publishing it on the Internet -- without prior permission from the U.S. government. Once again, the Electronic Frontier Foundation led the

charge to establish important cyberspace rights.

Today's Issues

While early threats to our right to communicate came from the government, current threats come also from industry, as it seeks to control and expand current revenue sources at the expense of traditional fair use. The trend has been for industry to use a combination of law and technology to suppress the rights of people using technology. Nowhere is this more evident than in the world of copyright law, where the movie and recording studios are trying to dumb down technology to serve their "bottom lines" and manipulate copyright laws to tip the delicate balance toward intellectual property ownership and away from the right to think and speak freely.

2600 Case:

In December of 1999, a Norwegian teenager who participated in the open source development of the Linux operating system, reverse-engineered the Content Scrambling System (CSS) encryption code on DVDs and posted his decryption code, called DeCSS, to the Internet. To make a DVD player for Linux-based machines, engineers closely examined existing DVD players, and new player software was written to operate similarly. This is a legal and common method of competing in all industries.

The DeCSS code spread like wildfire among Linux developers on the Internet. 2600 Magazine, like many other members of the press, printed the code and a story describing DeCSS's importance on the magazine's website. The story also included a list of links to other locations publishing the code.

Eight major motion picture studios sued 2600 Magazine based upon its publication of the DeCSS code, its news coverage of the controversy, and links the magazine provided to the code.

The case was brought under the Digital Millenium Copyright Act (DMCA). The 1998 law said that distribution of a tool that could be used to get around copyright protections was itself illegal. Any attempts to get to a digital work, even to use it for legitimate purposes (such as for scientific inquiry or presentation in educational materials) was in effect prohibited, since it was illegal to get past the copy protections to make the legal copies. It also meant that people who published the code were still vulnerable to prosecution, even if they never used the code to access any copyrighted materials.

EFF rushed to the defense of 2600 Magazine to argue that the DMCA is unconstitutional on First Amendment grounds since DeCSS was already widely available and therefore in the public domain and since the magazine has the right to publish and link to technology enabling the fair use of copyrighted materials. We pulled together a stellar legal team, including Kathleen Sullivan, noted constitutional scholar and Dean of Stanford Law School. The case is currently on appeal.

Felten Case:

The recording industry has tried for several years to establish methods of dispensing digital music that mirror their traditional revenue streams, where limited access to packaging and distribution channels creates a huge demand for their services. They have struggled with recent technological innovations, since the Internet does not require a "middleman" for artists to get music to their fans. In fact, the technology facilitates copying and distribution, making music industry attempts to maintain the current scarcity model very difficult indeed. The music industry asked several technology vendors to embed software in music to restrict use of the music. Using a music control technology, a copyright holder might choose to limit listeners to playing a song only once. Then the software would disable further playing of the song until the listener paid more money.

Six different technologies were developed for the music industry's Secure Digital Music Initiative (SDMI). SDMI decided to challenge the Internet community to see if anyone could break through these embedded instructions on any of these technologies and issued the "Hack SDMI Challenge." As well as letting anyone try the Challenge, SDMI also offered \$10,000 to anyone who was willing to sign over his or her winning method to SDMI and keep it secret from the public.

A Princeton University computer science professor named Edward Felten participated in the challenge, along with graduate students from Princeton and Rice Universities and a researcher from Xerox PARC. They largely succeeded in defeating the technologies. They decided to forego the \$10,000 prize, however, and sought to present their findings at a technical conference. A couple of weeks before the conference, Professor Felten received a threatening letter from SDMI telling him that if he made the presentation at the conference, the researchers, the universities and the conference itself would all be in violation of the DMCA. Professor Felten gave in to the forced by SDMI and withdrew the paper at the last minute.

The Electronic Frontier Foundation is now representing Professor Felten and the other researchers in a lawsuit against the recording industry, asserting their rights under the First Amendment to publish and speak about their findings at a scientific conference and their right to publish and present future works. We also represent USENIX Association, which is sponsoring the conference where the paper is to be presented, and, of course, intends to sponsor future conferences.

Related Challenge:

In *Pavlovich v. DVDCCA*, the DVD Copy Control Association, which is associated with the Motion Picture Association of America (MPAA), is suing hundreds of individuals who put DeCSS on their websites, alleging that plaintiffs misappropriated trade secrets when they reverse engineered DVD technology. EFF is coordinating the defense and won an initial victory in December 2000 when the California Supreme Court granted defendant Matthew Pavlovich's petition for review, sending the matter back to the trial judge. At issue is whether California courts have jurisdiction over computer users outside California, the First

Amendment right to free expression, and the right to engage in lawful reverse engineering.

Challenging Internet Blocking:

Congress passed the Children's Internet Protection Act (CHIPA), a controversial censorware law that will force public and private libraries and schools that receive federal funding to install Internet blocking or filtering software for both child and adult Internet users. As part of its Blue Ribbon Campaign, EFF opposes this mandatory censorware law. March 2001, EFF, ACLU, the American Library Association (ALA) and other organizations filed a lawsuit challenging the new federal law.

EFF believes that the government should not mandate how schools and libraries protect children from inappropriate materials. Filtering software is currently abysmally ineffective and damaging to the educational process, blocking out many materials that children should be able to see (including groups that do not share the same political philosophy as the filtering software manufacturer), and not effectively blocking materials that are legally obscene, child pornography or harmful to minors in a given local community. Studies have shown that the more effectively a filtering program blocks inappropriate materials, the more overblocking of appropriate materials occurs, restricting the flow of information available on the Internet to a trickle. Knowing this, schools and libraries may protect children in another way, such as through education on Internet use and age-appropriate supervision by parents, teachers and librarians. The federal government should not be involved. Along with the legal cases, EFF has been working with other groups, such as the Online Policy Group and the ACLU, on a public education campaign.

Trademark Law - Domain Name Cases:

EFF has taken on several legal cases to protect the right to publish on the Internet without fear of trademark infringement lawsuits. In the Ford v. Great Domains case, the Ford Motor Company has sued several independent website operators whose domain names contain the words "volvo," "ford" or "jaguar" using a law intended to prevent "cybersquatting." EFF is defending several of those charged by Ford. In the most egregious example, Ford is accusing www.jaguarcenter.com - a site about big cats -- of trademark infringement.

Anonymity:

EFF is currently combating the growing practice of using the threat of unsubstantiated civil lawsuits to undermine the privacy rights of Internet users. Companies or individuals who want to know the identity of an anonymous Internet poster have begun serving legal documents on the poster's Internet Service Provider (ISP), which is then legally required to release the identity of the anonymous poster. Often, these posters are employee-whistleblowers who are posting anonymously for fear of losing their jobs. After forcing disclosure of the poster's identity, the company or individual then drops their spurious lawsuit, often firing the employee who did the posting. EFF has taken on several legal cases to quash such civil subpoenas because of the free speech

implications of the cases. We believe that the people filing the lawsuit must show some sort of likelihood of winning the case on the merits before an ISP reveals the poster's identity. Along with our legal cases, we've created a campaign to educate ISPs on their rights and responsibilities in relation to civil subpoenas.

Peer-to-Peer Technologies:

EFF is concerned that the creators and developers of peer-to-peer (P2P) technologies have become music industry targets, especially in the wake of the 9th Circuit Court of Appeal's Napster decision and the music industry's public vows to sue other P2P systems. Unfortunately, the recording industry has targeted the technology instead of the users who are actually violating their copyrights. Peer-to-peer technology is a wonderful tool for the mass distribution of all sorts of content. EFF believes that, in its zeal to stop illegal trading of copyrighted songs online, the music industry will cause significant damage to the developers of this new technology.

We have begun meeting with P2P developers to discuss the possible legal challenges they may face. We have suggested methods for limiting legal liability, and we are preparing to defend them if the need should arise.

Representing the Rights of People

- EFF has a well-earned reputation among "netizens" for being the premier source of information about freedom in cyberspace. For over 11 years, EFF has been providing legal counsel and assistance to users of new technologies who get caught on the front line where technology and law collide.
- EFF sponsors legal cases intended to protect users' online civil liberties. Four of the most important electronic communications cases of the last decade are EFF cases: *Steve Jackson Games v. U.S. Secret Service* (email privacy), *Bernstein v. U.S. Department of Justice* (export controls on encryption), *Universal City Studios, Inc. v. Reimerdes* (expansion of copyright law), and *Felten v. RIAA* (copyright fair use). In addition, we were plaintiffs and part of the legal teams of both *ACLU v. Reno* and *ACLU v. Ashcroft*, the cases that challenge the Communications Decency Act (CDA) and Child Online Protection Act (COPA), and currently participate on the legal team for *American Library Association v. United States of America*, challenging the Children's Internet Protection Act (CHIPA).
- EFF submits amicus briefs for cases that concern our issues and which are of major importance to modern communications. We have weighed in on *Religious Technology Center v. Henson* (free speech), *Intel v. Hamidi* (sending email as trespassing), *U.S. v. Thomas* (jurisdiction), and *U.S. v. Morris* (computer trespass) among others.
- EFF supports innovations in technology that protect and enhance civil liberties. EFF built an encryption-cracking machine that proved once and for all that the government's Data Encryption Standard (DES) is woefully insecure, despite NSA testimony to the contrary.

- EFF maintains a pro bono database of legal counsel for cases that raise issues of online freedoms, and we act as a referral service for people requesting legal assistance.
- EFF produces analyses to educate government policymakers and the public about the civil liberties implications of their actions and decisions. We have advised the Federal Trade Commission (FTC) on consumer privacy rights, the Sentencing Commission on intellectual property, the Child Online Protection Act (COPA) Commission and the National Research Council (NRC) on online censorship, and the National Science Foundation (NSF) and the Federal Communications Commission (FCC) on encryption, to name a few.
- EFF monitors legislation and agency actions affecting the online community, working with EFF members and other organizations on global, national, state and local levels to affect positive change in technology policy.
- EFF provides a free telephone and email hotline for members of the online community who have questions regarding their legal rights.
- EFF speaks to reporters, federal agencies, law enforcement organizations, state attorney bar associations, conferences, summits, and university classes on the work that we do and how these groups can become more informed and more positively involved in the progress of the digital age.
- EFF maintains one of the most linked-to websites on the Internet: www.eff.org is home to an extensive archive of information related to free speech, privacy and civil liberties in the world of high technology.

Helping Others Know Their Rights

EFF is committed to protecting users of new technologies. We see ourselves as being part of this community, and we believe it is our responsibility to be good electronic citizens.

Working With Other Groups

EFF is a member of many organizations working to protect rights in the digital age, including the Internet Free Expression Alliance (IFEA), the Global Internet Liberty Campaign (GILC), the Digital Future Coalition (DFC), and the Free Expression Network (FEN). In addition, EFF tries to help local organizations throughout the world working on our issues. EFF also works with other groups sharing our concerns about civil liberties, such as the American Civil Liberties Union (ACLU), the Electronic Privacy Information Center (EPIC), Public Citizen, the Online Policy Group (OPG), and the Privacy Rights Clearinghouse (PRC).

Bay Area EFF (BayFF)

EFF presents monthly meetings to address important issues where technology and policy collide. These San Francisco Bay Area meetings, entitled, "BayFF," serve as a community forum, helping us to bring our work to those around us in a creative and personal way. BayFFs are also webcast in order to be available to the greater community.

EFFector

EFF's biweekly electronic newsletter, EFFector, keeps readers informed of issues that are important to Internet users and tells them how they can participate. EFFector has been in publication for over a decade and has over 27,000 subscribers.

Blue Ribbon Campaign:

EFF created, sponsored and promotes the international grassroots Blue Ribbon Campaign opposing online censorship and protecting the essential human right of free speech embodied in the U.S. Bill of Rights and the United Nations Declaration of Human Rights.

Campaign for Audiovisual Free Expression (CAFE):

CAFE is EFF's participatory project to thwart recording and movie industry attempts to seize control over MP3, DVD and other emerging digital media formats. CAFE engages and educates people on these issues. Through CAFE, we inform artists and others of their rights regarding electronic publication and copying. We are also in the process of creating a library of "open art licenses" that artists can use to authorize distribution of their works online.

Brown Bag Lunches:

EFF staff members take their expertise on the road by providing brown bag lunch speakers to local businesses, universities and civic organizations. Brown bag lunches give EFF staff members an opportunity to speak with members of the community and to inform them about areas in which we are working. This helps to garner support for our work. In addition, this provides a lively forum for hearing new ideas and topics that deserve our attention.

Cooperative Computing Awards:

EFF sponsors cooperative computing awards, with an endowment of over half a million dollars in prize money, to encourage ordinary Internet users to contribute to solving huge scientific problems. EFF award prizes to the first individuals or groups that discover new prime numbers. EFF hopes to spur the technology of cooperative networking and encourage Internet users worldwide to join together in solving scientific problems involving massive computation.

EFF was created to protect freedom in an increasingly digital world, and we have spent more than a decade fighting off threats to our rights. We cannot give up this fight. The cost to our humanity is too great.


Join with us. As a donor-supported, nonprofit membership organization, EFF needs your help. Your generous gift can help us guarantee the best world we can imagine.

Contact Us:

EXHIBIT G
PAGE 58

Electronic Frontier Foundation
454 Shotwell Street
San Francisco, CA 94110
Phone: 415/436-9333 Fax: 415/436-9993
Website: <http://www.eff.org> / Email: eff@eff.org

[Staff/Board List](#)

Search:  [Site Map](#) [Most Popular EFF Pages Today](#)

Please send any questions or comments to webmaster@eff.org.

EXHIBIT H



Electronic Frontier Foundation

[EFF Home](#)

[Action Home](#) [Login](#) [Subscribe](#) [Help](#) [Legislative Directory](#) [Tell A Friend](#) [F](#)

[Join EFF/Donate!](#)

[About EFF](#)

[Free Speech Online](#)

[Audiovisual Freedom](#)

[Online Privacy](#)

[Active Legal Cases](#)

[Recent News](#)

[EFF Blogs](#)

[EFF Newsletter](#)

[Internships & Jobs](#)

[EFF Topics](#)

[Radio EFF](#)

[Contact Us](#)

[Calendar](#)

[Media Resources](#)

[EFF Privacy Policy](#)

TAKE ACTION! SEND A MESSAGE

Tell Your Legislators to Repeal CIPA's Internet Blocking Provisions



The Children's Internet Protection Act of 2000 (CIPA) requires all public schools and libraries receiving certain federal funds or discounts to install controversial Internet blocking or "filtering" software. This software is supposed to prevent

children from viewing material considered "harmful to minors." Unfortunately, no filter can identify these illegal materials or distinguish them from valuable web content of all kinds. Use your voice to protect students' right to learn on the Internet!

[Learn More About This Issue](#)

1 Read the Letter

September 20, 2002

Your U.S. representative

Your U.S. senators

Dear Congressperson,

I am writing to urge repeal of the Children's Internet Protection Act of 2000 (CIPA).

As a result of this law, public schools that can't afford to risk loss of federal funding or discounts are forced to install ineffective Internet filtering software.

While I understand that filtering software is supposed to censor online pornography, the filters are not effective in blocking target websites while at the same time mistakenly censoring many websites that provide important educational opportunities for students. Because of filtering software, students have found it impossible to research a number of assignment topics, including those dealing with controversial issues like mental illnesses, sexually transmitted diseases, sexual orientation, drug use, suicide, pregnancy, and other important issues. Even more alarming, filters often block sites that contain nothing remotely controversial, like a punctuation primer, Dr. Pace's Chopin performance techniques, and the Archie Dykes Medical Library, among hundreds of thousands of other examples.

Furthermore, manufacturers design and maintain filtering software that cannot take into account the educational standards and goals of diverse local communities. I think that taking fundamental

- [To D](#)
- [Acti](#)
- [Tell Rep Bloc](#)
- [Tell to Fi Man NY](#)
- [Tell to Fi Man MA](#)
- [Tell to Fi Man CA](#)
- [Tell to Fi Man NC](#)
- [Cop Wan](#)
- [Con Your](#)
- [Publi USA](#)
- [Tins Stop](#)
- [Me](#)
- [Emai](#)
-
- [Pass](#)
-
-
- [Subs](#)

Cent
Ben

questions about how students learn out of the hands of people in the community is a poor policy choice. A community ought to have the right to decide how best to educate its children.

The purpose of the Internet is to make information readily available to all citizens, and our public schools ought to be a place where that information is accessible. Instead, these filters create a digital divide. While wealthier students can simply do their research at home when filtering gets too frustrating, students with more limited resources are left at a discriminatory disadvantage.

Instead of resorting to censorship tactics like filters, teachers should educate students about the Internet and show them how to use it safely through media literacy programs. As the National Research Council of the National Academy of Sciences noted in its May 2002 study "Youth, Pornography, and the Internet," this would give students the critical thinking skills necessary to navigate the World Wide Web and understand the wide array of conflicting images they can find there.

CIPA forces local schools into a no-win situation with a loss of funding on one side and damage to students' ability to learn on the other.

As you may know, the public library filtering provisions of CIPA have already been found unconstitutional by a federal court of appeals in Philadelphia. I urge you to follow their sentiment and vote to repeal CIPA's filtering provisions for public schools.

Thank you for taking the time to read this. I hope you will take action and help protect the educational potential of the Internet for our students.

Sincerely,

Your signature will be added from the information you provide below.

To be able to modify the following letter:

- » [Subscribe to the EFF Action Center](#)
- » [Log in to your Personal Action Center](#)
- [Need some advice on how to edit?](#)

2 Sign the Letter

Already a member? All you need to enter is your email address and send the letter. If not, all fields are required.

Please use your physical address. P.O. Boxes do not have Congressional districts associated with them and cannot be used with our Congressional lookup service.

Email

Prefix

First Name

Last Name

Address

City
State
Zip Code
Country/Other

YES! I want to subscribe to the **EFF Action Network!**

Send an Email Send a Fax

③ Send the Letter



Comments on this page? Problems? [Click here](#) to send us feedback

EXHIBIT I

***Final Report of the Co-Chairs of the
Broadcast Protection Discussion Subgroup
to the Copy Protection Technical Working Group***

June 3, 2002

***Robert Perry
Mitsubishi Digital Electronics America***

***Michael Ripley
Intel Corporation***

***Andrew Setos
Fox Group / Fox Technology Group***

BPDG: FINAL REPORT TO CPTWG

0. Introduction

0.1 This report is presented by the co-chairs of the Broadcast Protection Discussion Group (“BPDG”) to the Copy Protection Technical Working Group (“CPTWG”), to summarize the work and conclusions of the BPDG in evaluating technical solutions for preventing unauthorized redistribution (including unauthorized redistribution over the Internet) of unencrypted digital terrestrial broadcast television (referred to hereinafter as “DTV”).

0.2 As detailed in sections 1-3 of this Report, this effort has focused primarily upon the evaluation of a particular proposed technical solution using a “broadcast flag,” and the creation of compliance and robustness requirements that would effectuate this solution when implemented in consumer products. This proposed solution, and the work undertaken by the BPDG, was intended only to address means by which DTV content could be protected against unauthorized redistribution, while minimizing the burden on implementers and, for some participants, avoiding unnecessary interference with other content protection technologies. Other than necessarily requiring that DTV content continue to be protected against unauthorized redistribution when copied or output in digital form, the proposed technical solution does not interfere with the ability of consumers to both make copies of DTV content, and to exchange such content among devices connected within a digital home network.

0.3 Many of the provisions of the Compliance and Robustness Requirements document attached to this Report reflect fundamental points of agreement among participants. The points of agreement are summarized in section 4.

0.4 The BPDG did not reach complete agreement on all necessary elements of the Compliance and Robustness Requirements, however, due to principled differences of view among the participants (and, in certain cases, because of time constraints). The points as to which general agreement was not reached are discussed in section 5.

0.5 A number of questions raised in the course of the BPDG discussions related to enforcement and related policy issues. There was general agreement that such questions, while highly pertinent to any decisions as to how a broadcast protection method should be implemented, are not appropriately addressed by the BPDG. Anticipating that this would be the case, the BPDG Work Plan (described below) recommended establishment of a parallel group. Section 6 of the Report suggests a number of significant issues that could be discussed and considered by such parallel group.

1. Background

1.1 Work undertaken by the CPTWG beginning in 1996 focused primarily upon means for content owners to protect physical media distributed to the public in encrypted form, and means by which consumer electronics and computing devices could perpetuate protections applied to encrypted content delivered to the consumer by such physical media and by cable and satellite transmission. Under current FCC regulations, most digital terrestrial television broadcasts are delivered in unencrypted form (“in the clear”). Thus, unlike prerecorded encrypted digital media such as DVD, or premium digital cable and satellite video transmissions delivered via conditional access, there may not be any licensing predicate to establish conditions for the secure handling of such content. Consequently, consumer products can be legally made and sold that allow this unprotected DTV content to be redistributed (including via unauthorized redistribution over the Internet) without authorization from the copyright holders.

1.2 In the course of negotiations between major motion picture studios and the Digital Transmission Licensing Administrator LLC (“DTLA”), relating to the licensing of DTLA’s “DTCP” technology for protecting encrypted conditional access digital video content within local digital network environments, the studios requested that the DTCP license also require licensed products to apply DTCP to protect DTV. Although the DTLA stated that it could not impose such requirements through the DTCP license, the DTLA companies stated that they would be willing to contribute their efforts to a multi-industry effort to develop solutions for protecting DTV against unauthorized redistribution.

1.3 In May 2001, an Advanced Television Standards Committee (“ATSC”) subcommittee began consideration of a proposal from Fox Broadcasting (News Corporation) to define in the ATSC technical standards for DTV a “Redistribution Control” descriptor. This Redistribution Control descriptor proposal was accepted, by ballot of the ATSC members, as part of the ATSC Standard as of April 2, 2002.

1.4 Also in May 2001, Fox developed and presented to the member companies of DTLA a technical proposal whereby this Redistribution Control descriptor, when detected in ATSC transport streams, could be used to signal protection of broadcast audiovisual content against unauthorized redistribution (including unauthorized Internet redistribution).

1.5 By a joint letter dated November 26, 2001, the Consumer Electronics Association and Information Technology Industry Council invited the Motion Picture Association of America and its member companies to join in a request to the CPTWG to form a group to explore a technical solution to the unauthorized redistribution of DTV content over the Internet. Following an exchange of letters, the three trade associations agreed to support such a collaborative effort under the aegis of the CPTWG.

1.6 On November 28, 2001, representatives of the five member companies of DTLA – Intel Corporation, Hitachi Ltd., Matsushita Electric Industrial Co. Ltd., Sony Corporation and Toshiba Corporation (collectively also referred to as the “5C” companies) – described in a presentation to the CPTWG a refined version of the Fox technical proposal using the ATSC Redistribution Control descriptor as a “Broadcast Flag” (and possibly a “consensus watermark” as a “Broadcast Watermark”) to signal protection for DTV content against such unauthorized redistribution. A

copy of the presentation, entitled "Protecting Against Unauthorized Redistribution of Digital Broadcast Content" is attached to this report at Tab A.¹ The presentation suggested that DTV content be protected beginning at the point of demodulation of the ATSC stream, so as to assure that DTV content in usable form would be securely routed to ATSC transport stream processors that would read the Broadcast Flag (or, at the election of the implementer, screen for the "Broadcast Watermark").² If the flag (or watermark) were determined by the ATSC transport stream processor to be present, then the DTV content would be securely delivered to protected digital output and recording technologies. If the flag (or watermark) were determined by the ATSC transport stream processors not to be present, then no further protection need be applied to the DTV content. The presentation outlined possible requirements for compliant devices, and rules to ensure robust implementation of the suggested protection system.³

1.6 The five companies recommended that a group be formed, including representatives from all industries that would potentially be affected by the proposal, for the purpose of evaluating the suitability of this technical proposal for protecting DTV content and determining whether there was substantial industry support for the proposal as a solution to the redistribution problem.

¹ The presentation is available from the CPTWG website at <http://www.cptwg.org/Assets/TEXT%20FILES/ProtectingWDC9911-01.PPT>.

² The presenters proposed leaving this decision to the implementer such that products that included watermark detection for other purposes might leverage this capability, but stated that their preference was to make the broadcast flag implementation sufficiently robust so that watermark detection (which would likely be more expensive and burdensome than flag detection) should remain optional.

³ It was suggested that a more effectual technical and enforcement solution would be to encrypt DTV content at the source (*i.e.*, the transmitter). Given the current political and business environment, this approach was rejected by motion picture studios and broadcasters, as well as by representatives of consumer electronics manufacturers, in favor of the approach reflected in the presentation.

2. The Work of the BPDG

2.1 In a meeting the afternoon of November 28, 2001, approximately 70 representatives of the consumer electronics, information technology, motion picture, cable and broadcast industries agreed to form the Broadcast Protection Discussion Group. License Management International LLC established an email reflector to promote discussions of any technical issues.⁴

2.2 A proposed Work Plan for the BPDG was drafted and circulated to BPDG, which stated the BPDG's Charter, in pertinent part, to be as follows:

“to evaluate proposed solutions for (a) the secure signaling of protection for unencrypted digital terrestrial broadcast content against unauthorized redistribution outside of the personal digital network environment (*e.g.*, the home or the automobile)⁵, and (b) the secure handling of such content by products when such signaling has been applied.”

This proposal was discussed by the BPDG participants during a conference call on December 18, 2001. A copy of the Work Plan is attached to this Report at Tab B.⁶

2.3 The Work Plan proposed that co-chairs for the group be selected from multiple affected industries. Accordingly, during the December 18, 2001, conference call, co-chairs from the consumer electronics, information technology and motion picture industries were nominated, and approved without objection.

2.4 On January 15, 2002, the co-chairs of the CPTWG reviewed the statement of charter in the Work Plan and approved the BPDG as a working group under the aegis of the CPTWG.

⁴ As of the date of this Final Report, more than 230 individuals (representing more than 70 consumer electronics, information technology, motion picture, broadcast, cable and satellite companies and associations, had subscribed to the bpdg-tech reflector. While originally conceived as a multi-industry forum comprised of representatives of affected industries, as such list indicates, BPDG participation was in fact open to any group or individual wishing to participate, with one exception. In keeping with longstanding policy and practice of the CPTWG, there was general agreement to exclude journalists in their capacity as such from BPDG meetings and conference calls because it was felt that such participation would have a "chilling effect" on the discussions. However, each BPDG participant was left wholly free to speak to journalists outside of BPDG proceedings. Several BPDG participants objected to this exclusion on public policy grounds, but others responded that public policy was not involved, since the BPDG is a wholly private discussion group with no official or unofficial governmental standing.

⁵ See section 5.1 with respect to disagreements regarding the appropriateness and meaning of the phrase "outside of the personal digital network environment (*e.g.*, the home or the automobile)."

⁶ The BPDG Work Plan suggested that a "parallel group" be constituted, outside of BPDG, to address means by which any Compliance and Robustness Requirements applicable to the Broadcast Flag solution could be implemented and enforced, and policy issues relating thereto. This parallel group has been established and has held several meetings. A separate email reflector for this parallel group also has been established, and can be joined by sending an email message to reflector@lmicp.com, and including in the body of the message the sender's name and a request to subscribe to the "policyg list". As of the date of this report, more than 135 individuals (representing more than 50 companies and associations) have subscribed to this reflector.

2.5 Certain participants have noted that while the Broadcast Flag proposal addressed protection in the digital domain beginning at the point of demodulation, it did not address the "analog hole," whereby unprotected video in analog form can be converted by consumers to digital form without the protection originally applied to the digital content (the comments of one company, Digimarc, in this regard are attached to this Report at Tab O). Participants have generally recognized that because this issue applies to a range of content far broader than DTV, the BPDG would not be an appropriate forum in which to address it.

2.6 Certain participants opposed the premise on which the BPDG was formed, expressing the view that no technological restrictions on the handling of broadcast signals should be imposed. Comments from those parties are attached at Tab N.

2.7 The Work Plan proposed March 31, 2002, as a target for completing an evaluation of the Broadcast Flag proposal. The target was substantially met with respect to the fundamental elements of the broadcast flag proposal. Notwithstanding, due to the complexity of certain issues raised by BPDG participants, the target was extended such that the work of the BPDG would be completed prior to the June 5, 2002, meeting of the CPTWG.

2.8 The BPDG held 16 meetings as follows:

- 2.8.1 November 28, 2001 organizational meeting in Los Angeles
- 2.8.2 December 18, 2001 teleconference
- 2.8.3 January 15, 2002 meeting in Los Angeles
- 2.8.4 January 24, 2002 teleconference
- 2.8.5 February 7, 2002 teleconference
- 2.8.6 February 21, 2002 teleconference
- 2.8.7 February 27, 2002 meeting in Los Angeles
- 2.8.8 March 14, 2002 teleconference
- 2.8.9 March 21, 2002 meeting in Los Angeles
- 2.8.10 March 27, 2002 teleconference
- 2.8.11 April 1, 2002 teleconference
- 2.8.12 April 3, 2002 meeting in Los Angeles
- 2.8.13 April 15, 2002 teleconference
- 2.8.14 April 17, 2002 meeting in Los Angeles
- 2.8.15 April 29, 2002 meeting in Los Angeles
- 2.8.16 May 23, 2002 teleconference

2.9 The Co-Chairs recognize that the work of the BPDG has been undertaken in a compressed timeframe, reflecting the concern of content providers over the harmful effects of allowing continued broadcast of DTV without protection against unauthorized redistribution, the concern of certain members of Congress that the transition to DTV has stalled and the assertion by certain content providers that broadcast protections would contribute to the more timely deployment of high value content over DTV. Although general agreement was rapidly reached in support of fundamental elements of the proposal, addressing many of the detailed aspects of implementing the proposal proved to be more challenging and, therefore, time-consuming. Consequently, it has been difficult for those making technical and drafting proposals to unflinchingly meet the targeted dates for distribution of such proposals, so as to give all participants

ample advance opportunity to fully consider the proposals to be discussed. We recognize that this process at times has been imperfect; and that, with more time or additional resources, perhaps we could have enhanced the timing and operation of the project. Nevertheless, the Co-Chairs commend all parties for their good faith efforts to work within the bounds of this expedited process, and believe that the process ultimately has given all participants a fair opportunity to express their views through the reflector, in telephone conferences and in meetings.

2.10 The Co-Chairs wish to express their deep appreciation to the many parties who participated in the BPDG process and who have extended truly extraordinary efforts to support the rapid conclusion of this project. It is indeed noteworthy that so many people invested a great deal of time, resources and energy in these proceedings. The companies and interested parties involved in the BPDG have gained a deeper understanding of the needs that different industries and consumers have in addressing the issue of protecting over-the-air DTV from unauthorized redistribution. The Co-Chairs believe that participants have acted in good faith to understand the issues raised by others, as well as to advance their own perspectives and interests. Despite these efforts, and in part given the constrained deadlines as noted in section 2.9, the BPDG process had certain inherent limitations, and this report necessarily reflects those limits.

2.10.1 First, as its name implies, the BPDG is a discussion group. It is not a standards body or public policy decision-making forum. Individuals, companies, and groups of companies were free to meet separately to form and negotiate proposals and present those to the full BPDG. This may have given the unintended appearance that BPDG was not fully transparent and some parties may have felt "excluded" from particular discussions. Nevertheless, every proposal contained in the Requirements document and described in this report was subject to considered discussion and scrutiny by all BPDG participants in meetings, on teleconferences, and/or on the email reflector scrutiny.

2.10.2 Second, the purpose of the BPDG was not to develop complete consensus. Rather, as noted in Section 2.2 above, it was to evaluate proposed solutions to the stated problem. Where BPDG participants offered substantial support for a proposal, we have so indicated. Where substantial differences remained, they are so noted.

2.10.3 Third, the discussions have been important to advance understanding, but they have not resolved all of the critical technical, enforcement, and policy issues. In particular the list of enforcement and policy issues to be handled by the parallel group is significant and as substantial as the issues addressed herein.

Consequently, the Co-Chairs suggest that the value of this report lies less in reaching particular "conclusions" than in describing the important discussions of the group, and in finding the many points of agreement as well as explaining the substantial points of disagreement.

2.11 In preparing this Report, the Co-Chairs have sought input from all participants, and have received several sets of comments. The Co-Chairs have endeavored to fairly summarize and reasonably reflect all comments in this Report. In doing so, the Co-Chairs have given particular deference to suggested changes concerning participants' characterization of their own

statements. In the interests of brevity, the Co-Chairs have not reflected all comments verbatim, and have tried to avoid making repetitive references to the same or similar points in numerous sections of the Report. Moreover, the Co-Chairs have not endeavored to set forth in detail the comments of certain participants that have opposed the premise on which the BPDG was formed (see section 2.6 above). Because no summary report can thoroughly convey all comments received, all submitted comments are attached hereto at Tab P.

2.12 Individual Comments of the Consumer Electronics Industry Co-Chair:

The CE industry supports the concept of a narrowly focused process to protect copyright asserted digital television broadcasts from distribution on the Internet. Although many CE companies support most of the provisions in the final draft Compliance and Robustness Requirements, there is no full consensus within the CE industry supporting this current process. This lack of full consensus is due to the following concerns by a number of CE companies:

2.12.1 Some CE companies are concerned that while the initially understood goal was to protect retransmission of content over the internet, the actual document is less than clear in specifically narrowing this protection to the public network known as the Internet, and that while exclusions have been made for home and personal networks, these limits are not clear.

2.12.2 Some CE companies are concerned that there is no affirmative recognition of the CE industry's historical and unwavering support of "fair use" consumer rights with regard to the personal, non-commercial use of legally obtained content.

2.12.3 Some CE companies are concerned that the process, in recognition of the desired timeline, did not use the normal standards processes (such as dispute resolution, voting, procedural rules, etc) in it's work efforts, and therefore did not benefit from the complete participation of all parties in a structured manner.

2.12.4 Some CE companies are concerned that the process of having technologies "approved" for inclusion to accomplish the protection goal is not objective, and may be used as a competitive weapon or barrier to entry.

2.12.5 Some CE companies are concerned that this process will negatively impact the ability to build DVD recorders for digital television that would be backward compatible with the 30 million or so existing players in consumers homes.

2.12.6 Some CE companies are concerned that this work product contains accommodations and structures that are designed to allow for future protection systems such as watermarking. Because no watermarking proposals for DTV have been discussed, nor the surrounding issues, these companies are uncomfortable in accepting any framework for such systems until all the issues are known.

2.12.7 Some CE companies are concerned that while there appears to be oral agreement among the parties about the use of VSB modulators, it is not yet understood whether the wording in the document accurately reflects such agreement and requires more lengthy review, and that specifically, consumers should be able to send unrestricted content (such as camcorder outputs)

as well as unscreened and properly screened content (such as free over-the-air TV programming) to other devices in their home using VSB modulation.

3. The Work Product of the BPDG

3.1 The BPDG recognized the need for requirements defining how compliant systems should implement the proposal on an architectural level, and how the implementation of such systems could be made robust against consumer hacking. The Work Plan proposed that a small task force be created to begin drafting "strawman" compliance and robustness requirements. Accordingly, during the December 18, 2001, conference call, volunteers were requested for such a task force. In response, a number of participants who had experience in drafting analogous documents for digital protection technologies already in the marketplace volunteered, during the call and subsequently by e-mail to the Co-Chairs, to form a small drafting task force to prepare, for discussion by the BPDG, a draft of such Compliance and Robustness Requirements. Those who volunteered for and participated in this drafting group included representatives from the Computer Industry Group, Fox, Hitachi, Intel, MPAA, Sony, Sony Pictures, Viacom and Warner Brothers.

3.2 On February 15, 2002, this drafting group circulated to the BPDG a first "strawman" draft of the Compliance and Robustness Requirements.

3.3 The Compliance and Robustness Requirements document has been the subject of discussion during 10 meetings and conference calls, and additional comments concerning the document were circulated on the BPDG-tech email reflector. Based upon discussion and comment by the BPDG participants, the Compliance and Robustness Requirements has undergone five complete draft revisions.

3.4 The first three drafts were prepared by the drafting group, reflecting numerous comments received from BPDG participants. The fourth draft was proposed for comment by a group representing companies of the MPAA, 5C and Computer Industry Group. (This fourth draft was part of a proposal that included criteria by which technologies might be approved for protection of digital output transmissions and digital recordings of DTV content. This and another proposal from Philips for such criteria are described below in section 6.)

3.5 The "final" draft of the Compliance and Robustness Requirements document, attached at Tab C, is the primary work product of the BPDG. Although the BPDG has no voting rules or other formal means by which to determine the extent of agreement, it is nevertheless the considered view of the Co-Chairs that the draft reflects substantial agreement among the BPDG participants as to most provisions. A number of significant comments concerning the draft were not resolved by the BPDG participants. These comments are reflected in brackets in the Compliance and Robustness Requirements document, and are explained below in section 5 of this Report.

3.6 The initial draft of the Compliance and Robustness Requirements included, for frame of reference, two alternative proposals for section X.2, each of which described which devices would be required to comply with the Compliance and Robustness Requirements prior to being sold or distributed. The two different proposals for section X.2 were submitted respectively by certain Motion Picture Association of America member company representatives, attached at Tab D, and by representatives of member companies of DTLA and Computer Industry Group, attached at Tab E. The BPDG briefly reviewed these documents for purposes of understanding

the proposed methods of assuring implementation of the proposed Compliance and Robustness Requirements, but it was understood that any proposals for section X.2 would receive further discussion and appropriate consideration by the parallel group.⁷

⁷ Some participants expressed concern that drafting of Compliance and Robustness Requirements could not be meaningfully completed until the parties determined under what circumstances its provisions apply (i.e., until section X.2 was completed and agreed upon).

4. Summary of Conclusions

The discussions to date have yielded substantial agreement among the BPDG participants concerning the use of the ATSC RC descriptor to signal protection for DTV content, and many of the requirements to be imposed upon certain products that handle DTV content that is to be protected.⁸ These fundamental points of agreement among the BPDG are set forth in the final draft Compliance and Robustness Requirements, and are summarized below:

4.1 An approach based on a "broadcast flag" is technically sufficient for the purpose of signaling protection of DTV content in digital form, beginning at the point of demodulation, against unauthorized redistribution.⁹

4.2 The specific "Broadcast Flag" to be used for this purpose is the Redistribution Control descriptor set forth in ATSC Standard A/65A: Program and System Information Protocol for Terrestrial Broadcast and Cable, 31 May 2000, Amendment 3, 6 February 2002.

4.3 Protection requirements should begin at the point of demodulation of the incoming 8-VSB, 16-VSB, 64-QAM or 256-QAM (collectively "n-VSB" or "m-QAM") modulated DTV signal that thereby produces a data stream consistent with ATSC Standard A/53 Annex C¹⁰ (e.g., in demodulation software or a demodulation chip).

4.4 A product covered by the Compliance and Robustness Requirements must handle demodulated content in a protected manner unless/until the product screens for the Broadcast Flag and determines that it is not present.

4.5 Where the demodulated DTV content has been screened and the Broadcast Flag has been determined not to be present, no further requirements or limitations should be imposed upon the handling or recording of such unmarked content.

4.6 Unscreened Content and Marked Content should be recorded by or output from covered products via only the following permitted methods:

- a. Analog outputs and recording methods;
- b. n-VSB and m-QAM modulators (subject to refinement of conditions);

⁸ As noted above in footnote 6, a parallel group has been constituted to address means by which any Compliance and Robustness Requirements applicable to the Broadcast Flag solution could be implemented and enforced. Any points of agreement reflected in this Report, or in draft Compliance and Robustness Requirements, should be understood as being addressed only to anticipated possible governmental action.

⁹ While certain participants have suggested consideration of additional technologies, such as a "broadcast watermark," to perform this particular signaling function in a second phase implementation, there is no current plan for such a second phase as there is not a broadly held view that it is necessary. The suggestions of one company, Digimarc, in this regard are attached at Tab O.

¹⁰ These requirements would need to be supplemented or amended if, in the future, new modulation standards replace those listed.

- c. Unprotected DVI outputs (at limited resolution); and
- d. Digital outputs and recording methods that provide specified levels of protection against unauthorized redistribution.

4.7 The requirements to protect digital recordings should not interfere with the ability of consumers to make secure copies of DTV content marked with the Broadcast Flag, either on personal video recorders (*e.g.*, a hard-disk based device such as TiVo or ReplayTV) or on removable media (*e.g.*, on D-VHS tapes or DVD recordable discs). Similarly, the requirements to protect digital outputs should not interfere with the ability of consumers to send DTV content across secure [home and personal digital networks]¹¹, such as a home digital network connecting digital set top boxes, digital recorders, digital servers and digital display devices.¹²

4.8 Unscreened and marked content should be protected when passed in digital compressed form across a user accessible bus within a device.

4.9 General agreement has been reached as to the specific robustness requirements to be implemented by covered products.

4.10 For digital cable distribution of DTV, the requirements can be implemented in cable systems utilizing a "POD" module by one method whereby the DTV content is delivered in encrypted form and passed through the POD module, or by another method whereby the content is delivered in-the-clear and does not pass through the POD module. It was to address the latter method, and thereby provide for protection in homes with cable-ready digital television sets that do not require POD modules, that 64-QAM and 256-QAM modulation were added as modulation schemes to which protection requirements would attach.

4.11 Satellite and cable services can encrypt DTV signal retransmissions, so may not need to implement a Broadcast Flag-based solution. However, the parallel group should discuss any requirements necessary to ensure that such content is protected when retransmitted in encrypted form.

4.12 Both proposals for section X.2 of the Compliance and Robustness Requirements anticipate that an appropriate provision will be crafted so as to exempt the requirements from

¹¹ See section 5.1 with respect to the bracketed phrase.

¹² One BPDG participant asked that "unauthorized redistribution" should be agreed not to include any redistribution that would be deemed "fair use" of content that a consumer legitimately acquires. Several BPDG participants observed that although the requirements would not impinge upon the making of time-shift recordings, current content protection technologies inevitably cannot accommodate all instances where redistribution of DTV content (*e.g.*, the retransmission of program clips for educational purposes) might be fair use. Other participants noted that the Broadcast Flag would not prevent consumer copying, that the application of "fair use" depends upon detailed analysis of the concrete facts of a particular case, and that in any event debate or comment on application of fair use principles was outside the scope of the BPDG. Some other participants noted that, although fair use purposes might be met today by digitally recording the analog output from a player or recorder, it was their hope and expectation that future, more sophisticated systems that implement broadcast protection may better accommodate such fair uses.

applying to products that are specifically intended for professional and broadcast use (e.g., equipment used by studios, TV broadcasters, satellite and cable operators).

5. Summary of Points as to which General Agreement was Not Reached

In the course of the discussions of the Compliance and Robustness Requirements, general agreement was not reached on a number of significant points, as to which various participants voiced specific disagreements. The Co-Chairs believe that additional time would not be likely to produce significant further agreement on most of these points. These points include:

5.1 The scope of protection to be accorded to DTV content has been described in the BPDG meetings and documents in various ways, such as, "protection against unauthorized redistribution (including the Internet)," or "unauthorized redistribution outside the home or personal digital network environment," or outside the "home or other similar local environment," and so forth¹³. Notwithstanding, all statements of the scope of the BPDG project have included redistribution over the Internet as an example of such protection. Some participants contend that the scope of protection should be limited simply to unauthorized redistribution over the Internet. Others suggest that the parallel group consider a more precise definition of the contours of such protection, so as to clarify that the protection would limit redistribution of DTV to "personal" environments, which they described as including the home, automobile, personal portable devices, and communications between primary and secondary residences.

5.2 The draft Robustness Requirements proposes, consistent with analogous requirements for certain protection technologies already in the marketplace, to set certain levels of robustness according to the type of tools that would be required to circumvent the protection. Some BPDG participants maintain that certain Robustness Requirements should instead be based on a defined level of technical skill, such as that of an ordinary consumer, so that unreasonably stringent requirements (e.g., preventing successful hacks by even the most knowledgeable professional technicians) are not imposed on device manufacturers. The MPAA member companies have maintained that an approach based on a defined level of skill would be inconsistent with the structure of the Robustness Requirements, stating by way of example that the requirements should not permit a professional to defeat protection with a screwdriver.

5.3 The draft Compliance Requirements would permit computer products to continue to deliver protected DTV content through unprotected DVI outputs, at MPEG-2 main profile @ main level video quality. This provision is designed to accommodate legacy computer monitors that receive content only through DVI. Some participants have suggested that this capability also should apply to consumer electronics products, inasmuch as some manufacturers might wish to market devices, such as cable or satellite set-top boxes, that would be capable of delivering DTV to such legacy computer monitors, and inasmuch as they believe it is generally not sound policy to discriminate among the products of the converging CE and IT industries. The MPAA member companies have stated that the provision is narrowly tailored to address a relatively small number of currently existing legacy displays, and have maintained that there is no material

¹³ The phrase "home or other similar local environment" is used specifically in relation to the output of DTV content using a self-certified "Robust Method", and some participants have requested that it be changed to "home or personal digital network environment" consistent with wording used elsewhere, whereas the MPAA member companies have maintained that "personal digital network" is unduly broad, especially in this context.

benefit to expanding the provision in such a manner, and that there may be substantial harm in doing so.

5.4 The draft Compliance Requirements would permit the use of a self-certified "Robust Method" for outputs only where the DTV content was unaltered Unscreened Content (e.g., Unscreened Content that had not yet been transport stream processed). Some participants have requested such an output be permitted for Marked Content as well, noting concern that without it, the development of innovative content protection systems for home networks, and rapid deployment of same, would be significantly affected. The MPAA member companies have maintained that Marked Content, having been subject to transport stream processing, is particularly susceptible to unauthorized redistribution and should therefore be subject to the more rigorously and clearly identified protections provided by "authorized" protection technologies, citing benefits to both manufacturers and consumers arising from the certainty and resulting increased access to attractive digital broadcast content that would be afforded by this approach.

5.5 The draft Robustness Requirements include the requirement, included in similar content protection technology agreements, that Covered Products "shall be manufactured in a manner clearly designed to effectively frustrate" attempts to modify such Covered Products to defeat the Compliance Requirements. A few participants have proposed that the word "effectively" be deleted, stating that it adds unnecessary ambiguity to the requirement and could be construed in an unintended fashion (e.g., as requiring foolproof design). The MPAA member companies maintain that deleting the word "effectively" would afford an insufficient level of protection, and would be inconsistent with the language and intent of the Robustness Requirements.

5.6 Philips submitted a presentation describing a potential method whereby unencrypted recordings of broadcast content could be protected by an alternative "flag preserving" mechanism. Protection in this scheme, as with the obligation to detect the Broadcast Flag, would derive from "compliance" rather than "self-protection." Technical and related policy questions and comments for and against the proposal were discussed at length in BPDG meetings and conference calls. Several favored the proposal because it would permit content recorded in unencrypted form on the DVD+RW format (and possibly other backwards-compatible DVD recording formats) to be played on certain legacy DVD players. The MPAA member companies have objected to the proposal, arguing that it would provide inadequate technical security, particularly with respect to legacy devices. There were other objections to the broader scope of legislation that would be necessary for purposes of enforcement (i.e., legislation that would regulate all DVD players, recorders, drives and interfaces). Others observed that this proposal benefited a particular DVD recording format, yet would impose technical and legal mandates upon DVD players and drives of all formats. In response to inquiries at two meetings, the BPDG participants voiced insufficient interest in further pursuing the proposal within the BPDG.

5.7 A proposal was later made by Philips and certain other consumer electronics companies that, for a limited number of years (intended to capture the reasonable life of legacy DVD players), in-the-clear recordings of Unscreened Content and Marked Content could be made using standard definition DVD recorders. This was consistent with assertions by these and some other participants that any technological protections should be applied only to HD content. Motion picture companies opposed such a "grandfather" provision, inter alia, because tens of

millions of legacy DVD-ROM drives would remain capable of unauthorized redistribution of such content when played back, including over the Internet.

5.8 A few participants suggested that the method for transmitting DTV content that is received from a trusted source and remodulated using an n-VSB modulator could be included on Table A. Those who supported this suggestion contended that as long as DTV content was freely available over the air, it made no sense to apply a higher degree of protection for DTV content circulating within the home, and that any technology that provided equivalent prevention of redistribution should be accepted for inclusion on Table A. Motion picture companies objected to this proposal on grounds that n-VSB remodulation is not a "protection" technology at all, and it was not appropriate to include on Table A technologies that were not protection technologies. Additionally, it was noted by others that the impact of this proposal would be to permit other non-protection technologies to be listed on Table A, under criteria proposed by companies of the Motion Picture Association of America, DTLA and Computer Industry Group (*see* section 6.6).

5.9 During early BPDG meetings certain participants expressed the view that an approach based on a "broadcast flag" for protecting DTV content must be designed so as to avoid negatively affecting other content protection systems. A specific concern noted was the possibility that such a flag-based system, in conjunction with consumer n-VSB and m-QAM modulators, might be misused to "launder" content taken from other protection systems. For example, motion picture content might be misused by being taken from a DVD-Video disc, converted into a transport stream, and passed through a consumer modulator such that a product compliant with the flag-based requirements would demodulate it and handle it as DTV content. Certain other BPDG participants expressed the view that such concerns related to other content protection systems or to non-DTV content were outside the scope of the BPDG. Pursuant to such concerns, the MPAA member companies proposed during an April BPDG meeting that consumer n-VSB and m-QAM modulators be required to block content that arrived from "non-trusted sources" and contained the Broadcast Flag from being modulated. On May 1, the MPAA member companies posted to the BPDG reflector an outline of such proposal, which described "trusted source" content as including content received via DTCP or other conditional access systems and described "non-trusted sources" as including unprotected analog-to-digital converters and unprotected digital inputs. On May 24 and May 29, Fox and the MPAA member companies, respectively, proposed language for Sections X.3(a)(2) and X.4(a)(2) of the Compliance and Robustness Requirements that would extend their earlier proposal so as to apply obligations on modulators with respect to all content other than Unscreened and Marked Content. A number of BPDG participants, while supporting the inclusion of n-VSB and m-QAM modulated outputs as permitted outputs under Sections X.3(a)(2) and X.4(a)(2), objected to the MPAA proposal that such sections also impose obligations on modulators with respect to content other than Unscreened and Marked Content. The basis for such objections were that (a) any obligations that might be imposed on consumer modulators with respect to non-broadcast content were not appropriate subject matter for Sections X.3(a) and X.4(a) (whose scope is limited to requirements imposed on Covered Products with respect to Unscreened and Marked Content); (b) if any obligations are imposed on modulators, they should not extend beyond the "non-trusted" unprotected analog or unprotected digital content originally proposed by the studios and (c) there had not been sufficient time for analysis and discussion of the proposal.

5.10 In mid-May, pursuant to the same concerns described above in section 5.9, MPAA member companies proposed that the draft Compliance Requirements be modified so as to prevent Unscreened Content from being passed to outputs protected by “authorized” protection technologies, on the basis that Unscreened Content is not known by the device to be DTV content. Because this proposal was made near the scheduled conclusion of the work of the BPDG, and entailed a substantial change to the Compliance Requirements, participants have generally expressed the need for further opportunity to consider and understand its rationale and impact. Nevertheless, a number of participants have commented regarding possible alternatives or modifications to the proposed solution that might be preferable, but others objected to them.

6. Matters Suggested for Referral to the Parallel Group

In the course of the BPDG discussions, several issues arose that related to enforcement and related policy issues. The BPDG therefore recommends that the parallel group should discuss and consider the following issues:

6.1 It is the understanding of the BPDG that the parallel group will consider means of enforcement of broadcast protection requirements, including by legislative or regulatory means. As noted above, two approaches have been proposed in drafts of section X.2, setting forth concepts as to how the Compliance and Robustness Requirements might be implemented and enforced. The BPDG recommends that the parallel group give consideration to these and potentially other proposed approaches for section X.2.

6.2 As noted in paragraph 5.1 above, certain BPDG participants recommend that the parallel group consider language that might better define the scope of limitation upon the unauthorized redistribution of DTV content.

6.3 The proposed definition of "Downstream Product" includes a provision whereby the manufacturer of such product "has committed in writing that such product will comply with the Compliance Requirements and be manufactured in accordance with the Robustness Requirements, such that such product shall be a Covered Product." The BPDG suggests that the parallel group consider the nature of the requisite written commitment.

6.4 The BPDG recognized that certain cable and satellite systems might retransmit to the home in encrypted form content that initially was broadcast as Unencrypted Digital Terrestrial Broadcast Content. The BPDG recommends that the parallel group should discuss any requirements necessary to ensure that such content is protected when retransmitted in encrypted form.

6.5 Consistent with industry practice, the BPDG acknowledges that some period of time must be given before manufacturers must produce products in compliance with any instrument that implements the Compliance and Robustness Requirements. The BPDG requests the parallel group to consider a reasonable time, taking into account both the goals of promptly implementing broadcast protection, and practical considerations relating to the development and licensing of technical methods that comply with the particular instrument, the design, manufacture and distribution in sufficient quantities of compliant products, and the sale of products manufactured before such instrument took effect.

6.6 The BPDG requests that the parallel group consider proposed criteria that could be used to determine whether a particular technology should be "authorized" as a digital output protection technology or recording method. Three proposals were presented to the BPDG. Two proposals coalesced into a single proposal offered by companies of the Motion Picture Association of America ("MPAA"), DTLA and Computer Industry Group ("CIG"), which was part of an overall proposal that included amendments to the Compliance and Robustness Requirements (the "MPAA, DTLA and CIG" proposal). That proposal is attached to this Report at Tab F. The other proposal for criteria, offered by Philips and supported by several

participants, is attached to this Report at Tab G. The two approaches can be summarized as follows:

6.6.1 The MPAA, DTLA and CIG proposal includes three criteria that are intended to reflect demonstrated marketplace use or approval of the technology by content owners (and, in the case of Criterion Two, by implementer licensees), and one criterion (Criterion Three) by which a proponent may demonstrate that a proposed technology provides protections at least as effective as those offered by any other technology on the list. Several organizations and participants have submitted statements noting that certain of their technologies would qualify under the criteria noted above.

6.6.1.1 DTLA submitted a statement that the DTCP transmission protection technology satisfies at least Criterion Two of the MPAA, DTLA and CIG proposal; and that protection technologies that were approved to protect DTCP-protected content, namely, HDCP for transmission protection and CPRM and D-VHS for recording protection, would therefore qualify under the criteria as authorized technologies. This submission is attached at Tab H. DTLA proposed "Associated Obligations" that define the requirements for implementation of DTCP in conjunction with the BPDG Compliance and Robustness Requirements, which obligations also are included in the attachment to Tab H. At the BPDG meeting on April 29, participants speaking on behalf of Sony Pictures and Warner Bros. confirmed that those companies had entered into licenses to use DTCP and that they believe DTCP and the other three technologies mentioned above satisfy the criteria set forth in the MPAA, DTLA and CIG proposal. Representatives from four other MPAA companies also stated at the April 29 meeting that they believe the four technologies satisfy the criteria and should be included on Table A.

6.6.1.2 Digital Content Protection, LLC submitted a statement that the HDCP technology satisfies at least Criterion Four of the MPAA, DTLA and CIG proposal, and proposed "Associated Obligations" for HDCP, both of which are attached at Tab I.

6.6.1.3 4C Entity, LLC submitted a statement that the CPRM technology satisfies at least Criterion Four of the MPAA, DTLA and CIG proposal, and proposed "Associated Obligations" for CPRM, both of which are attached at Tab J.

6.6.1.4 JVC submitted a statement that the D-VHS technology satisfies at least Criterion Four of the MPAA, DTLA and CIG proposal, and proposed "Associated Obligations" for D-VHS, both of which are attached at Tab K.

6.6.1.5 Microsoft submitted a statement that the Windows DRM satisfies one or more of these criteria. This submission is attached at Tab L. Microsoft provided a description of how its Windows DRM protects content through renewability of compromised security components, enforcement of revocation and other means.

6.6.2 The Philips proposal is set forth as a combination of "objective" technical criteria, and criteria defining specific attributes that would be required of licenses for any proposed

technology (e.g., that licenses should be available for use of a technology only to protect broadcast content).

6.6.2.1 Philips submitted a statement that its OCPS transmission protection technology satisfied both its proposed criteria and one of the MPAA, DTLA and CIG proposed criteria. Philips attached to its submission a technical description of the OCPS technology, a term sheet outlining proposed license terms, and proposed compliance and robustness rules. This submission is attached at Tab M. Philips subsequently proposed "Associated Obligations," which are also attached at Tab M.

6.6.3 Proponents and opponents of each approach described specific concerns and objections at length in several meetings, and particularly in the meetings on April 3 and April 29. Inasmuch as issues surrounding the appropriateness of each approach, or of particular criteria, implicate policy considerations, the BPDG recommends that this issue be considered further by the parallel group.

6.7 The MPAA, DTLA and CIG proposal suggested that several additional issues be referred to the parallel group:

6.7.1 On the belief that adding to Table A technologies that satisfy the proposed criteria should be as seamless and transparent as possible, the MPAA, DTLA and CIG proposal requested that parallel group undertake the task of creating a straightforward process under Criteria One and Two, whereby a proponent would give notice that one or more of the criteria are satisfied (which notice would, where applicable, specify which companies have used or approved a technology), and an adequate opportunity would be given to each company named in such notice to dispute the claim that the named company used or approved the technology. If no such dispute were forthcoming, the proposed technology would be added to Table A. The process would need to provide a speedy process to resolve any such disputes.

6.7.2 Some determinations of whether a company has "used or approved" a technology may be capable of resolution only through information in the hands of the entity that has used or approved it. Accordingly, the MPAA, DTLA and CIG proposal requests the parallel group to consider a process whereby a company that proposes a technology for addition to Table A may obtain information regarding whether such an entity has used or approved the technology.

6.7.3 When a technology has been "significantly compromised" in relation to its ability to protect Unscreened Content and Marked Content from unauthorized redistribution (including unauthorized Internet redistribution) it may no longer be used as a comparison metric under Criterion Three for technology proposed to be added under this criterion. Accordingly, the MPAA, DTLA and CIG proposal requests the parallel group to consider a process for determining whether such a compromise has occurred.

6.7.4 If a technology has been compromised, and the compromise is substantially higher than "significantly compromised" noted above, the MPAA, DTLA and CIG proposal requests the parallel group to consider a standard for removing a technology from Table A. Such a standard should take into account the protection of Unscreened Content and Marked Content from unauthorized redistribution, as well as the impact on content owners, consumers, and

manufacturers that would result from removal of a technology from the list and the continued use of such compromised technology. The proposal also requests that the parallel group address a process by which (a) requests can be made to remove a technology from Table A on the basis that such standard has been met; (b) interested parties can object to such requests for removal; and (c) a timely determination would be made as to whether or not such technology will be removed from Table A (after a reasonable grace period).

6.8 Computer Industry Group companies have requested that the parallel group consider the establishment of additional or variations of the objective criteria set forth in Criterion Three of the MPAA, DTLA and CIG proposal, and other implementers have requested that additional or variations of the objective criteria be added as separate criteria. Criterion Three already contains tests for a technology which is proposed to be added to Table A without direct content owner "use or approval." Computer Industry Group companies believe that the parallel group could examine such Criterion in light of the limits of the BPDG goals as stated in the work plan for the BPDG: "to prevent unauthorized redistribution of unencrypted digital over-the-air broadcast content." Those companies believe that some of the criteria could be altered or additional criteria substituted that would permit a technology to be added to the list consistent with those goals and consonant with the Compliance and Robustness Requirements. Those companies were concerned that comparing license terms relating to security (*i.e.*, output and recording controls), enforcement and Change Management might not be objective. Those companies believe that (a) it should not be difficult, in the context of protecting over-the-air digital television, to create alternatives or variations of those criteria that both are objective and are consistent with the robustness and compliance provisions of the Compliance and Robustness Requirements and (b) it is critical that the requirements be objective and readily understood by a manufacturer proposing a technology to be added to the list.

6.9 A number of participants including Computer Industry Group companies requested that the parallel group determine that the Compliance and Robustness Requirements not go into effect until a minimum number of technologies have been included in Table A. (The MPAA, DTLA and CIG proposal does not require this.) Those participants view this as an important precondition to compliance obligations for two reasons: (a) since compliance will be a new government mandate, there should be a reasonable number of technologies to select from in order to ensure that no manufacturer is forced to adopt one of a small number of alternatives; (b) Criterion Three of the MPAA, DTLA and CIG proposal only functions adequately if there are a sufficient number of technologies to compare a technology proposed to be included on the list.

6.10 Similarly, some companies have requested that no technologies be placed on Table A (as "recommended," "approved" or otherwise) until the criteria for Table A have been finalized. The Co-Chairs note that the Table A document attached at Tab C summarizes proposals made by each of various technology companies and the statements made in support of or in contradiction to such proposals.

[END]

EXHIBIT J

Copyright 2002 Warren Publishing, Inc.
PUBLIC BROADCASTING REPORT

June 14, 2002, Friday

SECTION: LATEST NEWS**LENGTH:** 1121 words**HEADLINE: INDUSTRY GROUPS SEE LIMITED CONSENSUS ON BROADCAST FLAG STANDARD****BODY:**

Cross-section of industry executives said they had reached consensus on how to protect digital broadcast content from unauthorized retransmission over Internet. But it was apparent from report they released June 4 that there wasn't unanimity on the subject. Many companies and groups that were part of negotiating process objected to final agreement, citing problems with almost every aspect. Report by Bcst. Protection Discussion Group (BPDG) -- composed of movie, TV, consumer electronics and other executives -- said there was "substantial agreement" on use of redistribution control descriptor established earlier by Advanced TV Systems Committee (ATSC) for signal protection for digital TV (DTV) content. Report was sent to Copy Protection Technical Working Group, which is expected to submit it to Congress for possible legislation. BPDG said it didn't think it was appropriate venue to address enforcement issues, so it recommended establishing parallel group to work on those questions. Specific "broadcast flag" to be used is ATSC standard A/65A, and protection requirements should begin at point of demodulation of incoming 8-VSB, 16-VSB, 64-QAM or 256-QAM digital signal, report said. For digital cable distribution of DTV, requirements can be implemented in cable systems using point of deployment (POD) module to pass through content in encrypted form, it said. Because satellite and cable services can encrypt DTV signal retransmissions, they may not need to implement broadcast flag solution. However, another group of executives was asked to recommend any requirements necessary to ensure that such content is protected when retransmitted.

When demodulated DTV content has been screened and broadcast flag isn't present and it's otherwise unmarked, no further requirements or limitations should be imposed on handling or recording, study said. It said requirements to protect digital recordings shouldn't interfere with ability of consumers to make secure copies of DTV content marked with broadcast flag either on personal video recorders or tapes or discs. Report said requirements to protect digital outputs shouldn't interfere with ability of consumers to send DTV content across secure home digital network digital devices.

But that was major point of contention for group members who manufacture consumer electronics. Draft requirements would permit computer products to continue to deliver protected DTV content through unprotected outputs at certain level of video quality. Provision was designed to accommodate legacy computer monitors. Some participants suggested that that capability also apply to CE products so that cable and satellite set-top boxes could deliver DTV content to legacy computer monitors.

Some participants said scope of protection should be limited to unauthorized redistribution over Internet. Others said parallel group should consider more precise definition of protection to clarify whether it applied to retransmission of DTV in "personal" environments, such as in home, car, portable devices and communications devices between primary and secondary homes. Philips also offered alternative "flag preserving" method, but that was rejected by majority because they said it would be based on compliance rather than self-protection. Philips and some other CE manufacturers also suggested that for limited number of years, in-the-clear recordings of unscreened yet marked content could be made using standard definition DVD recorders. Motion picture companies opposed such "grandfather" provision because millions of legacy DVD-ROM drives would remain capable of unauthorized redistribution of that content.

MPAA Pres. Jack Valenti said he was pleased industries were able to reach consensus, although he admitted it was far from unanimous decision. He expressed hope that all CE manufacturers would have to conform all of their licensed products to protect digital broadcast content. "This will undoubtedly require some kind of government mandate by way of legislation or regulation or a combination of both, but whatever it is, it would be very narrowly focused and very tightly drawn," Valenti said. He said agreement didn't address either analog hole or peer-to-peer file sharing. CEA said it still was reviewing report and so couldn't comment on it in its entirety. However, CEA's spokesman said Assn. agreed with objections laid out by many of its members on home recording and fair use rights. He also said he believed process was rushed because of copy protection bill recently introduced by Senate Commerce Committee Chmn. Hollings (D- S.C.). CCIA said pact would harm industry and betray consumers -- and plan wouldn't work. "Since all PCs must copy files to function, no computer scientist has yet developed an anticopying technology that is actually effective without simultaneously hobbling the machine," the group said. CCIA also criticized plan for giving "Hollywood -- not consumers -- the right to decide what the public may and may not record in the privacy of their own homes."

Also objecting was **Electronic Frontier Foundation**, which said Hollywood studios essentially were demanding that CE industry redesign DTVs. "Congress, industry and consumers must all reject Hollywood's attempt to force an unconscionable government mandate restricting technology innovation and the rights of digital television consumers," EFF staff technologist Seth Schoen said. EFF said whole process was flawed because group reached many of its decisions based on views of few private companies.

Meanwhile, Rep. Tauzin (R-La.) set July 15 deadline for movie studios, broadcasters, cable, consumer electronics industry and others to resolve all policy and technical issues involving broadcast flag. Industry executives announced June 4 that their Broadcast Protection Discussion Group had reached consensus, although their report included much dissension. Tauzin's demand came in 2-1/2-hour DTV roundtable discussion June 11 with more than 2 dozen industry executives, FCC staff, others. Group included **MPAA** Pres. Jack Valenti, Fox Group Pres.-Engineering Andrew Setos, NCTA Pres. Robert Sachs. Tauzin, chmn. of House Commerce Committee, has been holding series of such informal, private discussions to facilitate solutions to DTV transition. His spokesman, Ken Johnson, said meeting covered copyright protection, DTV cable compatibility, broadcast flag and other issues: "Chairman Tauzin was encouraged by today's discussions. He believes we're making steady progress and we now have a game plan in place designed to produce an agreement on many of the contentious issues holding up the transition."

LOAD-DATE: June 17, 2002

EXHIBIT K



Electronic Frontier Foundation

[EFF Home](#)

[Join EFF/Donate!](#)

[About EFF](#)

[Free Speech Online](#)

[Audiovisual Freedom](#)

[Online Privacy](#)

[Active Legal Cases](#)

[Recent News](#)

[EFF BPDG Blog](#)

[EFF Newsletter](#)

[Internships](#)

[EFF Topics](#)

[Radio EFF](#)

[Contact Us](#)

[Calendar](#)

[Media Resources](#)

[Subscribe to the EFF Action Center](#)

Got a domain name (UDRP) problem? [Click here.](#)

[EFF Privacy Policy](#)

Search:



[Site Map](#)

[Most Popular EFF Pages Today](#)

EFF Needs YOU!

SUPPORT EFF! - YOUR tax-deductible gift is what we need to keep going strong!

[Calendar of Events](#) [Active Legal Cases](#) [EFF in the Media](#) [Newsletter](#) [Join EFF!](#)

Featured News

■ **Internet Filtering Software Wrongly Blocks Many Sites** - Damages Educational Opportunities for Public School Students [[EFF media advisory](#)] (September 18, 2002)

■ **School Communities Give Internet Filtering Law Failing Grade** - Speak Out in San Francisco, New York, and Boston [[EFF media release](#)] (September 18, 2002)

■ **School Communities Give Internet Filtering Law Failing Grade** - Research Reports Thousands of Sites Incorrectly Blocked [[EFF media advisory](#)] (September 16, 2002)

■ **Motions Filed in Morpheus Peer-to-Peer Case** - Judge to Consider Legality of Gnutella Software [[EFF media release](#)] [[Court briefs](#)] (September 9, 2002)

■ **Electronic Frontier Foundation, Verizon Guard Client Privacy** - Consumers v. Recording Industry on Peer-to-Peer Anonymity [[EFF media release](#)] [[RIAA v. Verizon case documents](#)] (August 30, 2002)

■ **Recording Industry Withdraws Internet Attack** - Great Internet Firewall Remains in China

Resources

Spotlight:



Larry Lessig's Speech @ OSCON



Watch the Tinsel Town Club video

Campaigns:

[Online Free Speech](#)

[Audiovisual Freedom](#)

[Internet Privacy](#)

Topics:

[Detailed Topics Index](#)

[Activism/ Government](#)

[Alerts - Contacting Congress](#)

[Censorship/ Free Speech](#)

[Blocking/ Censorware](#) - [Censorship Laws](#) - [SLAPPS](#)

[Intellectual Property/ Fair Use](#)

[P2P - CBDTPA/ SSSCA - DMCA - UCITA/ UCC2B](#) -

[[EFF media advisory](#)] [[RIAA dismissal](#)]
(August 21, 2002)

■ **[Recording Industry Attacks Internet to Stop Chinese Pirates](#)** - Lawsuit Would Extend Great Internet Firewall of China to US
[[EFF media release](#)] [[Court filings](#)]
(August 19, 2002)

■ **[Judge Grants Consumer Voice in ReplayTV Lawsuit](#)** - Hollywood Tries to Skip Over Consumers' Concerns
[[EFF media release](#)] [[Court order](#)] [[EFF Fair Use FAQ](#)]
(August 16, 2002)

■ **[Musician Disputes Industry's Stance on Music Sharing](#)** - Janis Ian Urges Artists Speak Out, Support Free Downloads
[[EFF media release](#)]
(August 15, 2002)

■ **[ReplayTV Owners Defend Right to Digital VCRs](#)** - Hollywood Tries to Skip Over Customers' Concerns
[[EFF media advisory](#)]
(August 9, 2002)

■ **[Paper Explains Flaw in Videogame Security System](#)** - Researcher Escapes Chilling Effect of Digital Copyright Law
[[EFF media advisory](#)] [[Huang's paper \(pdf\)](#)]
(August 8, 2002)

■ **[FCC to Announce Hollywood's Controversial "Broadcast Flag"](#)** - Anti-Competitive Proposal Undermines Adoption of Digital TV
[[EFF media advisory](#)] [[EFF letter to FCC Chairman](#)]
(August 7, 2002)

■ **[Court Grants Access to Net Regulatory Corp Records](#)** - Director Successful in Challenge to ICANN's Obstruction
[[EFF media release](#)] [[Court ruling](#)]
(July 29, 2002)

■ **[Court Hearing in Net Regulatory Corp. Director Case](#)** - ICANN's Actions Illegal and Hampering Reform
[[EFF media advisory](#)] [[Case archive](#)]
(July 25, 2002)

[Elcomsoft/ Sklyarov](#) -
[Johansen](#) - DVD
[DeCSS/ 2600](#) - SDMI
- [DRM Systems](#) -
[HDTV](#) - [Copyright Abuse](#) - [Domain Disputes](#)

Privacy/ Security
[Surveillance](#) -
[Anonymity](#) -
[Marketing/ Profiling](#) -
[National ID](#) - [Crypto Export](#)


Infrastructure
[DNS/ ICANN](#) -
[Wireless](#)

Online Community
[Net Abuse](#) - [Spam](#)

Programs:

[EFF Blogs](#) -
[Pioneer Awards](#) -
[Radio EFF \(MP3s\)](#) -
[Support Us While Shopping](#)

[EFF's Top 12 Ways to Protect Your Online Privacy](#)

- **Electronic Frontier Foundation Joins Wireless Crusade** - New Project Tracks Wireless-Friendly Service Providers
[\[EFF media release\]](#) [\[Wireless friendly ISP list\]](#)
 (July 25, 2002)
- **Commerce Dept. Considers Digital Rights Management** - Electronic Frontier Foundation Submits Fair Use Comments
[\[EFF media advisory\]](#) [\[EFF DRM comments\]](#)
 (July 18, 2002)
- **Director Demands Disclosure From Net Regulatory Corp.** - ICANN's Actions Illegal and Hampering Reform
[\[EFF media release\]](#) [\[Reply brief\]](#)
 (July 15, 2002)
- **Privacy Groups Demand Protection of Users' Anonymity Online** - Urge Internet Providers Shield Clients From Spurious Suits
[\[EFF media release\]](#) [\[cyberSLAPP\]](#)
 (July 11, 2002)
- **Court Censors Tax Site, Restricts Searches** - Electronic Frontier Foundation Asks Court to Reconsider
[\[EFF media release\]](#) [\[Amicus brief\]](#)
 (July 10, 2002)
- **2600 Magazine Won't Seek Supreme Court Review in DVD Case** - Activists Vow to Continue Digital Copyright Fight
[\[EFF media release\]](#) [\[2600 release\]](#) [\[DMCA report card \(pdf\)\]](#)
 (July 3, 2002)
- **The Quest for Tunes: Carabella Trades Rights for Music** - Video Game Spotlights Threats to Online Privacy and Freedom
[\[Play the game\]](#) [\[EFF media release\]](#) 
 (June 19, 2002)
- **Biometrics, Surveillance, National ID Threats to Privacy** - Electronic Frontier Foundation Releases Reports
[\[EFF media release\]](#)
 (June 13, 2002)
- **Electronic Frontier Foundation Opposes "Broadcast Flag"** - Proposed Technology Mandate Will Harm

Consumers

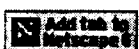
[[EFF media release](#)] [[Letter to Rep. Tauzin](#)]
(June 11, 2002)

■ **ReplayTV Users: "We Are Not Thieves"**

ReplayTV customers represented by the EFF have filed a lawsuit against the entertainment industry to protect their rights to skip over commercials and record television programs for later viewing using digital video recorders. [[EFF media release](#)] [[EFF case page](#)]

■ **Organizations Wary of Plan to Restrict Digital Television** - Electronic Frontier

Foundation Rejects Non-Consensus Report [[EFF media release](#)] [[Summary EFF comments](#)] [[EFF BPDG weblog](#)]
(June 4, 2002)

More Headlines

Add an EFF News item to your
Netscape/Mozilla "MySidebar"! (requires
JavaScript)

EFF'S AFFILIATIONS AND COALITIONS:

[Global Internet Liberty Campaign \(GILC\)](#)
[Internet Free Expression Alliance \(IFEA\)](#)
[Digital Future Coalition \(DFC\)](#)
[Free Expression Network \(FEN\)](#)

Search: 

[Site
Map](#)

[Most Popular EFF Pages
Today](#)

Server Hosting and Bandwidth
Donated by the good folks at:
UnitedLayer Inc.

Companies and Individuals who have made Significant Generous Donations to us who help make our work possible.

EXHIBIT L

In the 207th Issue of EFFector:

- [ALERT: Congress Calls For Public Participation on Digital Music Issues](#)
- [EFF Position on Joint AOL-Time Warner/Intel Pro-DRM Statement: A Step in the Wrong Direction](#)
- [Exchange Ideas with EFF Founders Mitch Kapor and John Perry Barlow](#)
- [Director Sues Organization that Oversees Internet - ICANN Broke Law](#)
- [Media Conglomerate Threatens Suit Against Gamer Community](#)
- [CHIPA Alert](#)
- [EFF Thanks RSA Security](#)

For more information on EFF activities & alerts: <http://www.eff.org/>

To join EFF or make an additional donation:

<http://www.eff.org/support/>

EFF is a member-supported nonprofit. Please sign up as a member today!

ALERT: Congress Calls For Public Participation on Digital Music Issues

Submit Comments Opposing Technology Mandates

(Issued: Friday, March 22, 2002 / Deadline: Monday, April 8, 2002)

Introduction:

Imagine a world where all digital media technology is either mandatory or forbidden -- Senator Fritz Hollings and a cabal of Hollywood entertainment interests are cooking up a set of laws aimed at conjuring this apocalyptic world into existence.

Today, Senator Hollings introduced the alarming Consumer Broadband and Digital Television Promotion Act (CBDTPA), which will give Hollywood plutocrats the power to stall new digital media technologies for a year, negotiating a phony "consensus" at lawyer-point with technologists. This "consensus" will receive the force of law, prescribing which user-hostile features are mandatory and which innovative features are forbidden. CBDTPA is derived from the draft SSSCA (Security Systems & Standards Certification Act), the subject of our last alert. Both the House and the Senate have called for comments on the future of digital music, an issue that is deeply entwined with technology mandates.

What YOU Can Do Now:

This is **YOUR** chance to voice your opposition to laws that make all digital media technology mandatory or forbidden.

- Send the EFF letter below to both the House and the Senate. Feel free to use this letter verbatim, or modify it as you wish. Please be polite and concise, but firm. The Senate Judiciary Committee's Chairman Patrick Leahy and Ranking Republican Member Orrin Hatch are accepting comments via a form at: http://judiciary.senate.gov/special/input_form.cfm?comments=1
The House Judiciary Committee Subcommittee on Courts, the Internet & Intellectual Property is accepting comments by email and fax, addressed to the Chair:
Hon. Howard Coble
howard.coble@mail.house.gov
fax: +1 202-225-3673
- For information on how to contact your legislators and other government officials, see EFF's "Contacting Congress and Other Policymakers" guide at: <http://www.eff.org/congress.html>
- Join EFF! For membership information see: <http://www.eff.org/support/>

Sample Letter:

Dear Senator Leahy, Senator Hatch, and Representative Coble:

I am writing to you today to express my concern at the growing trend to impose governmental technology mandates at the behest of the entertainment industry.

The introduction of the CBDTPA by Senator Hollings illustrates the inevitable conclusion of such mandates: a world where all digital media technology is either forbidden or compulsory. CBDTPA grants veto power over new technologies to the special interest groups who have opposed innovation since the Betamax fight.

Technology mandates are anti-consumer, treating us all as potential criminals and punishing us in advance for infringements we haven't committed. They are inevitably used to strengthen copy-prevention ("digital rights management") technologies that give disproportionate power to vendors, stripping us of our traditional fair-use rights, restricting our power to back up, sell, loan, transfer, and format-shift the products we've purchased.

Technology mandates are anti-innovative, stalling all new designs in lengthy one-sided "negotiations" where the entertainment industry can strong-arm technologists into adopting anti-customer "features."

Technology mandates hurt American companies by imposing expensive design requirements and lengthy design reviews. Foreign competitors are exempt from these restrictions, a situation that harms exports and will create a grey market for uncertified technologies from abroad.

I urge your committee to reject anti-consumer, anti-innovative, anti-competitive technology mandates, especially the CBDTPA and the "mini-CBDTPA" that is in the

offing to give force of law to the "consensus" developed by the Broadcast Protection Discussion Group for digital TV standards.

I further urge you to repeal the anti-circumvention provisions of the Digital Millennium Copyright Act (DMCA). Never used to prosecute anyone accused of infringing copyright, in practice these provisions have chilled the speech of computer scientists, stifled journalistic criticism, and prosecuted computer programmers and the companies for which they work.

Please, do the right thing for consumers, innovation and American business.

Sincerely,

[Your name;
include full address for maximum effectiveness]

Tips:

Please remember to be polite but firm. Ranting, swearing, or lack of clear focus and resolve will not make a good impression. Try to make it brief and clear, without getting into nitpicky details. Re-casting the letter in your own words will be more effective than copy-pasting our sample.

Activists Around the World

This alert is primarily for U.S. residents. However, this issue is of importance globally, so keep an eye out in your own jurisdiction for related matters you can act on.

CAFE Campaign:

This drive to contact your legislators about the CBDTPA and the threats it poses to fair use and innovation is part of a larger campaign to highlight intellectual property industry assaults against the public's fair use rights, and what you can do about it.

Check the EFF *Campaign for Audivisual Free Expression* (CAFE) website regularly for additional alerts and news:

<http://www.eff.org/cafe/>

Background:

The CBDTPA, Hollywood and Holling's bid to strangle the American technology industry, is just the latest salvo. Over the past year, the Copy Protection Technologies Working Group has convened the Broadcast Protection Discussion Group, which has been laying down the "consensus" on new digital television devices for a captive audience of representatives from electronics, software and computer companies.

These profoundly undemocratic proceedings sacrifice consumer rights, free speech and innovation on the altar of Hollywood's hysterical technophobia.

The CBDTPA promises a world where useful features would be eliminated if the possibility for their misuse existed, such as:

- limits on "format-shifting," for example, the ability to create mix-CDs of music you've paid for;

- controls built into hard-drives that would allow files to be labelled as "unmovable," so they could not be backed up, or moved to another machine, nor could the drive be effectively optimized;
- restrictions on the manufacture and distribution of devices and programs that can play unrestricted formats, such as MP3 audio and DivX video files.

Senator Hollings, called "The Senator from Disney" for his close ties with Hollywood money, continues to push for technology mandates, federally imposed specifications for technologies that outlaw legitimate functionality in order to control illegitimate uses. It's the technological equivalent of requiring that crowbars be made of foam-rubber on the grounds that metal ones may be used in the commission of burglaries.

This is not the way that copyright law works. The Betamax decision, handed down by the Supreme Court in 1984, established the principle of "substantial non-infringing uses." The Betamax principle allows technologists to create tools that can be used for good, **even if they can be used in other ways**. It is an affirmation of the social good of innovation and of "fair use." Every technology company in the world depends on this affirmation -- it is the foundation of creative, innovative technology.

Incremental CBDTPA

After 2006, the FCC will require all over-the-air broadcasts to be digitally encoded. Under the pretext of preventing the "Napsterization" of their video signals, the MPAA has convened the Broadcast Protection Discussion Group (BPDG) of the Copy-Protection Technical Working Group (CPTWG). The BPDG's "standards," developed in concert with a group of arm-twisted representatives from major technology vendors, will specify flags controlling the public's ability to store, copy, and share digital TV signals.

When Senator Hollings held his hearings on copyright reform in early March 2002, he heard testimony from studio-heads and technologists that presented the BPDG's process as a model for future "cooperative" ventures between Hollywood and technologists. The BPDG's representatives explained that their measures would only safeguard copyright if their "standards" were mandated by government.

Any hint that this mandate would limit the freedom to innovate was downplayed -- if the standard is voluntarily arrived at by all the affected parties, where's the loss of freedom?

Yet the standard must be mandated if it is going to be effective. Consumers will not "voluntarily" choose to purchase restrictive technology if they have other choices, and technology companies would be foolish to invest in restrictive technology that consumers will not buy. The only way the investment makes sense is if there is no competing "open" technology choice for the consumers. And the only way to kill off competition from products consumer prefer is to make those products illegal.

A mandated CPTWG standard is a clear abridgement of freedom. This "standard" has in reality been arrived at by a handful of players who exclude the press and have no means for receiving public comment. A mandated standard eliminates the ability for competing techniques to be tested in the marketplace. The public good is best served when vendors voluntarily adopt standards on the basis of consumer demand.

The scope of a CPTWG mandate was likewise downplayed. Receiving, storing, copying and transmitting DTV signals isn't merely the domain of set-top boxes. A CPTWG mandate would

necessarily extend into the PC, requiring substantial integration with device drivers, operating systems, firmware and application APIs.

Links:

Full text of CBDTPA (bill S. 2048):

http://www.eff.org/IP/SSSCA_CBDTPA/20020321_s2048_cbdtpa_bill.pdf

For more information about CBDTPA (and its older "parent", SSSCA), see:

http://www.eff.org/IP/SSSCA_CBDTPA/

For more information on the future of digital television, see:

<http://www.eff.org/IP/Video/HDTV/>

See also EFF's "Frequently Asked Questions (and Answers) About Fair Use":

http://www.eff.org/IP/eff_fair_use_faq.html

Declan McCullagh *Wired News* article on CBDTPA, "What Hollings' Bill Would Do":

<http://www.wired.com/news/politics/0,1283,51275,00.html>

Full text of CBDTPA bill:

<http://cryptome.org/broadbandits.htm>

About EFF:

The Electronic Frontier Foundation is the leading civil liberties organization working to protect rights in the digital world. Founded in 1990, EFF actively encourages and challenges industry and government to support free expression, privacy, and openness in the information society. EFF is a member-supported organization and maintains one of the most linked-to websites in the world:

<http://www.eff.org>

Contacts:

Robin Gross, EFF Intellectual Property Attorney

robin@eff.org

+1 415-436-9333 x112

Cory Doctorow, EFF Outreach Coordinator

cory@eff.org

+1 415 436 9333 x106

- end -

[Back to table of contents](#)

EFF Position on Joint AOL-Time Warner/Intel Pro-DRM Statement:

A Step in the Wrong Direction

Recently, Intel Corporation has issued two very different statements about the dangers to innovation and fair use posed by copyright owners' attempts to get Congress to put the power of federal law behind digital rights management schemes.

EXHIBIT M

Electronic Frontier Foundation
Robin D. Gross -- Attorney @ Law
Phone: 415.436-9333 Fax: 415.436-9993
Email: robin@eff.org Web: <http://www.eff.org>

TESTIMONY OF ELECTRONIC FRONTIER FOUNDATION (EFF) BEFORE COPYRIGHT OFFICE
PUBLIC HEARINGS ON DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)
May 19, 2000

The Electronic Frontier Foundation (<http://www.eff.org>) appreciates this opportunity to testify regarding the adverse effects from the prohibition against circumvention of technological protections enacted by the DMCA.

DVD technology causes to an adverse effect on people's ability to make non-infringing uses of copyrighted works and should therefore be exempted from the DMCA's circumvention ban.

The licensing terms imposed on DVD technology prevent player manufacturers from offering people the ability to bypass the region codes. The same terms prevent players from making noninfringing copies on traditional VHS tapes or computer hard drives for personal or educational use. People who have attempted to eliminate these restrictions, by making competing DVD players from legitimate reverse-engineering rather than by signing a license, have been sued and enjoined -- under the DMCA -- by major movie studios. (1)

The Content Scramble System (CSS) is deliberately designed to prevent legitimate purchasers from being able to view their own purchased movies. *The region coding scheme used by DVDs prevents individual US residents who purchase DVD movies from anywhere else in the world from simply VIEWING these movies on DVD players sold in the United States.* This diminishes the ability of these individuals to use copyrighted works in ways that are otherwise lawful. In other words, the DMCA is being used to prevent people from watching the movies they own on the machines that they own.

The adverse impact on persons outside the US is even greater. A large fraction of the world's movies are created by US movie studios, in the US, and released first on DVD in the US. At that time, persons anywhere in the world are free to purchase these DVDs from US retailers or wholesalers. However, when they arrive, the CSS technical protection measures prevent them from playing. Months later, some of these movies are re-released on DVDs coded for other regions. These re-releases are sold at higher prices than the original US release, particularly in Europe. This delays and diminishes the ability of the entire world's population to use these copyrighted works in ways that are otherwise lawful.

DVDs using region coding serve as a technological restraint on the global trade in copyrighted movies. The leading UK grocery chain, Tesco, started selling discount DVD machines in February 2000. By mid-February they were selling tens of thousands of players from 400 stores, "once Internet sites and electrical magazines showed customers how to change the player to recognize discs from around the world."

Tesco's press release mentions their letter to Warner Home Video "calling for an end to the 'unnecessary practice' of zoning - which uses technology to prevent customers from buying DVD discs from around the world to play on machines in the UK. The letter goes on to say that Tesco believes 'This is against the spirit of free competition and potentially a barrier to trade.'" Their World Sourcing Director, Christine Cross, said "If we find a practice that we believe is keeping prices high -- we'll fight to change it so prices come down." (2)

The licensing organization that controls DVD technology, the DVD Copy Control Association has taken steps to exterminate this supply of 'region free' players. Its FAQ says, "In cases where DVD-CCA learns of such products, immediate action is taken through the manufacturer to have the product corrected to conform with the CSS license." (3) Indeed it enforced a contract term on December 31, 1999 that eliminated its licensees' ability to sell computer DVD drives whose region controls were implemented in software.

Millions of users of DVD technology have been adversely affected in their ability to make noninfringing uses of copyrighted works. The 'region coding' scheme prevents virtually every commercial DVD from being playable in most regions of the world, raising the prices and reducing the availability of works to legitimate buyers. ***This has an adverse effect on the ability of buyers to simply VIEW a work which they have purchased -- the most noninfringing use possible.***

CSS together with the web of laws and contracts around it also eliminate the individual's ability to make noninfringing copies of DVD images. Fritz Attaway, MPAA's Washington General Counsel, declared under oath, "Under the terms of the CSS license, such players may not enable the user to make a digital copy of a DVD movie."(4) The restriction is imposed by contracts, implemented by technology, and enforced by DMCA lawsuits.

There is no balance. CSS does not follow the boundaries of the copyright law. Professors are unable to make excerpts to show their classes. Parents are unable to make VHS copies for their kids' VCRs. Programmers and artists are unable to manipulate the images with their own software. The CSS's blanket prohibition of copies and excerpts throws the baby out with the bath water. ***CSS prohibits all fair use copying, as well as all illicit copying. It prohibits all copying.***

Congress expressed its clear intent in Section 1201(c)(1) of the DMCA by stating that "Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title."

According to the DMCA's plain wording the traditional limitations to the copyright holders' exclusive rights shall remain in the digital realm. Congress' choice of the word "shall" indicates its intention is not permissive or optional at the choice of the copyright holder, but rather a mandatory requirement that balance and longstanding traditional doctrines, such as fair use and the First Sale Rule continue to have meaning in the digital paradigm.

There is no debate that Congress intended balance in the DMCA and preservation of traditional copyright principles in the digital world. Congress recognized the inherent dangers in enacting a circumvention ban and instructed this body to anticipate adverse effects and rule additional classes exempt from the general ban as a remedy.

As the U.S. Supreme Court has explained, fair use serves as a First Amendment safety valve within copyright law. *Harper & Row, Publishers v. Nation Enters.*, 471 U.S. 539, 555-60 (1985). Copyright law's fair use privilege fulfills its Constitutional purpose by allowing individuals to copy works for socially important reasons without the permission of the author. Thus granting perfect control to copyright holders would be Constitutionally impermissible. This rule-making is charged with effectuating the DMCA in such a way that it does not violate the spirit of the Constitutional limitations placed on copyright. To find otherwise would allow the DMCA to swallow fair use in clear contradiction to Congress' plain intent in section 1201(c).

At a recent conference at Yale Law School, the MPAA publicly stated that it was the organization's position that an individual should be required to obtain a license before making fair use of a DVD. (5) Clearly, this position cannot withstand legal sanction. ***It would be an abuse of intellectual property law to allow the motion picture industry to obtain all of the economic benefits of copyright protection with none of the accompanying social responsibilities.*** Technological protection systems such as CSS that prevent the public from exercising their legitimate rights abuse the copyright bargain and should be exempt from the general circumvention ban.

EFF is not spending years in court merely to exonerate one or two individuals, or to enable distribution of a limited software prototype. We are here to establish the principle that the anticircumvention provisions cannot be used to eliminate fair use broadly throughout society. Nor can it be used to eliminate competitors who would offer legitimate access and copying capabilities to a major consumer market. Several lawmakers verified Congressional intent by insisting that the DMCA does not and is not intended to overrule the Betamax Supreme Court case. (6)

Two years ago, there could have been some doubt about whether the ill effects of the CSS system were

caused by the existence of the prohibition against circumvention. Certainly the movie studios spent a lot of energy lobbying for these DMCA provisions, but the evidence was circumstantial.

This year it is clear. The movie studios have made a clear and obvious causal connection in their own briefs, tying their motivation in building the CSS system to the technological measures that restrict access and fair use, and then tying those to the DMCA anti-circumvention statute.

The top eight movie studios they themselves declared, in their initial legal briefs:

"Each of the Plaintiffs relied on the security provided by CSS in manufacturing, producing and distributing to the public copyrighted motion pictures in DVD format. ... CSS is a technological measure that (a) effectively controls access to works protected by the Copyright Act, and (b) effectively protects rights of copyright owners to control whether an end user can reproduce, manufacture, adapt, publicly perform and/or distribute unauthorized copies of their copyrighted works or portions thereof.... Thus, [the DMCA] encourages technological solutions, in general, by enforcing private parties' use of technological protection measures with legal sanctions for circumvention and for producing and distributing products . . . that are aimed at circumventing" protection measures like CSS. (7)

To be sure, technology provides opportunity for benefit and abuse on behalf of all parties to the copyright bargain. Individuals engaging in piracy for commercial gain abuse intellectual property and harm society and creators. Likewise, the imposition of technology such as CSS onto the public that prevents creative works from readily passing into the public domain and restricts people from exercising their fair use rights is similarly abusive. The use of such abusive systems that do not uphold their end of the copyright bargain should not be backed-up by force of law, if copyright is to continue to serve as the engine of free expression.

Contrary to the fears expressed by the publishing industry, it is possible to preserve Constitutional values without destroying the value behind creative expression. In its justification for greater control over creative expression, the industry claims the new found phenomena of digital technology leaves copyright holders at the mercy of massive unchecked piracy. While the industry has loudly over-stated any potential harm it might face resulting from digital technology, it quietly looks the other way without mentioning the unprecedented power technology provides to copyright holders to control access and use over creative expression.

The copyright industries' glaringly self-interested suggestion that this committee exempt nothing from the circumvention ban ignores Congress' stated desire that DMCA not effect this nation's core Constitutional values -- such as the creation and dissemination of knowledge, freedom of speech, and promoting democratic values.

It is crucial that this Committee consider the longer societal view in deciding these important issues. If you don't have the ability to exercise your rights - then you don't have rights. There are greater issues at stake than mere economic interests of a few corporations. Unencumbered access to information is essential to knowledge creation, innovation, and the democratic discourse of a free and healthy society. We must diligently resist the content industry's push to build a legal system that optimizes our children for commercial consumption of creative expression at the expense of their imagination, education, and cultural enrichment.

I'd like to address the unfounded fears expressed by the content industry that any additional exemptions would violate the U.S.' WIPO Treaty obligations. Article 11 of the WIPO Copyright Treaty provides that: "Contracting parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures that are used by authors in connection with the exercise of their rights ... which are not authorized by the authors concerned **or permitted by law.**"

The DMCA went well beyond what was agreed to among contracting parties to the treaty by granting an additional and completely separate access right. Thus any additional exemptions on that right would have no effect on U.S. treaty obligations under WIPO. Additionally, the plain language of the treaty permits circumvention for fair use.

The Copyright Office should define an exempted class as "DVD movies". The movie studios stated in court filings that over 1 million copies of such works are sold every week. This is the class of works currently showing adverse effects.

It would be disingenuous to designate a class such as "DVD movies protected by a region coding system". Since consumers have flocked to hardware and software devices whose region codes can be disabled, and manufacturers are starting to rebel, the movie studios might decide to 'throw region coding overboard' in order to save the rest of their restrictive scheme. A designation that only applied to CSS works with region coding would still enable them to suppress competitors whose equipment provides fair use copying.

Similarly, the industry could evade a ruling against a class such as "DVDs protected by CSS" by merely switching to a different, but equally restrictive, protection system. An improved "CSS2" system already exists, and the industry is actively designing stronger one.

Therefore the entire class of "DVD movies" is threatened with adverse effects within the next three years, and should be exempted from the anti-circumvention provisions of the DMCA.

The movie studios stated in court filings in January that about 4,000 movie titles have been released in the US on DVD, that over five million DVD players have been sold, and that over 1 million copies of such works are sold every week. This is NOT an issue of "individual cases", but broadly implemented system that impacts all segments of society. A deliberately designed inability to play the work you purchased is no "mere inconvenience".

In the comments and testimony provided by the content industry before this proceeding, the charge continues to surface that no one has supplied any evidence of actual harm resulting from the use of such dangerous protection systems we discuss today. I need not remind the Committee of the hundreds of individuals who submitted comments complaining about their inability to simply view or make fair use of DVDs. Additionally, in testimony before this Committee, CCUM described a teaching method using DVD that has become unavailable to educators.

It is imperative that this proceeding recognize that the public's sheer inability to exercise its legal rights with respect to certain types of works because technological protections have been applied is by its mere existence a substantial harm perpetrated against the First Amendment. As the U.S. Supreme Court said in *Elrod v. Burns* 427 U.S. 347, 373 (1976), "The loss of First Amendment freedoms, for even minimal periods of time, unquestionably constitutes irreparable injury." I encourage the Librarian to weigh the Constitutional considerations into its determination about the societal harm.

Copyright's goal is to create a world full of creators with a rich and thriving public domain where creativity flourishes. In addition to legal protection designed to enable a market for works, creators vitally rely upon ready access to information including a vibrant public domain and the ability to engage in a wide range of legitimate uses including fair use. If copyright is to achieve its objective, society's true creators must continue to be allowed to build upon the works of their ancestors.

Because of the demonstrated widespread adverse impact on noninfringing use including fair use imposed by their technological restrictions, DVD movies should be exempt from Section 1201.

Thank you.

Footnotes:

1 http://www.eff.org/pub/Intellectual_property/MPAA_DVD_cases/Universal_City_Studios,_et_al_v._Reimerdes,_Corley_and_Kazan
Universal City Studios, et al v. Hughes

2 <http://www.tesco.co.uk/press/press-00feb17a.htm> &

<http://www.tesco.co.uk/press/press-00feb17b.htm>

3 <http://dvdcca.org/dvdcca/faq.html> & <http://dvdcca.org/dvdcca/rpc.html>

4 http://www.eff.org/pub/Intellectual_property/MPAA_DVD_cases/20000114_mpa_a_ny_attaway_pi_decl.html

5 http://www.eff.org/pub/Intellectual_property/MPAA_DVD_cases/20000503_def_linking_reply.html#Gross

6 *Sony Corp. v. Universal City Studios* 464 U.S. 417 (1984)

See: <http://www.virtualrecordings.com/betamax.htm>

7 http://www.eff.org/pub/Intellectual_property/MPAA_DVD_cases/20000114_mpa_a_ny_complaint.html

EXHIBIT N


Electronic Frontier Foundation

 Search:

Go

[Site Map](#) [Most Popular EFF Pages Today](#)

Active EFF Legal Cases and Efforts

[Our Legal Team](#) [Current Docket](#)

For a look at some of our recent cases please look at [Recent Legal cases](#)

Digital Millennium Copyright Act (DMCA) & DeCSS

The Digital Millennium Copyright Act ("DMCA") was passed in 1998 over the objections of many people, including scientists, librarians and cryptographers.

§1201 of the DMCA bans devices that enable circumvention of technical protection systems, and also prohibits the circumvention of technological protection or access control measures.

The DMCA is *very* bad news because it destroys the delicate balance between copyright and First Amendment too heavily toward the copyright holders. This is because circumvention of technical protection measures is necessary in order to make fair use, do scientific research, and make many kinds of ordinary, legal uses of DVDs, such as playing them on Linux machines. (See Staff Attorney Robin Gross's [insight](#) into how, overnight, millions of Americans became criminals under the DMCA.) (See also Professor and EFF Board Member Pam Samuelson's [paper on why the DMCA is flawed](#).)

More recently the congress led by Senator Fritz Hollings in the Senate has been trying to strengthen the DMCA to give even more power to copyright holders and further weaken the public right to the intellectual commons. This newest attempt is known as the "

" (SSSCA). See our alert at:

http://www.eff.org/alerts/20010921_eff_sssca_alert.html. In response to this threat, which has slowed due to some of the major players complaining, EFF wrote this [letter to the Senate Commerce Committee](#). It is important to monitor this situation closely, as all the expensive court battles that we can wage cannot stop the immediate damage of terrible legislation.

The Trusted Computer Platform Alliance (TCPA) has recently made news with its system for locking down everyone's computers using integrated DRM mechanisms. For an excellent background on this see [Dr. Ross Anderson's FAQ](#).

See also: stoppoliceware.org;

Letter from [the ACM](#) (Association for Computing Machinery); and this article in [CNet News](#).

(Updated June 25, 2002)

- [Universal v. Reimerdes](#) (a.k.a. the NY DVD case)

Eight major motion picture studios brought a suit under the DMCA against defendant, *2600 Magazine* to enjoin it from publishing or linking to DeCSS, a computer program that circumvents the encryption on DVDs, called CSS. DeCSS was developed to help enable DVDs to be

Subscribe to the
EFF Action Center

Got a domain
name (UDRP)
problem? Click
here.

played on computers running the Linux system. It also allows the constitutionally protected fair use of DVDs, which is otherwise prevented by the encryption.

The 2nd Circuit Court of Appeals affirmed, EFF moved for an en banc hearing in NY; En banc denied
(Updated June 13, 2002)

At issue: Whether fair use, free software, linking and reverse engineering will survive the digital age.

EFF's role: defending 2600 along with pro bono lead counsel Dean Kathleen Sullivan of Stanford Law School.

- **DVD-CCA v. Bunner** (the CA DVD case)

The DVD Copy Control Association (DVD-CCA), a newly formed mouthpiece of the MPAA, is suing dozens of unnamed individuals who put DeCSS on their Web sites in various places around the country and around the world. The case alleges that plaintiffs mis-appropriated trade secrets when they published DeCSS.

On March 28, 2002 the DVD-CCA filed its brief to have the preliminary injunction against Andrew Bunner's posting of DeCSS code reinstated. On May 22, 2002 Bunner answered, and on June 11, 2002 DVD-CCA filed their reply. We are now awaiting a date for oral argument from the court which could take up to 18 months.

At issue: Same First Amendment implications as the NY case; also whether the pretense of "trade secrets" will enable companies to punish those engaged in lawful reverse engineering.

EFF's role: Pay for and coordinate the defense in this case.
(updated June 14, 2002)

- **U.S. v. Elcomsoft** (formerly *U.S. v. Sklyarov*)

The case involves Advanced eBook Processor (AEBPR) software legally developed by Dmitry Sklyarov, in Russia, for his Russian employer Elcomsoft. According to the company's website, the software permits eBook owners to translate from Adobe's secure eBook format into the more common Portable Document Format (PDF). The company maintains that the software only works on legitimately purchased eBooks. Dmitry Sklyarov was arrested when he came to the United States to give a talk on computer security and the case has proceeded from there.

Currently the U.S. has dropped charges against Dmitry in return for testimony which he would have provided for Elcomsoft anyway. Dmitry is presently back in Russia. On March 27, 2002, Judge Whyte denied Elcomsoft's motion to dismiss for lack of subject matter jurisdiction. Then on May 8, 2002 Elcomsoft's motion to dismiss on 1st amendment grounds was also dismissed. We are currently waiting for the trial on the merits of the case.

At issue: Whether it is legal to build software tools with substantial non-infringing uses, and whether U.S. law supersedes that of other sovereign nations.

EFF's role: EFF is currently acting as amicus in this case. EFF amicus brief
(updated June 14, 2002)

Peer-to-Peer (P2P) Systems

As part of our continuing efforts to spur discussion about the legal issues involved in peer-to-peer systems, we offer EFF Staff Attorney Robin Gross's _____, and a white paper summary written by Fred von Lohmann, formerly a fellow at the Berkeley Center for Law and Technology and now EFF's Senior IP Counsel, discussing post-Napster [legal tips for peer-to-peer developers](#). We urge any developers of such systems who have further questions about the legal and policy issue surrounding P2P to talk to us directly.

- **MGM v. Grokster** This case is about the freedom of technologists to innovate and the public's right to communicate. Twenty-eight of the world's largest entertainment [companies have sued](#) MusicCity, the Nashville-based developer of the leading peer-to-peer communications software Morpheus, in federal court in Los Angeles. Morpheus is a communications tool that allows users to connect with each other and share information of all kinds. The entertainment companies claim that MusicCity should be held responsible for the alleged copyright infringements committed by Morpheus users. On Nov. 18, 2001 there was an [additional complaint](#) filed by the National Music Publishers Association. On Jan 22, 2002, the MusicCity defense team filed a [motion](#) for partial summary judgement in the case. Relying on the famous Supreme Court case relating to the Sony Betamax VCR, the motion points out that the Morpheus software is capable of substantial non-infringing uses, and thus [cannot be banned](#) under copyright law. The motion will be heard in Los Angeles on March 4, 2002. (In a [related case](#) Paramount filed suit against ReplayTV over whether allowing the removal of commercials is fair use.)

At issue: Whether the entertainment industry, which previously tried to ban the VCR, is able to outlaw the technology that is the next killer app. of the Internet.

EFF Role: To act as co-counsel, raise money and [publicize](#) the case.

OnLine Activism

- EFF has been developing materials to inform online activists of the state of the law concerning their protest activities online. Set to be launched in summer, 2002, the website will augment presentations that EFF legal staff have given at several conferences of and about activists, including the 2002 Computers, Freedom & Privacy Conference, the Berkman Center's Cybertree Conference in May, 2002 and the Ruckus Society Tech Toolbox Camp in June, 2002.

At issue: Educating online activism about the state of the law

EFF's Role: EFF's legal team is working with Professor Anita Ramasastry and her students at the University of Washington and Nancy Chang of the Center for Constitutional Rights to develop the website and ongoing presentations.

Consumer Fair Use

Copyright law embodies a bargain: Congress gave copyright holders a set of six exclusive rights for a limited time period, and gave to the public all remaining rights in creative works. Up till very recently it was assumed that when a work was no longer covered by copyright it would enter the public domain or "intellectual commons" as it is called by Professor [Lawrence Lessig](#). Now with digital rights management (DRM) technology corporate rights holders threaten to take the building blocks of future ideas and technologies out of most peoples hands. EFF is fighting to maintain fair use as a tool to ensure an enlightened future.

- [Newmark, et al. v. Turner, et al.](#)

ReplayTV: Responding to both the lawsuit brought against ReplayTV and the industry's public claims that these actions are "theft," five customers of ReplayTV, represented by the Electronic Frontier Foundation (EFF) and Ira Rothken of the Rothken Law Firm in San Rafael, filed a federal lawsuit in Los Angeles asking the court to rule that their use of the ReplayTV device is legal under copyright law.

At Issue: fair use in the digital era, specifically the fair use rights secured by the Sony Betamax decision allowing home taping and manipulation of content for personal use.

EFF Role: Representing the five plaintiffs along with Ira Rothken of the Rothken law firm. (Updated June 18, 2002)

Reverse Engineering

Reverse engineering is taking an object or computer program apart to see how it works or functions, in order to be able to make the object oneself, to interact with the object, or give it additional functionality. It was a common practice in earlier mechanical industries that is now frequently used on computer hardware and software. It is also a practice that is under attack as entrenched industries try to keep their secrets and limit competition. The Digital Millennium Copyright Act (DMCA) has given a strong push in this direction, given the weak encryption that protects some products, the only thing that can protect them is a law which takes away a former fair use.

- [Blizzard v. BnetD](#)

Davidson & Associates d.b.a. Blizzard Games v. Internet Gateway (Bnetd case): Game maker Blizzard Entertainment, along with its parent company Vivendi Universal Games, has sued a small Internet Service Provider, its owner and several volunteer software developers for developing and distributing free software that emulates Blizzard's free Battle.net gaming service. The bnetd software allows Blizzard game purchasers online or on a local area network to chat, find competition, and start multiplayer games. A group of volunteers created the BnetD project for Blizzard games because Blizzard's Battle.net service was undependable and had limited functionality.

At issue: The right to do reverse engineering to create inter-operable software products.

EFF Role: representing the defendants along with Fish & Richardson and Thomson Coburn. (Updated June 18, 2002)

Anonymity/Pseudonymity

The right to speak and post anonymously online is being threatened by companies and individuals who have begun using civil subpoenas to demand that the speaker's Internet service provider reveal his or her identity. Unlike criminal warrants, civil subpoenas do not require showing of probable cause or any other court review. The cases we are currently working on involve people who anonymously posted comments on chatrooms for publicly traded companies and have subsequently been targeted by employers or other parties who want their identities revealed.

- [HighSchoolNation.com](#)

HighSchoolNation.com: EFF, along with the ACLU of Northern California and San Francisco's Farella, Braun & Martel are representing a high school student who was threatened with expulsion, criminal charges and civil charges for hosting a website where students could anonymously rate their teachers. The school and the local police attempted to convince

the student to turn over identifying information about posters of allegedly defamatory and threatening messages and to disable the website. EFF pointed out that, under the Electronic Communications Privacy Act, the student is prevented from turning over this information without a subpoena and that under the Communications Decency Act section 230 he cannot be held civilly liable for the allegedly defamatory messages of others.

At issue: Protection of anonymity of speakers on a website forum; webmaster protection for hosting a free speech website.

EFF Role: Legal representation of the high school student.

ICANN

- Auerbach v. ICANN

Auerbach v. ICANN: EFF represents a member of the ICANN Board of Directors in a lawsuit that seeks to force ICANN management to grant him some reasonable access to corporate records. Karl Auerbach, the North American Elected Director of the Internet Corporation for Assigned Names and Numbers (ICANN) began asking for corporate records in December 2000, shortly after he was elected to the Board. ICANN management dragged its feet for nine months, then issued a new "policy" -- never brought before the Board for discussion or vote -- requiring Auerbach to sign a non-disclosure agreement that placed Auerbach's ability to discuss the records at the discretion of ICANN management.

At issue: ICANN's accountability to the public begins with accountability to its own Board of Directors

EFF Role: Counsel to Mr. Auerbach along with Attorney James Tyre. (Updated June 18, 2002)

Domain Name Trademark Disputes

- CNN v. CN news

CNNNews.com: 4th Circuit. EFF Filed an amicus brief arguing that the rem provisions of Anti-Cybersquatting Protection Act (ACPA) should not apply to allow jurisdiction in Eastern District Virginia over domain (China news) registered with Chinese Registrar simply because some of Verisign's servers are located there. Also pointed out that since Verisign itself is no longer located in Virginia--its headquarters has moved to California--jurisdiction in Virginia is even more tenuous.

At Issue: Jurisdictional issues in the domain resolution process.

EFF Role: EFF wrote an amicus brief.

Censorship Laws

- Ashcroft v. ACLU a.k.a. ACLU v. Reno II (the Child Online Protection Act [COPA] case)

COPA makes it a federal crime to "knowingly" communicate online material considered "harmful to minors" (not based on where you live, but in the most conservative jurisdictions anywhere in the country). COPA was found unconstitutional by the U.S. District Court for the Eastern District of Pennsylvania, which enjoined enforcement of COPA for the time being. The government appealed that decision to the U.S. Court of Appeals for the Third Circuit, which affirmed -- but for a different reason than had the district court. The district court had found that COPA

was unlikely to survive "strict scrutiny" because it was not the least restrictive means of preventing minors from accessing "harmful to minors" material. In contrast, the Third Circuit held that COPA was substantially overbroad because its definition of "harmful to minors" material relied on "contemporary community standards," and using geographical "community" standards would permit the least tolerant communities to decide what could be published on the Internet. The government then asked the U.S. Supreme Court to review the Third Circuit decision. On May 13, 2002, the Supreme Court vacated the Third Circuit's decision in a very narrow ruling that featured five separate opinions. Most important, the injunction against COPA's enforcement remains in effect. Also, the ruling did not disturb any of the district court's grounds for decision. The Supreme Court only found that the record did not support the Third Circuit's decision, and sent the case back ("remanded") for further proceedings. Note that the Supreme Court did not really decide whether the use of "community standards" on the Internet is constitutional. Only the three justices who joined the plurality opinion (Rehnquist, Thomas, and Scalia) found that geographic community standards can or should be applied to Internet speech without considering the "least tolerant community" problem. Each of the other six justices, some more strongly than others, expressed concern that the use of local community standards will cause problems for regulation of obscenity on the Internet. The case is now again before the Third Circuit and the government filed its brief on July 24, 2002. Our brief, which is being drafted by the national ACLU, is due Aug. 22. The case, which was titled *ACLU v. Reno II* in the trial court, is now titled *Ashcroft v. ACLU* (because of the recent change in DoJ administration). (updated August, 2002)

At issue: Our online First Amendment rights are threatened by this legislation in much the same way they were with its predecessor, the defeated Communications Decency Act (CDA).

EFF's role: The EFF and the ACLU have established a joint litigation strategy to combat COPA.

- ***Nitke, et al. v. Ashcroft, et al.*** (Communications Decency Act (CDA) case)

This case challenges the obscenity provisions of the CDA, which were not at issue in the first CDA case, *Reno v. ACLU* (1997). The plaintiffs are Barbara Nitke, an artist, the National Coalition for Sexual Freedom and the National Coalition for Sexual Freedom Foundation. They ask for a preliminary injunction, arguing that the use of "contemporary community standards" to determine obscenity on the Internet will inevitably result in the least tolerant communities' determining what can be published on the Internet. The case is being heard by a three-judge district court in the Southern District of New York. The plaintiffs are represented by John Wirenius of Leeds, Morelli and Brown in New York.

The case is being argued on Aug. 29, 2002 at 3 p.m. in the Southern District of New York. (Updated: August 2002)

At issue: Whether defining obscenity in terms of local geographic community standards violates the First Amendment when applied to the Internet.

EFF's role: EFF filed an amicus brief on behalf of the plaintiffs. (updated August 2002)

Censorware (Internet content blocking, filtering, ratings & labelling)

- **American Library Association v. United States**

American Library Ass'n, Inc. v. Ashcroft (Children's Internet Protection Act (CIPA) case)

In December 2000, Congress passed CIPA, which forces libraries and schools that receive certain federal funds to use censorware. The American Library Association (ALA) and a variety of other plaintiffs (libraries, library patrons, and website owners) filed two lawsuits challenging CIPA's constitutionality as to libraries. The two cases were consolidated.

After an eight-day trial, a three-judge district court in the Eastern District of Pennsylvania held on May 31, 2002, that CIPA violates the First Amendment. *American Library Ass'n, Inc. v. United States*, 201 F.Supp.2d 401 (E.D.Pa. 2002) [post/link]. The court found that censorware overblocks protected speech and underblocks obscenity, child pornography, and material harmful to minors. The court also found that there are less restrictive alternatives that will further the government's legitimate interests.

The government announced its intention to appeal on June 20, 2002, and must file its jurisdictional statement with the U.S. Supreme Court by Sept. 6, 2002. Plaintiffs' response will be due about 30 days later.

For more information on why CIPA is unconstitutional, see EFF's [CIPA analysis](#). To find out what you can do to help stop censorware, join EFF's [Blue Ribbon Campaign for Free Speech](#). (Updated: August 2001)

At issue: Mandatory blocking software denies individuals access to constitutionally protected materials.

EFF's role: EFF is co-counsel on the case and EFF member James Geringer is a library patron plaintiff. (Updated August 2002)

Consumer Privacy

Government Surveillance

- **Konop v. Hawaiian Airlines**

In this case a Hawaiian Airlines executive impersonated an airline pilot in order to gain access to a private, password-protected Web site established by Hawaiian Airlines pilot Robert Konop as a confidential forum for criticizing labor-management issues. Once there, the Hawaiian executive acquired the contents of Konop's communications with registered users of his Web site. The [Ninth Circuit decision](#) held, among other things, that Hawaiian "intercepted" Konop's communications under Title I of the Electronic Communications Privacy Act ("ECPA"). EFF supports the decision, which rejected the erroneous interpretation of "interception" in *Steve Jackson Games Co. v. U.S. Secret Service*.

The defendant, Hawaiian Airlines, petitioned the Ninth Circuit for rehearing. EFF filed an amicus brief in support of Konop, as did the National Association of Criminal Defense Lawyers. The U.S. Department of Justice filed an amicus brief in support of Hawaiian Airlines.

On Aug. 28, 2001, the Ninth Circuit withdrew its original decision while

finding Hawaiian Airlines's petition for rehearing moot. A new decision has not yet been issued (yes, it has been a long time).

At issue: In order to protect 4th Amendment rights, acquisition of private Web site communications should be treated as an "interception" under ECPA.

EFF's role: EFF filed an amicus brief on behalf of Web site operator Konop. (Updated August 2002)

E-mail/Trespass to Chattels

E-mail spam is a result of the Internet age that everyone wants to get rid of, however the issue is more complex than it seems.

- **Intel v. Hamidi**

When Ken Hamidi was fired by Intel Mr. Hamidi responded by e-mailing his side of the dispute to the Internal e-mail list. Intel sued and got him enjoined, eventually getting a judgment for trespass to chattels. This is a dangerous precedent and EFF is supporting the appeal to overturn the decision

At issue: Whether virtual real estate should be considered the same as physical real estate.

EFF's role: EFF submitted a brief Amicus Curiae to the California Supreme Court advocating the reversal of this trespass theory. (Updated August 2002)

SLAPP Suits

One of the favorite tactics of well financed entities when facing embarrassing information is to seek to silence the adversary through expensive lawsuits. (Recent cases only)

Copyright and ISP Liability

Search: [Site Map](#) [Most Popular EFF Pages Today](#)

Please send any questions or comments to webmaster@eff.org.

EXHIBIT O

CALIFORNIA LAWYER

JUNE 2002

FAMILY COURTS AND THE INTERNET

California

LAWYER

JUNE 2002 \$6

the Net Effect

Disaffected family court litigants use the internet to get what they can't get in court.

REPLAY TV

The latest gadget turns into the next big copyright battle

ABOUT FACE

One lawyer's struggle with mental illness

What to say when someone asks, "HOW CAN YOU DEFEND HIM?"

*****PIRM**CAR-RT LOT**C-017



081093
ARTHUR F SILBERGELD
PROSKAUER ROSE LLP
2043 CENTURY PARK E #1290
LOS ANGELES CA 90067-3206

20

3888
24

REPLAYTV ZAPS ADS AND PERMITS SHOW SWAPPING.

GET READY FOR THE NEXT BIG COPYRIGHT BATTLE

The VCR has been, by all accounts, one of the most successful consumer electronics products of the past three decades. And though one can be found perched near a TV set in almost every American household, the venerable VCR, with its analog tapes and clock blinking "12:00," is looking a bit tired in our digital, Internet-ready age.

Into the breach have stepped two innovative Silicon Valley companies—TiVo and Sonicblue—intent on reimagining the VCR and changing the way Americans experience television with the help of the DVR, or digital video recorder, a new breed of device that takes time-shifting to a new level. Consider Sonicblue's ReplayTV RTV 4040, shipping now for \$700, or the Philips HDR312 TiVo Personal Video Recorder, available for \$300. Both units download the electronic equivalent of *TV Guide* into electronic memory, so there is no need to program the unit, per se—you simply choose the programs you want to record from a simple menu, and the DVR does the rest. If the special musical episode of *Buffy the Vampire Slayer* goes almost ten minutes over its time slot (it did), your DVR knows and automatically adjusts the recording time. You can even have your DVR seek out and record programs by actor, director, or genre—collect all of Woody Allen's films, say, or create your own "all Westerns" station.

The ReplayTV DVR, however, provides two additional features that its competitors have not had the courage to offer for fear of attracting Hollywood's ire. First, the ReplayTV offers Commercial Advance, a feature that automatically skips commercials for recorded shows (TiVo offers only fast-forward, like most VCRs). Second, the ReplayTV connects to your home computer network and broadband Internet connection, enabling you to send recorded programs to other ReplayTV units in your house and, more important, to other ReplayTV owners over the Internet. Now, if a fellow ReplayTV owner emails you about last night's episode of *Law & Order*, you can download it from his or her ReplayTV if you missed it.

These last two features snagged the litigation trip wire and brought down the wrath of Hollywood. In the fall of

2001, around the time the ReplayTV 4000 line of products was launched, four copyright infringement lawsuits were filed against the ReplayTV and its manufacturer, Sonicblue, in federal district court in Los Angeles. The lawsuits all seek injunctions aimed at sweeping the ReplayTV off the market.

The plaintiffs arrayed against the ReplayTV include every major movie studio, every major television network, and several major cable networks. The law firms representing the plaintiffs are also among some of the nation's best known—Wilmer, Cutler & Pickering; Proskauer Rose; McDermott, Will & Emery; and O'Melveny & Myers.

These cases are not unlike the 1979 Betamax lawsuit, in which two movie studios filed a copyright infringement lawsuit seeking damages and an injunction against manufacture and distribution of Sony Betamax VCRs. The suit maintained that Betamax VCRs allowed consumers to make unauthorized copies of television programs. In fact, Jack Valenti, top lobbyist for the Motion Picture Association of America, went so far as to declare that "the VCR is to the American film producer and the American public as the Boston [S]trangler is to the woman home alone." Fortunately for both American film producers and the American public, a 5-to-4 majority of the Supreme Court ultimately sided with Sony (*Sony Corp. v Universal City Studios, Inc.* (1984) 464 US 417), and the VCR swept the nation and the world. The result, ironically enough, was a torrent of new revenue for Hollywood in the form of prerecorded videotape sales.

But Hollywood never warmed to time-shifting—the practice of recording television for later viewing. So in 2001 the Hollywood forces gathered for another assault, aimed at rolling back the effect of the Supreme Court's ruling in the Betamax case. This time the target would be a new, improved time-shifting device, the ReplayTV DVR.

According to one of the complaints, the ReplayTV DVR represents "an unlawful plan by defendants to arm their customers with—and continuously assist them in using—unprecedented new tools for violating plaintiffs' copyright interests...." In the eyes of the plaintiffs, the ReplayTV DVR threatens the financial foundations of the television and film industries. Though stopping short of Valenti's famous Boston Strangler quote, the complaints frame the ReplayTV DVR as a looming threat to the multibillion-dollar film and TV industry.

BY FRED VON LOHMANN
FRONTIER FOUNDATION

Fred von Lohmann is the senior intellectual property attorney for the Electronic Frontier Foundation, a nonprofit that seeks to protect civil liberties in the digital age.

First, ReplayTV owners skip commercials, undermining the basis of free television in America (never mind that a majority of Americans now pay for cable). Second, DVRs could undermine the notion of prime time, with its premium rates for ad spots. After all, what difference does it make whether a show is aired at 8:00 P.M. or 3:00 A.M.? Either way, it'll be waiting for you on your ReplayTV whenever you're ready to watch it. Third, the ability to share programs with other ReplayTV owners creates a vast private archive of television. Rather than purchasing season five of the *X-Files* on DVD, ReplayTV owners might just rely on the reservoir of *X-Files* episodes amassed by other ReplayTV owners. All the comfortable assumptions of television executives appear to be upset by this upstart innovation.

But pity not the poor Hollywood executive. Technological change disrupts the comfortable assumptions of executives in virtually every industry every day.

It is hard to see why Hollywood's business models should be exempt from the disruptive effects of innovation any more than the railroad industry should have been rescued from the internal combustion engine. But more significant, what's bad for today's Hollywood executive will almost certainly be a boon to tomorrow's copyright owners. A century of experience teaches that new technologies, no matter how disruptive in the short run, have invariably expanded the revenue pie for copyright owners in the long run.

At the dawn of the 20th century, for example, the music industry was dominated by sheet-music publishers. The rise of recording technology effectively wiped them out, giving birth to the modern (and much larger) music industry. The revolutions brought by radio broadcasting, color television, cable television, and the VCR each taught the same lesson.

But to return from the realm of policy to the lawyer's question, does it violate copyright law? Just as in the Sony Betamax case, the answer turns on two distinct, but related, questions. First, are ReplayTV owners violating copyright law when they time-shift and share programs broadcast on television? The fact that Hollywood has sued only ReplayTV's maker, rather than ReplayTV users, raises the second question: Can Sonicblue be held liable for infringements that may be committed by its customers?

The first question is destined to gather the better sound bites. In the words of Laurence Pulgram of Fenwick & West in San Francisco, who is leading the defense of the ReplayTV, "If dodging commercials is against the law, you'd have to strap people in their chairs and snatch the remote out of their hands." Andy Wolfe, chief technical officer of Sonicblue, puts the matter more bluntly: "Obviously the networks don't like it if I go to the bathroom during a commercial, but I am still allowed to do it." After all, the Supreme Court held that time-shifting constituted a "fair use" under copyright law,

notwithstanding the fast-forward button on Sony's Betamax VCR. An automatic commercial-skipping feature, in fact, has been available on certain higher-end analog VCRs for several years, without legal protest from copyright owners.

As for the Send Show feature that allows one ReplayTV owner to send a show to another, this ability is limited to a list of 15 people, and it blocks the sharing of pay-per-view content. As a result, this ability is not terribly different from the ability to swap copies of last night's *ER* episode with a coworker on videotape, or the ability of AOL subscribers to exchange digital files through AOL's Instant Messenger service.

But it is the second question—when can a technology vendor be held liable for the infringements of its customers?—that is the more important one, with implications for virtually all technology companies. If these companies can be held liable for every infringement committed by a customer, on pain of ruinous damage awards and injunctions that sweep products off the market, innovation would grind to a halt. Xerox, for example, would never have built a photocopier, nor would Netscape have shipped a Web browser. In 1984 the Supreme Court in the Betamax case struck a more sensible balance: A technology vendor will not be liable for the infringements of its customers so long as its products are "capable of substantial noninfringing uses." 464 US at 442.

In the ReplayTV litigation, Hollywood is arguing for a very different rule, urging the court to hold Sonicblue liable for copyright infringement because "they could have designed the ReplayTV 4000 to prevent or greatly limit" the infringing activities of ReplayTV owners. This "could have designed it differently" rule would be devastating to technology companies, effectively deputizing them into the role of copyright police. Technology companies would be put to a Hobson's choice—either take your chances proving a negative in court ("Your Honor, there was nothing more we could have done to protect copyrights") or invite Hollywood's lawyers into engineering meetings, in hopes of securing prior approval for new technologies.

ReplayTV is already getting a glimpse of this dystopian alternate reality, a reality where copyright litigators pick through design decisions after the fact, looking for any evidence that the engineers failed to take an opportunity to add more "policeware" to the product. According to Pulgram, the plaintiffs have already demanded to see all the internal design documents that led up to the ReplayTV 4000 series, seeking evidence that the product could have been designed more to Hollywood's liking.

Technology companies take note—this case is not just about whether couch potatoes can skip commercials. Whatever the outcome, it could influence not just the future of television but the course of innovation for decades to come. ■

Why should Hollywood be exempt from the disruptive effects of innovation any more than the railroad industry was?

EXHIBIT P

August 17, 2002

Record Labels Want 4 Internet Providers to Block Music Site

By AMY HARMON

Testing out a tactic to combat online piracy, a group of record companies asked a judge yesterday to order four major Internet service providers to block Americans from viewing a China-based Web site that offers thousands of copyrighted songs free of charge.

The 13 record labels that filed the suit in Federal District Court for the Southern District of New York in Manhattan say the site, Listen4ever .com, is "even more egregious" than the music-sharing service Napster, which was shut by a court order.

But in the Napster case, the recording industry sued Napster itself. The new action is the first time record companies have sought to compel the companies that control the Internet backbone to intervene. The four companies named in the suit are AT&T Broadband, Cable and Wireless, the Sprint Corporation and UUNet Technologies. The record labels in the lawsuit include Sony Music Entertainment, the Universal Music Group and RCA Records.

The lawsuit invokes an untested provision of a 1998 federal law, the Digital Millennium Copyright Act, that allows a court to order Internet providers to take limited steps to block offshore sites that violate United States copyright laws. Sarah Edler, a spokeswoman for AT&T Broadband, said the company had never before been asked to block access to a foreign site.

David Farber, a University of Pennsylvania computer scientist and an early architect of the Internet, filed an affidavit in the case, saying it would be relatively easy for the Internet companies to block the Internet address of the Web site without disrupting other traffic.

"It's not a big hassle," Mr. Farber said. "There's no way to stop everybody, but a substantial number of people will not be able to get access."

The companies named in the suit declined to comment. But a person who works closely with Internet providers said that they were concerned about how easy it

EXHIBIT P
PAGE 112

was for a Web site to change Internet addresses. If copyright holders began asking them to block sites in large numbers, and to keep track of every new address, it could divert resources from running regular Web traffic.

Pirate sites that set up in countries that do not enforce United States copyright laws are a growing problem for the music and movie industries as they try to control the free exchange of their material online.

The Listen4ever site is written in English and appears aimed at an American audience. Yesterday, it was possible to download songs by Bruce Springsteen and music from the soundtrack of "Blue Crush."

The site thanks a list of "top uploaders" under a note that reads:

"Attention: all music files here are uploaded by lots of music fans for sharing free. These music files are only for trial listening, please don't use these for business purpose and delete these files after you listen, thanks! (support your favorite singers, please buy their CDs)."

An e-mail message sent to a Yahoo e-mail account, the only contact information on the site, was bounced back. The recording companies said the only information they were able to find was that the domain name appeared to have been registered to a person in Tianjin, China.

Fred von Lohmann, a lawyer with the Electronic Frontier Foundation, a civil liberties group that monitors digital copyright issues, said that the law allowed a court to refuse the copyright holder's request if it decided there was a less burdensome way to prevent the copyright infringement.

"Wouldn't it be better to get an injunction from a Chinese court to punish the people behind this?" Mr. Von Lohmann said. "Are we going to have a situation where rather than going after the actual wrongdoers we just go block all these sites?"

[Copyright 2002 The New York Times Company](#) | [Permissions](#) | [Privacy Policy](#)