

1 RUSSELL J. FRACKMAN (State Bar No. 49087)
JEFFREY D. GOLDMAN (State Bar No. 155589)
2 MITCHELL SILBERBERG & KNUPP LLP
11377 West Olympic Boulevard
3 Los Angeles, California 90064-1683
Telephone: (310) 312-2000
4 Facsimile: (310) 312-3100

5 JEFFREY N. MAUSNER (State Bar No. 122385)
BERMAN, MAUSNER & RESSER
6 11601 Wilshire Boulevard, Suite 600
Los Angeles, California 90025-1742
7 Telephone: (310) 473-3333
Facsimile: (310) 473-8303

8 DANIEL J. COOPER (State Bar No. 198460)
9 PERFECT 10, INC.
72 Beverly Park Drive
10 Beverly Hills, California 90210
Telephone: (310) 205-9817
11 Facsimile: (310) 205-9638

12 Attorneys for Plaintiff
13
14

15 UNITED STATES DISTRICT COURT
16 CENTRAL DISTRICT OF CALIFORNIA

17 PERFECT 10, a California corporation,
18 Plaintiff,

19 v.

20 GOOGLE, INC., a corporation; and
21 DOES 1 through 100, inclusive,
22 Defendants.

CASE NO. CV 04-09484 AHM (SHx)

**DECLARATION OF ELENA
SEGAL IN OPPOSITION TO
MOTION OF ELECTRONIC
FRONTIER FOUNDATION FOR
LEAVE TO FILE BRIEF *AMICUS
CURIAE***

Date: November 7, 2005
Time: 10:00 a.m.
Crtrm: The Honorable A. Howard
Matz

[illegible]

3

4
5
6
7
8
9

11
12
13

15
16
17
18

20
21
22
23

25
26
27
28

1 information as to the amount of any such donations, or as to any other of its donors
2 that may be related to, or have an interest in this litigation. A true and correct copy
3 of the e-mail from Jason Schultz, dated September 30, 2005, in which this response
4 is provided, is included within Exhibit A attached hereto.

5
6 6. I have examined the EFF's website (eff.org), and have found
7 that, upon entering a search term in the Search box provided in the upper right-
8 hand corner of the screen, and clicking the "Search EFF" button, the screen that is
9 returned displays the Google logo at the top of the screen, and displays a bar
10 entitled "Sponsored Links" down the right-hand side of the screen. A true and
11 correct copy of a printout of the screen returned upon entering the search term
12 "copyright" in the search box on eff.org, and clicking the "Search EFF" button on
13 October 22, 2005 is attached hereto as Exhibit B.

14
15 7. Attached hereto as Exhibit C is a true and correct copy of an
16 article that I printed from the eff.org website on October 20, 2005, entitled "How
17 Not To Get Sued By The RIAA For File-Sharing." It is located at
18 <http://www.eff.org/IP/P2P/howto-notgetsued.php>.

19
20 8. Attached hereto as Exhibit D is a true and correct copy of an
21 article that I printed from the eff.org website on October 20, 2005, entitled "IAAL
22 [I am a lawyer]: What Peer-to-Peer Developers Need to Know About Copyright
23 Law." It is located at http://www.eff.org/IP/P2P/p2p_copyright_wp_v4.pdf. From
24 page 11 of the article, it provides advice to peer-to-peer developers as to how to:
25 "(1) reduce the chance that your project will be an easy, inviting target for
26 copyright owners; and (2) minimize the chances that your case will become the
27 next legal precedent that content owners can use to threaten future innovators."

9. Attached hereto as Exhibit E is a true and correct copy of an article that I printed from the eff.org website on October 19, 2005, entitled "A History of Protecting Freedom Where Law and Technology Collide." It is located at <http://www.eff.org/about/history.php>. On page 3 of this article, the EFF states that "[t]he trend has been for industry to use a combination of law and technology to suppress the rights of people using technology."

10. Attached hereto as Exhibit F is a true and correct copy of an article that I printed from the CNet news website (news.com.com) on October 22, 2005, entitled "Google Cache Raises Copyright Concerns." It is located at http://news.com.com/2102-1032_3-1024234.html?tag=st.util.print. On page 3 of this article, Fred von Lohmann, on behalf of the EFF, states that "Google is making copies of all the Web sites they index and they're not asking permission. . . . From a strict copyright standpoint, it violates copyright." He is further quoted, on page 4, as saying: "Most people agree that the caching exception in the DMCA is obsolete, . . . I don't think it would cover Google's cache. Google is not waiting for users to request the page. It spiders the page before anyone asks for it."

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

Executed this 24th day of October, 2005, at Los Angeles California.

Elena Segal
Elena Segal

EXHIBIT A

Frackman, Russell

From: Jeff Mausner [jeffmausner@bmrlaw.com]
Sent: Monday, October 03, 2005 12:03 PM
To: Jason Schultz
Cc: Zada, Norm; Dan Cooper; Frackman, Russell; Goldman, Jeffrey
Subject: RE: Consent To File Amicus in Perfect 10 v. Google

Jason: Perfect 10 opposes the EFF filing an amicus brief in support of Google in this case. First, EFF has received significant funding from Google, both directly and indirectly. As you stated, EFF has received \$50,000 directly from Google. I suspect that the amount it has received from Google in connection with matching funds from employees is even greater. Will you provide that figure to us?

Second, there is little doubt what position your organization will take. EFF always supports infringers. EFF not only takes the side of those who facilitate the infringement (like Napster and Grokster), but even tries to impede discovery of the actual direct infringers. I recollect that when EFF was supporting Napster and Grokster, your position was that the record companies should not proceed against Napster or Grokster but should instead proceed directly against the direct infringers who were using this technology to swap infringing files. However, when the record companies sought to subpoena information about the direct infringers, the EFF opposed those subpoenas. EFF not only acts as an amicus for infringers, but has served as counsel of record for the infringers in the Grokster case. Have you acted as counsel of record for any other contributory or direct infringers?

Third, Google, which is one of the highest market cap companies in the world with thousands of employees, is certainly capable of asserting a position contrary to Perfect 10's. Google has, in fact, raised the public interest in its opposition to the preliminary injunction, so there is no reason for EFF to have to assert it. Amazon, probably the largest retailer on the Internet, also has filed a brief opposing Perfect 10's Motion for Preliminary Injunction. These multi-billion dollar corporations have adequate representation, and there is no need for your organization to repeat their arguments.

Fourth, EFF's attempt to file a brief in this case will only delay things, since the hearing is set for November 7. If EFF filed an amicus brief, Perfect 10 would have to respond to it, and possibly other amicus briefs would be filed. This is a motion for preliminary injunction, and the hearing should not be delayed.

Please feel free to call me if you have any questions or would like to discuss this further.

Sincerely, Jeff Mausner.

-----Original Message-----

From: Jason Schultz [mailto:jason@eff.org]
Sent: Friday, September 30, 2005 4:09 PM
To: Jeff Mausner
Cc: Jason Schultz
Subject: Re: Consent To File Amicus in Perfect 10 v. Google

Dear Mr. Mausner,

We have received your request for a significant amount of additional

and detailed information about EFF's funding. While we have no requirement under law to answer these questions, and by doing so create no waiver as to any privacy interest in this or other information about EFF or its contributors, we will answer your questions in good faith in order to expedite our request for your consent to file the amicus brief at issue.

For the record, the reason we have decided to answer these questions is that it seems clear that you and others with whom EFF often disagrees about intellectual property legal issues are under the misimpression, or seek to create the misimpression, that EFF is bought or influenced by corporate money, and in particular the money of corporations you oppose. This is incorrect. EFF makes decisions about which issues to take on and which positions to take based upon an honest assessment of what is best for the public and innovation. We receive no significant corporate funding and have never allowed any of our funders to determine the positions we take on policy or legal issues. We give you this information, then, to prevent you from using the answers to these questions to fuel that misimpression.

We expect you to ensure that any such misimpression is not perpetuated in this case or in any other case where EFF participates as party or amicus. With that in mind, here are the answers to your questions.

1. Is the \$50,000 contribution made by Google just for this year? Has Google made other contributions to the EFF in other years?

There is no agreement for additional funding from Google for the ChillingEffects project. Google has never made any other direct contributions to EFF. However, Google does have a general corporate giving program that matches the donations of its employees and to the extent that Google employees have individually chosen to donate to EFF, Google has fulfilled its general obligation to match.

2. What other search engines has EFF received support from? How much was the contribution?

None.

3. Has your organization accepted contributions from Napster or the defendants in the Grokster case? If so, please specify the dates and amounts.

No contributions from Napster. Since we represent parties in the MGM v. Grokster case, and attorney-client and joint defense privilege issues arise, we do not believe it is appropriate for us to discuss that case.

4. Has your organization accepted contributions from other parties on behalf of which it has written amicus briefs? If so, please specify the names of the parties, the amounts contributed, and the cases in which EFF wrote the amicus brief.

As noted above, EFF does not track this type of information, nor does it take any donor information into account when we determine to file an amicus brief on behalf of the public interest.

Having gone beyond any duty we have to respond to your questions, we respectfully request that you now provide us with your decision regard consent as soon as possible, so we can inform the court promptly in our filings.

Sincerely,
Jason Schultz
EFF

On Sep 30, 2005, at 8:01 AM, Jeff Mausner wrote:

> Jason, I'm getting this e-mail bounced back. Please confirm that you
> received it. Jeff.

> -----Original Message-----

> From: Jeff Mausner [mailto:jeffmausner@bmlaw.com]
> Sent: Friday, September 30, 2005 7:57 AM
> To: Jason Schultz
> Cc: Russell Frackman (rjf@msk.com); 'Goldman, Jeffrey'; Norm Zada
> (normanz@earthlink.net); Dan Cooper (Dan@perfect10.com)
> Subject: FW: Consent To File Amicus in Perfect 10 v. Google

> Jason, Russ Frackman has asked me to respond to your e-mail. Could you
> please provide the following information to us:

> 1. Is the \$50,000 contribution made by Google just for this year?
> Has
> Google made other contributions to the EFF in other years?

> 2. What other search engines has EFF received support from? How
> much
> was the contribution?

> 3. Has your organization accepted contributions from Napster or
> the
> defendants in the Grokster case? If so, please specify the dates and
> amounts.

> 4. Has your organization accepted contributions from other
> parties on
> behalf of which it has written amicus briefs? If so, please specify
> the
> names of the parties, the amounts contributed, and the cases in which
> EFF
> wrote the amicus brief.

> Thank you, Jeff Mausner.

> -----Original Message-----

> From: Jason Schultz [mailto:jason@eff.org]
> Sent: Wednesday, September 28, 2005 11:18 AM
> To: Frackman, Russell
> Subject: Re: Consent To File Amicus in Perfect 10 v. Google

> Mr. Frackman,

> Neither Google nor Amazon are EFF members or otherwise "affiliated"
> with EFF. Google has given a small donation of \$50,000, which
> represents less than 3% of EFF's annual budget, to support the Chilling
> Effects project specifically. This is a joint project with several law
> schools, including Harvard, Stanford, University of Maine and several
> others hosted at www.chillingeffect.org.

> Best,
> Jason Schultz

> On Sep 26, 2005, at 10:18 AM, Frackman, Russell wrote:

>> Mr. Schultz,

>> So that we have all the information relevant to your request please
>> advise us whether Amazon and/or Google are members of, contributors to

>> or in any way affiliated with EFF

>>> RUSSELL J. FRACKMAN | Mitchell Silberberg & Knupp LLP | 11377 West
>>> Olympic Blvd., Los Angeles, CA 90064 | direct: 310 312-3119 | fax:
>>> 310 231-8319 | rjf@msk.com | www.msk.com
>>> THE INFORMATION CONTAINED IN THIS E-MAIL MESSAGE IS INTENDED ONLY FOR
>>> THE PERSONAL AND CONFIDENTIAL USE OF THE DESIGNATED RECIPIENTS. THIS
>>> MESSAGE MAY BE AN ATTORNEY-CLIENT COMMUNICATION, AND AS SUCH IS
>>> PRIVILEGED AND CONFIDENTIAL. IF THE READER OF THIS MESSAGE IS NOT AN
>>> INTENDED RECIPIENT, YOU ARE HEREBY NOTIFIED THAT ANY REVIEW, USE,
>>> DISSEMINATION, FORWARDING OR COPYING OF THIS MESSAGE IS STRICTLY
>>> PROHIBITED. PLEASE NOTIFY US IMMEDIATELY BY REPLY E-MAIL OR
>>> TELEPHONE, AND DELETE THE ORIGINAL MESSAGE AND ALL ATTACHMENTS FROM
>>> YOUR SYSTEM. THANK YOU.

>> -----Original Message-----

>> From: Jason Schultz [mailto:jason@eff.org]
>> Sent: Friday, September 23, 2005 3:55 PM
>> To: Frackman, Russell
>> Subject: Consent To File Amicus in Perfect 10 v. Google

>> Mr. Frackman,

>> On behalf of the Electronic Frontier Foundation, I respectfully
>> request Perfect 10's consent to file an amicus brief regarding the
>> motion for preliminary injunction in the Perfect 10 v. Google case.
>> Please let me know whether or not your client will consent to our
>> request at your earliest convenience.

>> Sincerely,
>> Jason Schultz

>> Jason M. Schultz
>> Staff Attorney
>> Electronic Frontier Foundation

(415) 436-9333 x 112
jason@eff.org
www.eff.org

> Jason M. Schultz
> Staff Attorney
> Electronic Frontier Foundation

(415) 436-9333 x 112
jason@eff.org
www.eff.org

Jason M. Schultz
Staff Attorney
Electronic Frontier Foundation

(415) 436-9333 x 112
jason@eff.org
www.eff.org

EXHIBIT B



copyright

Search

☐ Search WWW ☒ Search www.eff.org

Try Google AdWords and reach your best prospects across the web.

Web

Results 1 - 50 of about 45,100 from www.eff.org for **copyright**. (0.32 seconds)

Copyright Registration

Sponsored I

www.icreateditfirst.com Simple **copyright** protection for Art Musicians, Authors, Designers, Song

Sponsored Links

EFF: Computers & Academic Freedom

Copyright Law · Digital Rights Management · DMCA · Domain names · E-voting ·

File-sharing · Filtering · FTAA · Intellectual Property · International ...
www.eff.org/Censorship/Academic_edu/CAF/ - 16k - Oct 20, 2005 -

[Cached](#) - [Similar pages](#)

Become a Published Author

Join thousands of writers who published with us for over 85 yrs.
www.dorrancepublishing.com

EFF "Digital Millennium Copyright Act (DMCA)" Archive

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/ - 22k - [Cached](#) - [Similar pages](#)

Copyright Your Work

Books, Music, Pictures and More.
 Fast, Reliable and Affordable.
www.legalzoom.com

Final joint version of HR 2281, DMCA (Digital Millennium Copyright ...

SHORT TITLE. This Act may be cited as the 'Digital Millennium Copyright Act'.

... (b) SUBJECT MATTER OF COPYRIGHT; NATIONAL ORIGIN-
 Section 104 of title 17, ...

www.eff.org/IP/DMCA/hr2281_dmca_law_19981020_pl105-304.html - 101k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

Valuable Copyright?

Register it right. Hire a lawyer.
 \$149 total. No hidden fees.
www.yourpatentlawyer.com

EFF: Intellectual Property

An exhaustive list of annotated links to patent, trademark and **copyright** information

from the Electronic Frontier Foundation.

www.eff.org/IP/ - 15k - [Cached](#) - [Similar pages](#)

Register Your Copyright

Get Legal Proof You Own Your Work!
 Websites, Writing, Music & More.
www.GoCopyright.com

Washington Copyright

Full Service Package for only \$99.
 Register Your Work. Simple. 24Hrs
www.washingtoncopyright.com

EFF: Homepage

Yesterday, the Authors Guild filed a class-action **copyright** infringement suit

against Google over its Google Print library project. ...

www.eff.org/ - 22k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

Got Copyright Protection?

We file copyrights in 24 hrs & save you tons in legal fees.
www.clickandcopyright.com

www.eff.org/IP/P2P/20010227_p2p_copyright_white_pa...

1k - [Cached](#) - [Similar pages](#)

intellectual law office

Patent, trade mark, **copyright** and IP- related litigation
www.sidesun.com.cn

Copyright Attorney

Full-Service; Free Consultation
Copyright Registration \$120
danaugustyn.com

EFF: What Peer-to-Peer Developers Need to Know about Copyright Law

[Get Copyright Permission](#)

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/P2P/?f=p2p_copyright_wp_v4.html - 62k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

EFF: DeepLinks

Patry Calls Subway Map **Copyright** Threats "Shameful" ... **Copyright** is both unnecessary and inappropriate. The agencies' actions are shameful. Indeed. ...

www.eff.org/deeplinks/archives/004013.php - 12k - [Cached](#) - [Similar pages](#)

EFF: Bloggers' FAQ: Intellectual Property

Short quotations will usually be fair use, not **copyright** infringement. The **Copyright**

Act says that "fair use...for purposes such as criticism, comment, ... www.eff.org/bloggers/lg/faq-ip.php - 25k - [Cached](#) - [Similar pages](#)

EFF: ISP Rejects Diebold **Copyright** Claims Against News Website

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/legal/ISP_liability/20031016_eff_pr.php - 14k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

EFF Unintended Consequences: Four Years under the DMCA

Will Knight, "Computer Scientists boycott US over digital **copyright** law," New

... Rather than prevent **copyright** infringement, the DMCA empowered Apple to ...

www.eff.org/IP/DMCA/20030102_

[dmca_unintended_consequences.html](#) - 65k - [Cached](#) - [Similar pages](#)

Understanding Internet **Copyright**

Understanding Your Rights: **Copyright** Protection on the Internet ... Particularly on

the Internet, you should think about **copyright** in an international ...

www.eff.org/cafe/gross2.html - 10k - [Cached](#) - [Similar pages](#)

EFF: Breaking News

Contract and **Copyright** Trump Fair Use and Competition in BnetD Case ... The company claimed **copyright** violations and used the DMCA to demand that the ...

www.eff.org/news/archives/2004_09.php - 53k -

[Cached](#) - [Similar pages](#)

[PDF] August 8, 2003 Dear Colleagues: The problem of unauthorized peer ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

has prepared the enclosed paper on **copyright** law and the potential liability of

students ... **copyright** rights and responsibilities and P2P file sharing.

For millions of publications worldwide.

www.copyright.com

Copyright Questions?

Expert guide to patents and copyrights.

coachbiz.org

Worldwide-**Copyright**.com

Protection par constat d'Huissier

Valide pour 150 ans dans 159 pays

www.CopyrightFrance.com

Copyright Your Work

Protect Your Work - **Copyright** It.

\$68 - Quick, Easy, and Effective!

registermycopyright.com

Copyright Registration

Books, Websites, Music and more

Fast and Affordable

www.JurisCounsel.com

Copyright at Amazon.com

Buy books at Amazon.com and save.

Qualified orders over \$25 ship free

Amazon.com/books

Copyright

Get great info on

Copyright.

InfoScouts.com

Copyright

Looking for items related to

Copyright? Shop on eBay!

www.ebay.com

Free Copyrights

Make \$97/day with new mailorder CD-ROM.

Free Duplication rights!

silverdollarpublishingonline.com

All **copyright** information

Legal experts on **copyright**

throughout Africa

www.adamsadams.com/

Copyright

US and International Patents.

Learn About - **Copyright**

www.InternationalPatents.com

Copyright

Advice and Information related to

Copyright.

BambooWeb.com

What is a **Copyright**?

Learn about copyrights. patents

...

www.eff.org/IP/P2P/P2P_Joint_Committee_paper.pdf - [Similar pages](#)

EFF Copyright and Fair Use FAQ

What's Covered by **Copyright** and how long do the rights last? ...

Second, there's

copyright in the artist's interpretation and particular recording of the ...

www.eff.org/cafe/drmgame/copyright-faq.html - 67k -

[Cached](#) - [Similar pages](#)

Media Release: EFF Seeks to Protect Internet Radio Privacy (Apr ...

Last week, EFF released a joint comment to the **Copyright** Office, ...
In an

unprecedented invasion of listener privacy, the **Copyright** Office has proposed ...

www.eff.org/IP/Audio/20020410_joint_co_comments_pr.html - 7k -

[Cached](#) - [Similar pages](#)

[PDF] [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](#) ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

this Court, alleging that Diebold's claim of **copyright** infringement was based on

... exclusive legal basis for protecting a **copyright** or defending against ...

www.eff.org/legal/ISP_liability/

[OPG_v_Diebold/20040930_Diebold_SJ_Order.pdf](#) - [Similar pages](#)

EFF: Breaking News

Music Publisher Settles **Copyright** Skirmish Over Guthrie Classic ...
According to

EFF, the initial **copyright** term was triggered when Guthrie sold his first ...

www.eff.org/news/archives/2004_08.php - 33k -

[Cached](#) - [Similar pages](#)

EFF: Web Linking Need Not Cause Copyright Liability

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/Linking/Kelly_v_Arriba_Soft/

[20030707_9th_revised_ruling_pr.php](#) - 13k - [Cached](#) - [Similar pages](#)

EFF: DeepLinks

Last month we posted a bit about the **copyright** debates surrounding the Google Print

... But if a **copyright** owner does not want Google to scan her book, ...

www.eff.org/deepinks/archives/003954.php - 12k -

[Cached](#) - [Similar pages](#)

EFF: Librarian of Congress Fails Public Interest in Copyright ...

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/20031028_1201_pr.php - 14k -

and trademarks.

www.patents-info.com

Copyright

Find legal information on {any legal topic.}

legal-database.com

Copyright

Free Legal Resource.

Copyright

OnInformation.com

597 Business Letters

At your fingertips, just about every kind of letter or form needed
thesalesfloor.com/597letters.htm

Copyright

Copyright

Start your search here.

zimply.com

\$1.95 Domain Names

Includes Free Website. Easy Setup.
Spam-Free Email. 24/7 Phone Support
HostingDude.com

Copyright

World's largest online library.

1000s of popular research topics
Questia.com

Copyright in 3 minutes

By Internet, users in 35 countries
Since 2001 the most popular
www.copyrightdeposit.com

Copyright

Info - **Copyright**

Patent Search, Registration, Law.
www.ChinaPatent.com

Copyright Law

Information on

copyright laws.

Find-legal.info

Copyright Information

Search Online at Tunu.com for

Copyright Information

Tunu.com/Copyright

Copyright?

Brief and Straightforward Guide to Trademarks
wisegeek.com

Register Your Copyright

Easy and affordable international **copyright** registration service.

[Cached](#) - [Similar pages](#)

CopyrightWitness.com

EFF: USv ElcomSoft & Sklyarov

20021217_eff_pr.html: Jury Acquits Elcomsoft in eBook **Copyright** Case, ...

John Ashcroft that the Digital Millennium **Copyright** Act (DMCA) and its ...

www.eff.org/IP/DMCA/US_v_Elcomsoft/ - 32k - [Cached](#) - [Similar pages](#)

Copyright

Check Out Our Guide

For: **Copyright**

www.searchguide.biz

Copyright Infringement

Automated detection of **copyright**, trademark and other infringement.

www.DataShaping.com

EFF: DeepLinks

Judge Posner: Misuse Remedies for **Copyright's** Chill ... Judge

Posner recommends

the doctrine of **copyright** misuse too -- and as a judge, he doesn't just blog ...

www.eff.org/deepinks/archives/001842.php - 13k - Oct 20, 2005 -

[Cached](#) - [Similar pages](#)

UK Patent Company

Patent and trade mark searches,

IP valuation, prototyping service

www.patentseekers.com

EFF: Comments and Testimony to the **Copyright** Office

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/copyrightoffice/ - 11k - [Cached](#) - [Similar pages](#)

EFF: DeepLinks

And the **copyright** is now in the hands of Ludlow Music, Inc., a unit of The Richmond

... "This song is Copyrighted in US, under Seal of **Copyright** # 154085, ...

www.eff.org/deepinks/archives/001765.php - 12k - [Cached](#) - [Similar pages](#)

EFF "Intellectual Property - NII **Copyright** Bill (1996)" Archive

Did not pass. s1284_1995.bill: Senate version of the NII **Copyright** Protection Act of 1995. Did not pass. Subdirectories in This Archive ...

www.eff.org/IP/NII_copyright_bill/ - 4k - [Cached](#) - [Similar pages](#)

EFF Media Release: Jury Acquits Elcomsoft in eBook **Copyright** Case ...

Jury Acquits Elcomsoft in eBook **Copyright** Case. Dmitry Sklyarov Odyssey Leaves

Prosecutor Empty-Handed. Electronic Frontier Foundation Media Release ...

www.eff.org/IP/DMCA/US_v_Elcomsoft/20021217_eff_pr.html - 22k - [Cached](#) - [Similar pages](#)

AN INTELLECTUAL PROPERTY LAW PRIMER FOR MULTIMEDIA AND WEB ...

This primer will focus on US **copyright** law because **copyright** law is the most important ... PATENT LAW While **copyright** law is the most important intellectual ...

www.eff.org/Censorship/Academic_edu/CAF/law/multimedia-handbook - 52k - [Cached](#) - [Similar pages](#)

EFFector, Vol. 13, No. 11; Dec. 13, 2000

On October 28, 2000 the controversial Digital Millennium **Copyright** Act (DMCA) took

... EFF's Reply Comments to US **Copyright** Office on DMCA (March 31, 2000): ...

www.eff.org/effector/HTML/effect13.11.html - 27k - [Cached](#) - [Similar pages](#)

Joint Comments to **Copyright** Office on Internet Radio Privacy (Apr ...

In its Notice, the **Copyright** Office seeks comment on proposed ... In an unprecedented change to this status quo, the **Copyright** Office has proposed ...

www.eff.org/IP/Audio/20020405_joint_co_comments.html - 20k - [Cached](#) - [Similar pages](#)

EFF: Breaking News

Congress intended the DMCA to thwart mass **copyright** infringement on the Internet,

... Entertainment Giants Push Supreme Court to Rewrite **Copyright** Law ...

www.eff.org/news/archives/2004_10.php - 66k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

EFF: RIAA Petition

We respect reasonable **copyright** law, but we strongly oppose **copyright** enforcement that comes at the expense of privacy, due process and fair application of ...

www.eff.org/share/petition/ - 13k - Oct 20, 2005 - [Cached](#) - [Similar pages](#)

EFF: JibJab Media Inc., v. Ludlow Music, Inc.

That's a great thing, the real genius of **copyright**." ... **Copyright** Law · Digital Rights Management · DMCA · Domain names · E-voting · File-sharing ...

www.eff.org/legal/cases/JibJab_v_Ludlow/ - 13k - [Cached](#) - [Similar pages](#)

Understanding Internet Copyright

Since the Web itself is a collection of hyperlinks, nearly every Web page is probably a few clicks away from material that may violate someone's **copyright**, ...

www.eff.org/cafe/gross3.html - 5k - [Cached](#) - [Similar pages](#)

EFF: DeepLinks

As many have reported, the Family Entertainment and **Copyright** Act of 2005 ... Second, it modifies the criminal provisions of the **Copyright** Act to impose ...

www.eff.org/deeplinks/archives/003515.php - 15k - [Cached](#) - [Similar pages](#)

EFF: EFF Prepared Testimony at Copyright Office section 1201 rule ...

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/copyrightoffice/20030515_region_dvd.php - 25k - [Cached](#) - [Similar pages](#)

EFF: Prepared Testimony at Copyright Office section 1201 rule ...

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/copyrightoffice/20030513_unskippable_dvd.php - 23k - [Cached](#) - [Similar pages](#)

EFF: Electronic Frontier Foundation Renews Copyright Request

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/20030722_1201_pr.php - 14k - [Cached](#) - [Similar pages](#)

[PDF] DPITUSA

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Though **copyright**-like protection for facts and data within databases has been considered in a ... US **Copyright** Law Does Not Protect Facts Within Databases ...

www.eff.org/IP/WIPO/20040607_database_protection.pdf - [Similar pages](#)

[PDF] 1 Before the Library of Congress Copyright Office In re Exemption ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Copyright Act ("DMCA"), EFF has been involved in virtually all of the ... For the reasons set out above, EFF respectfully requests the **Copyright** Office ...

www.eff.org/legal/cases/Lexmark_v_Static_Control/SCC_031003.pdf - [Similar pages](#)

EFF: 321 Studios Advocates Fair Uses in Digital Copyright Law

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/20031111_321_studios_pr.php - 14k - [Cached](#) - [Similar pages](#)

EFF: Breaking News

Supreme Court Justices Grill Both Sides at **Copyright** Hearing. MGM v. Grokster Raises Questions About Innovation and Litigation ...

www.eff.org/news/archives/2005_03.php - 47k - [Cached](#) - [Similar pages](#)

EFF: Public Asks Copyright Office to Allow Common CD/DVD Uses ...

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/20030220_1201_pr.php - 14k - [Cached](#) - [Similar pages](#)

[PDF] MEASURING THE DIGITAL MILLENNIUM COPYRIGHT ACT AGAINST THE DARKNET ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

the **Copyright** Act, these anti-circumvention provisions of the DMCA ... the **Copyright** Act, and codified at 17 USC § 1201. References to the DMCA should be ...

www.eff.org/IP/DMCA/DMCA_against_the_darknet.pdf - [Similar pages](#)

[PDF] Library of Congress Copyright Office Notice of Inquiry In re ...

File Format: PDF/Adobe Acrobat - [View as HTML](#)

questions posed by the **Copyright** Office in its letter of June 5, 2003. ...

protected by **copyright**? (Please provide the specific titles in each such case). ...

www.eff.org/IP/DMCA/copyrightoffice/eff_posthg_032603.pdf - [Similar pages](#)

EFF: EFF Prepared Testimony at Copyright Office section 1201 rule ...

Electronic Frontier Foundation is a nonprofit group working to protect your digital rights.

www.eff.org/IP/DMCA/copyrightoffice/20030514_copyprotected_cds.php - 27k - [Cached](#) - [Similar pages](#)

[PDF] Before the **COPYRIGHT OFFICE LIBRARY OF CONGRESS Washington, DC In ...**

File Format: PDF/Adobe Acrobat - [View as HTML](#)

Radio submit the following comments in response to the **Copyright** ... on proposed requirements for giving **copyright** owners reasonable notice of the use of ...

www.eff.org/IP/Audio/20020405_joint_co_comments.pdf - [Similar pages](#)

EFF: DMCA Archive

Last Wednesday, the US **Copyright** Office issued a long-awaited report about ...

Let's look at how **copyright** owners have used the DMCA so far: to silence a ...

www.eff.org/IP/DMCA/?f=20010830_eff_dmca_op-ed.html - 14k - [Cached](#) - [Similar pages](#)

EFF: Content Protection for Recordable Media (CPRM) Archive

Copyright Terrorism and the Internet: by Dave Touretsky, Nov. 2001 (includes an example of a bogus "notice and takedown" legal threat letter to an ISP, ...

www.eff.org/Censorship/SLAPP/IP_SLAPP/ - 15k - [Cached](#) - [Similar pages](#)

EFF Media Release: Scientists Support Professor's Copyright Law ...

Trenton, NJ - Seventeen of the world's top scientists today supported Princeton University Professor Edward Felten and his research team's challenge to the ...

www.eff.org/IP/DMCA/Felten_v_RIAA/20010813_eff_felten_pr.html - 38k - [Cached](#) - [Similar pages](#)

Goooooooooooooogle ►

Result Page: 1 2 3 4 5 6 7 8 9 10 [Next](#)

copyright

Search

[Search within results](#) | [Search Tips](#)

[Google Home](#) - [Advertising Programs](#) - [Business Solutions](#) - [About Google](#)

©2005 Google

EXHIBIT C


[About EFF](#)
[Cases](#)
[Press Room](#)
[DeepLinks](#)
[Action Center](#)
[Join EFF](#)
[Sitemap](#) | [Calendar](#)

How Not To Get Sued By The RIAA For File-Sharing

(And Other Ideas to Avoid Being Treated Like a Criminal)

The Recording Industry Association of America (RIAA) announced on June 25, 2003, that it will begin suing users of peer-to-peer (P2P) file-sharing systems within the next few weeks. According to the announcement, the RIAA will be targeting users who upload/share "substantial" amounts of copyrighted music. The RIAA has stated that it will choose who to sue by using software that scans users' publicly available P2P directories and then identifies the ISP of each user. Then, using the Digital Millennium Copyright Act (DMCA), the RIAA will subpoena the ISP for each user's name, address, and other personal information in order to sue that user.

To find out whether your name has been subpoenaed from your ISP, check out our [Subpoena Query](#) page.

More information about the RIAA lawsuits and responses to them, check out our [RIAA v. The People](#) page.

While there is no way to know exactly what the RIAA is going to do, who it is going to sue, or even how much music qualifies as a "substantial" amount, users of P2P networks can take the following steps to reduce their chances of being sued:

1. Either:

- a. Make sure there are no potentially infringing files in your shared folder. This would ordinarily mean that your shared folder contains only files 1) that are in the public domain, 2) for which you have permission to share, or 3) that are made available under pro-sharing licenses, such as the [Creative Commons](#) license or other open media licenses, and
- b. Remove all potentially misleading file names that might be confused with the name of an RIAA artist or song (e.g., "Usher" or "Madonna") from your shared folder.

Or:

- c. Disable the "sharing" or "uploading" features on your P2P application that allow other users on the network to get copies of files from your computer or scan any of your music directories. We hate this option, but it does appear that it will reduce your chances of becoming an RIAA target right now. For instructions on how to do this for particular applications, EFF suggests (but cannot guarantee) the following links:
 - Grokster
 - <http://www.grokster.com/helpfaq.html#Stop%20Sharing%20files>
 - <http://www.oit.duke.edu/helpdesk/filessharing/grokster.html>

- Morpheus
 - <http://www.oit.duke.edu/helpdesk/filessharing/morpheus.html>
 - <http://penguin.cc.edu/peer/peer2peer.html#morpheus>
- KaZaA
 - <http://www.oit.duke.edu/helpdesk/filessharing/kazaa.html>
 - <http://penguin.cc.edu/peer/peer2peer.html#kazaa>
- Aimster/Madster
 - Windows
 - <http://www.oit.duke.edu/helpdesk/filessharing/aimster.html>
 - Mac OS
 - http://www.oit.duke.edu/helpdesk/filessharing/aimster_mac.html
- Gnutella
 - Mactella
 - <http://www.oit.duke.edu/helpdesk/filessharing/mactella.html>
 - Gnucleus
 - <http://www.oit.duke.edu/helpdesk/filessharing/gnucleus.html>
 - Gnotella
 - <http://www.oit.duke.edu/helpdesk/filessharing/gnotella.html>
 - LimeWire
 - MacOS
 - <http://www.oit.duke.edu/helpdesk/filessharing/limewiremac.html>
 - Windows
 - <http://www.oit.duke.edu/helpdesk/filessharing/limewirewin.html>
 - <http://penguin.cc.edu/peer/peer2peer.html#limewire>
 - BearShare
 - <http://www.oit.duke.edu/helpdesk/filessharing/bearshare.html>
 - <http://penguin.cc.edu/peer/peer2peer.html#bearshare>
 - iMesh
 - <http://www.oit.duke.edu/helpdesk/filessharing/imesh.html>
 - WinMX
 - <http://www.oit.duke.edu/helpdesk/filessharing/winmx.html>
 - <http://penguin.cc.edu/peer/peer2peer.html#winmx>

2. The RIAA appears to be targeting subpoenas at users who allow their computers to be "Supernodes" on the FastTrack P2P System (used, for instance, by KaZaA and Morpheus). In order to further reduce the risk of having your ISP subpoenaed or of being sued yourself, we recommend that you make sure your computer is not being used as a Supernode. To learn more about Supernodes and how to make sure your computer is not one, look here: <http://www.whtvcable.com/fasttrack> and <http://helpdesk.princeton.edu/kb/display.plx?ID=9245>. See also [Disabling the Supernode function with KaZaA \(PDF 331k\)](#).
3. If you receive notice that your ISP has been subpoenaed for your name and address, consider contacting www.subpoenadefense.org, where you can find information about how to defend your privacy and a list of attorneys willing to help. Contact your ISP and ask the people there to notify you immediately if they receive a subpoena seeking your identity.
4. If you receive a cease and desist letter from the RIAA, consider contacting [Chilling Effects](#), where EFF and several law school clinics are creating a gallery of cease and desist letters along with basic information about the claims being made and your rights online.

Don't like the idea of turning off file-sharing or changing your file names to prevent stupid

robots or RIAA employees from mistaking your files for infringements?

Neither do we!

Join EFF's campaign to make file-sharing legal while getting artists paid:

1. Contact your Congressional Representative and demand that Congress hold immediate hearings on ways to save P2P technology and file-sharing while ensuring that artists get paid.
2. Learn more about alternatives. EFF's peer-to-peer web pages gather together some of the best ideas and describe how similar sorts of technology changes have been handled in the past.
3. Tell a friend, family member, colleague or even stranger on the street about the damage that the RIAA is doing to the Internet, innovation, and consumer choice. There are over 57 million Americans who use P2P file-sharing -- more than voted for President Bush -- and millions more worldwide -- so chances are good that the person sitting next to you on the bus, walking beside you on the sidewalk or driving in the car in front of you is using file-sharing, too. Start the conversation.
4. Join EFF and support our efforts to protect file-sharing.

[HOME](#) | [CASES](#) | [ACTION CENTER](#) | [PRESS ROOM](#) | [ABOUT THE EFF](#) | [DONATE](#) |
[VOLUNTEER](#) | [PRIVACY POLICY](#)

EXHIBIT D



Electronic Frontier Foundation

Defending Freedom in the Digital World

IAAL*: What Peer-to-Peer Developers Need to Know about Copyright Law

by Fred von Lohmann
Senior Intellectual Property Attorney
Electronic Frontier Foundation
fred@eff.org

v. 4.0, September 2004

I. What this is, and who should read it.

The future of peer-to-peer file-sharing is entwined, for better or worse, with copyright law. Copyright owners have already targeted not only the makers of file-sharing clients like Napster, Scour, Audiogalaxy, Aimster and Kazaa, and Morpheus, but also companies that provide products that rely on or add value to public P2P networks, such as MP3Board.com, which provided a web-based search interface for the gnutella network.

If these early skirmishes yield any lesson for P2P developers, it is that a legal strategy needs to be in place early, preferably at the beginning of development, rather than bolted on at the end.

This piece is meant as a general explanation of the U.S. copyright law principles most relevant to P2P file-sharing technologies. It is aimed primarily at:

- Developers of core P2P file-sharing technology, such as the underlying protocols, platform tools, and specific client implementations; and
- Developers of ancillary services that depend upon or add value to P2P file-sharing networks, such as providers of search, security, metadata aggregation, and other services.

The following discussion is meant as a general introduction, and thus glosses over many of copyright law's more subtle nuances. It is aimed not at giving you all the answers, but rather at allowing you to recognize the right questions to ask.

What this is not: The following discussion focuses only on U.S. copyright law, and does not address any issues that may arise under non-U.S. law. While non-copyright principles may also be mentioned, this discussion does not attempt to examine other legal principles that might apply to P2P file-sharing, including patent, trademark, trade secret, or unfair competition. Nothing contained herein constitutes legal advice—please discuss your individual situation with your own attorney.

II. Copyright basics and the intersection with P2P file sharing.

Copyright law applies to virtually every form of expression that can be captured (or, to use the copyright term of art, “fixed”) in a tangible medium, such as on paper, film, magnetic

* Acronym for “I am a lawyer,” to distinguish from the common “IANAL” (“I am not a lawyer”) that appears on Slashdot and other online forums. This white paper was originally titled “IAAL: Peer-to-Peer File Sharing and Copyright Law after Napster.”

tape, hard drive, optical media, or (arguably) in RAM. Songs, books, photographs, software, and movies are all familiar examples of copyrighted works. Copyright law reserves certain rights exclusively to the owner of the copyright, including the right to reproduce, distribute, and publicly perform the work.

The nature of file-sharing technology inevitably implicates copyright law. First, since most digital files are “fixed” for purposes of copyright law (whether on a hard drive, CD, or possibly in RAM), the files being shared generally qualify as copyrighted works. Second, the transmission of a file from one person to another results in a reproduction, a distribution, and possibly a public performance (in the world of copyright law, “public performance” may include the act of transmitting a copyrighted work).

Thus, to a copyright lawyer, every reproduction, distribution, and public performance requires an explanation, and thus file-sharing seems suspicious from the outset.

A. The end-users: “direct” infringement.

For the individuals who are sharing files, the question becomes whether all of these reproductions, distributions, and public performances are authorized by the copyright owner or otherwise permitted under copyright law (as “fair use,” for example). So, if the files you are sharing with your friends are videos of your vacation, you are the copyright owner and have presumably authorized the reproduction, distribution, and performance of the videos.

However, if you are sharing MP3’s of Metallica’s greatest hits, or disc images of the latest Microsoft Office install CD, the issue becomes more complicated. In that case, assuming that the copyright owner has not authorized the activity, the question of copyright infringement will depend whether you can qualify for any of the limited exceptions to the copyright owner’s exclusive rights. If not, you’re what copyright lawyers call a “direct infringer”—you have directly violated one or more of the copyright owner’s exclusive rights.

In a widely-used public P2P file-sharing environment, it is a virtual certainty that at least some end-users are engaged in infringing activity (unless the application is specifically designed not to function as a general purpose networking tool, but instead to permit only certain “authorized” files to be shared). When the major record labels and music publishers decided to sue Napster, for example, it was not difficult for them to locate a large number of Napster users who were sharing copyrighted music without authorization.

B. The P2P tool maker: contributory and vicarious infringement.

But what does this have to do with those who develop and distribute peer-to-peer file-sharing tools? After all, in a pure P2P file-sharing system, the vendor of the file-sharing tool has no direct involvement in the copying or transmission of the files being shared. These activities are handled directly between end-users.

Copyright law, however, can sometimes reach beyond the direct infringer to those who were only indirectly involved in the infringing activity. As in many other areas of the law (think of the “wheel man” in a stick up, or supplying a gun to someone you know is going to commit a crime), copyright law will sometimes hold one individual accountable for the actions of another. So, for example, if a swap meet owner rents space to a vendor with the knowledge that the vendor sells counterfeit CDs, the swap meet owner can be held liable for infringement alongside the vendor.

Under copyright law, this indirect, or “secondary,” liability can take two distinct forms: contributory infringement and vicarious infringement.

1. Contributory infringement.

Contributory infringement is similar to “aiding and abetting” liability: one who knowingly contributes to another’s infringement may be held accountable. Or, as the courts have put it, “one who, with knowledge of the infringing activity, induces, causes, or materially contributes to the infringing conduct of another, may be held liable as a contributory infringer.”

So, in order to prevail on a contributory infringement theory, a copyright owner must prove each of the following elements:

- **Direct Infringement:** There has been a direct infringement by someone.
- **Knowledge:** The accused contributory infringer knew of the underlying direct infringement. This element can be satisfied by showing either that the contributory infringer actually knew about the infringing activity, or that he reasonably should have known given all the facts and circumstances. At a minimum, however, the contributory infringer must have some specific information about infringing activity—the mere fact that the system is capable of being used for infringement, by itself, is not enough.
- **Material Contribution:** The accused contributory infringer induced, caused, or materially contributed to the underlying direct infringement. Merely providing the “site and facilities” that make the direct infringement possible can be enough.

2. Vicarious infringement.

Vicarious infringement is derived from the same legal principle that holds an employer responsible for the actions of its employees. A person will be liable for vicarious infringement if he has the right and ability to supervise the direct infringer and also has a direct financial interest in his activities.

Thus, in order to prevail on a vicarious infringement theory, a copyright owner must prove each of the following:

- **Direct Infringement:** There has been a direct infringement by someone.
- **Right and Ability to Control:** The accused vicarious infringer had the right and ability to control or supervise the underlying direct infringement. This element does not necessarily set a high hurdle. For example, the *Napster* court found that the ability to terminate user accounts or block user access to the system was enough to constitute “control.”
- **Direct Financial Benefit:** The accused vicarious infringer derived a “direct financial benefit” from the underlying direct infringement. In applying this rule, however, the courts have not insisted that the benefit be especially “direct” or “financial”—almost any benefit seems to be enough. For example, the *Napster* court found that “financial benefit exists where the availability of infringing material acts as a draw for customers” and the growing user base, in turn, makes the company more attractive to investors.

The nature of vicarious infringement liability creates a strong incentive to monitor the conduct of your users. This stems from the fact that knowledge is not required for vicarious

infringement liability; a person can be a vicarious infringer even if they are completely unaware of infringing activity.

As a result, if you exercise control over your users and derive a benefit from their activities, you remain ignorant of their conduct at your own risk. In the words of the *Napster* court, “the right to police must be exercised to the fullest extent. Turning a blind eye to detectable acts of infringement for the sake of profit gives rise to liability.”

3. The “Betamax defense.”

Holding technology developers responsible for the unlawful acts of end-users obviously can impose a crushing legal burden on those who make general-purpose tools. Fortunately, the Supreme Court has defined an outer limit to copyright's indirect liability theories.

In *Sony v. Universal City Studios*, 464 U.S. 417 (1984), a case brought by the movie industry to ban the Sony Betamax VCR, the Supreme Court found that contributory infringement liability could not reach the manufacturer of a device that is “capable of substantial noninfringing use.” In that case, the Court found that the VCR was capable of several noninfringing uses, including the time-shifting of television broadcasts by home viewers. Rather than focusing on the *proportion* of the uses are noninfringing, the Supreme Court adopted a standard that asks whether the technology is “merely capable” of substantial noninfringing uses.

As will be discussed in more detail below, the “Betamax defense” has been under sustained legal attack in the recent cases involving P2P technology. In the *Napster* case, for example, the court found that this defense does not apply at all to vicarious liability. Accordingly, if you have control over, and derive a financial benefit from, direct infringement, the existence of “substantial noninfringing uses” for your service is irrelevant. In the *Aimster* case, the court suggested that the Betamax defense may require an evaluation of the proportion of infringing to noninfringing uses, contrary language in the Supreme Court’s *Sony* case notwithstanding. In contrast, a different court in the *MGM v. Grokster* case found that the “Betamax defense” protected the makers of Morpheus and Grokster from contributory infringement liability, irrespective of the “proportion” of infringing to noninfringing uses.

In short, the law surrounding the Betamax defense remains in flux, putting P2P developers (and all technologists) on unpredictable legal ground.

III. Indirect liability and P2P file sharing: the cases so far.

As of September 2004, there have been three major court opinions that have applied indirect liability theories to companies that distribute P2P software:

A&M Records v. Napster, 239 F.3d 1004 (9th Cir. 2001)

In re Aimster Copyright Litigation, 334 F.3d 643 (7th Cir. 2003)

MGM v. Grokster, 380 F.3d 1154 (9th Cir. 2004)

Unfortunately, these three cases are not entirely consistent in their analyses. The law continues to evolve, and other courts may further muddy the waters in the months to come.

A. The *Napster* case.

In the *Napster* case, the music industry plaintiffs admitted that Napster did not, itself, make or distribute any or their copyrighted works. Instead, they argued that Napster was liable

for contributory and vicarious infringement. Based on these theories, the plaintiffs convinced a federal district court to grant a preliminary injunction against Napster. That ruling was appealed and affirmed by the Ninth Circuit Court of Appeals. In its February 12, 2001 opinion, the Ninth Circuit rejected each of Napster's proposed defenses.

Turning first to contributory infringement, the Ninth Circuit upheld the lower court's findings:

- **Direct Infringement:** At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Knowledge:** Napster had actual knowledge of infringing activity, based on internal company emails and the list of 12,000 infringing files provided by the RIAA. Moreover, Napster should have known of the infringing activity, based on the recording industry experience and downloading habits of its executives and the appearance of well-known song titles in certain promotional screen shots used by Napster.
- **Material Contribution:** Napster provided the "site and facilities" for the directly infringing conduct of its users.

The Ninth Circuit also endorsed the lower court's vicarious infringement analysis:

- **Direct Infringement:** At least some Napster users are direct infringers, because they distributed and reproduced copyrighted music without authorization.
- **Right and Ability to Control:** Napster has the ability to control the infringing activity of its users because it retains the right to block a user's ability to access its system.
- **Financial Benefit:** Napster derived a financial benefit from the infringing activities of its users because this activity acted as a "draw" for customers, and a portion of Napster's value is derived from the size of its user base.

The Ninth Circuit concluded, however, that the lower court had not adequately considered the technological limits of the Napster system when crafting the preliminary injunction. In ordering the district court to revise its injunction, the Ninth Circuit spelled out some guiding principles. First, in order to prevent contributory infringement, Napster was required to take reasonable steps to prevent further sharing of music *after receiving notice* from a copyright owner that a particular recording is being shared on its system without authorization. Ultimately, Napster voluntarily implemented a number of filtering mechanisms (including file name filters and acoustic fingerprinting filters) intended to filter out works that were not approved for sharing. These filters were never accurate enough to satisfy the district court judge, and Napster ended up in bankruptcy before a trial could be held.

Second, in order to prevent vicarious infringement, the Ninth Circuit declared that "Napster...should bear the burden of policing its system within the limits of the system." During the period until its bankruptcy, Napster and the plaintiffs bitterly disagreed about what these monitoring obligations entailed. At a minimum, Napster had the duty to terminate users who were identified as infringers. Beyond that, there was little agreement. The disagreement was never fully resolved by the court, since Napster was shut down while it worked on improving its filtering technologies.

B. The *Aimster* case.

In the *Aimster* case, the music industry plaintiffs made the same vicarious and contributory infringement claims that they did in the *Napster* case. They succeeded in obtaining a preliminary injunction that ultimately shut Aimster down pending the trial on the merits (like Napster, Aimster went bankrupt before a trial could occur). In June 2003, the Seventh Circuit Court of Appeals upheld the preliminary injunction ruling.

In upholding the preliminary injunction, the appeals court relied solely on the contributory infringement claim. The court did not engage in the traditional contributory infringement analysis, instead engaging in a more general discussion of several relevant concepts, including the *Betamax* defense. In the end, the court upheld the injunction because Aimster had (1) failed to introduce *any* evidence of noninfringing uses and (2) had engaged in activities that demonstrated clear knowledge of infringing activities.

With respect to the issue of knowledge, the court focused on “tutorials” that specifically encouraged Aimster users to download popular copyrighted music. The court also was not impressed by the fact that Aimster network traffic was encrypted, allegedly making it impossible for Aimster to know exactly what files were being shared by individual end-users. In the eyes of the court, the steps taken by Aimster to avoid knowledge supported an inference of “willful blindness.”

Turning to the *Betamax* defense, the court concluded that Aimster had failed to introduce *any* evidence that the Aimster software had ever been used for anything other than infringing activity. This finding alone was enough to disqualify Aimster from relying on the *Betamax* defense (which requires a showing that the technology in question is at least capable of a substantial noninfringing use).

The court, however, went on to suggest that application of the *Betamax* defense requires a consideration of the *proportion* of the infringing to noninfringing uses. This is in direct conflict with language contained in the Supreme Court’s opinion in the *Betamax* case. This view of proportionality, however, was specifically rejected by the Ninth Circuit Court of Appeals in its *MGM v. Grokster* ruling (discussed below). In addition, the discussion of proportionality in the *Aimster* opinion is arguably not binding on any subsequent court, as the outcome in that case was determined by Aimster’s failure to introduce *any* evidence of noninfringing uses for its technology. In any event, the *Aimster* ruling simply underscores the continuing controversy over whether the proportion of infringing and noninfringing uses is relevant to the *Betamax* defense.

C. The *Grokster* case.

The *MGM v. Grokster* case involves three sets of defendants—the makers of Kazaa, Morpheus and Grokster. In April 2003, the district court ruled that two of the defendants—StreamCast (maker of Morpheus) and Grokster—could not be held liable for contributory or vicarious copyright infringement. This represented the first U.S. victory by P2P developers in a copyright action brought by the entertainment industry. The Ninth Circuit Court of Appeals (the same court that issued the *Napster* ruling in 2001) affirmed the district court’s ruling in August 2004.

Contributory Infringement: With respect to contributory infringement, the court emphasized the importance of the *Betamax* doctrine in measuring the “knowledge” element:

Thus, in order to analyze the required element of knowledge of infringement, we must first determine what level of knowledge to require. If the product at issue is not capable of substantial or commercially significant noninfringing uses, then the copyright owner need only show that the defendant had constructive knowledge of the infringement. On the other hand, if the product at issue *is* capable of substantial or commercially significant noninfringing uses, then the copyright owner must demonstrate that the defendant had reasonable knowledge of specific infringing files and failed to act on that knowledge to prevent infringement.

The appeals court then agreed with the district court that Grokster and Morpheus are both capable of substantial noninfringing uses, including the distribution of public domain (such as Project Gutenberg e-books) and authorized materials (such as promotional music videos and video game demos). The court specifically rejected any measurement of the proportion of infringing and noninfringing uses, reiterating that the *Betamax* doctrine requires that a technology merely be *capable* of a substantial noninfringing use.

In order to overcome the *Betamax* doctrine, the Ninth Circuit held that the entertainment companies would have to show that StreamCast and Grokster had “specific knowledge at a time at which they contributed to the infringement, and failed to act upon that information.”

In other words, a copyright owner has to show that you had knowledge of infringement *when you could have done something about it*. StreamCast and Grokster (like vendors of photocopiers and VCRs) never had knowledge of a specific infringement at a time when they could have prevented it. The critical factor was the decentralized architecture of the Grokster and Morpheus software. The software gave the defendants no ability block access to the network, or to control what end-users searched for, shared, or downloaded. Accordingly, by the time the defendants were notified of infringing activity, they were unable to do anything about it (just as Xerox is not able to stop infringing activities after a photocopier has been sold). In the words of the court: “even if the Software Distributors closed their doors and deactivated all computers within their control, users of their products could continue sharing files with little or no interruption.”

The Ninth Circuit also found that neither StreamCast nor Grokster materially contributed to infringement. The decentralized architecture of the software was again a critical factor, with the court emphasizing that StreamCast and Grokster did not provide the “site and facilities” for infringement because they did not provide access to the network, nor did they control any indices. The court concluded that it was the end-users who provided the “site and facilities,” not the software vendors.

The court went on to emphasize that StreamCast and Grokster’s very limited involvement with the network—such as communicating “incidentally” with users or providing network bootstrapping information by hosting “root supernodes”—was not enough to satisfy the “material contribution” threshold.

Vicarious Liability: The Ninth Circuit also concluded that the defendants could not be held vicariously liable. After reviewing the decentralized architecture of the gnutella and fasttrack networks created by Grokster and Morpheus users, the court found that the defendants had no ability to supervise or control what users were searching for, sharing or downloading.

The plaintiffs argued that Grokster and Morpheus could have been designed to include advanced filtering technologies, so as to enable more control over end-user activities. The court found that whether or not such filtering was possible, the defendants had no obligation to redesign their technologies to suit the desires of the entertainment industries. Moreover, the court went out of its way to reject the notion that StreamCast or Grokster had any obligation to “upgrade” its existing users’ software in order to protect copyright owners: “We agree with the district court that possibilities for upgrading software located on another person’s computer are irrelevant to determining whether vicarious liability exists.”

The *MGM v. Grokster* ruling suggests that, with careful attention to the relevant legal principles, indirect liability can be avoided by P2P developers. Because this case may still be appealed to the Supreme Court, however, developers should exercise caution in relying on the ruling.

IV. Potential defenses against contributory and vicarious liability.

A. No direct infringer: “All of my users are innocent.”

If there is no direct infringement, there can be no indirect liability. Consequently, if a peer-to-peer developer can establish that no users in the network are sharing copyrighted works without authorization, this would be a complete defense to any contributory or vicarious infringement claims. Unfortunately, this may be extremely difficult to demonstrate, given the decentralized nature of most P2P networks and the wide variety of uses to which they may be put. Even if file sharing by some users is privileged under the “fair use” doctrine or another statutory exception to copyright, it will be very difficult to show that *every* use falls within such an exception. Nevertheless, in certain specialized networks that permit the sharing of only secure, authorized file types, this may be a viable defense.

B. The Betamax defense: “Capable of substantial noninfringing uses.”

As discussed above, the Supreme Court concluded in *Sony v. Universal* that contributory infringement liability could not reach the manufacturer of a device, so long as the device is “capable of substantial noninfringing use.”

Unfortunately, the “*Betamax* defense” has been under sustained legal attack in recent cases involving P2P technology. The various rulings have not always been consistent, creating considerable ambiguity. But all three of the major court rulings—*Napster*, *Aimster*, and *Grokster*—make it clear that developing a clear record of substantial noninfringing uses is critically important for software developers who fear they may be sued for contributory infringement.

The *Grokster* decision gives the clearest exposition of the requirements of the *Betamax* defense in the P2P context. According to that ruling, a court must first ascertain whether your technology is capable of substantial noninfringing uses. If it is capable of substantial noninfringing uses, then the copyright owner cannot prevail unless it can demonstrate that you knew about specific infringements at a time when you could have done something to prevent them.

There remain some unsettled questions, however. First, it is unclear whether the *Betamax* defense applies to both contributory and vicarious infringement claims, or only against the former. The Ninth Circuit in *Napster* limited the defense to contributory infringement claims, but a different court might rule otherwise. In addition, there is still some question about whether the

proportion of infringing and noninfringing uses can be a relevant factor in applying the *Betamax* defense. The *Grokster* decision says no, while the *Aimster* decision says yes.

The conflicting court interpretations of the “Betamax defense” have at least two important implications for P2P developers. First, they underscore the threat of vicarious liability—at least in the Ninth Circuit, a court will not be interested in hearing about your “substantial noninfringing uses” if you are accused of vicarious infringement. Accordingly, “control” and “direct financial benefit,” as described above, should be given a wide berth. This will likely reduce the attractiveness of business models built on an on-going “service” or “community-building” model, to the extent that these models allow the provider to control user activity (i.e., terminate or block users) and create value by attracting a large user base.

Second, with respect to contributory infringement, the *Grokster* ruling strongly favors technology implementations that leave the software vendor with no ability to control user activities after the software has been downloaded and installed. After all, once you receive specific notices from copyright owners about infringing activities, you may have a legal duty to “do something” about the infringing activities. In that context, the scope of your obligation will depend on the extent that the architecture allows you to “do something.” In cases involving truly decentralized P2P networks, there may be nothing a software developer or vendor can do to stop infringing activities (just as Xerox cannot control what a photocopier is used for after it is sold). To the extent you want to minimize your obligation to police the activities of end-users, this counsels strongly in favor of software architectures that leave you with no ability to control, disable, or influence end-user behavior once the software has been shipped to the end-user.

Copyright owners have recently begun arguing that technologists have a duty to *redesign* technologies once they are put on notice regarding infringing end-users. The *Grokster* ruling strongly rejected this view, but future developments are difficult to predict. Breaking developments on this front may have important ramifications for P2P developers and should be closely monitored.

C. The DMCA Section 512 “safe harbors.”

In 1998, responding in part to the concerns of ISPs regarding their potential liability for the copyright infringement of their users, Congress enacted a number of narrow “safe harbors” for copyright liability. These safe harbors appear in section 512 of the Copyright Act, which in turn appears in title 17 of the U.S. Code (17 U.S.C. § 512). These safe harbors apply only to “online service providers,” and only to the extent that the infringement involves four functions: transitory network transmissions, caching, storage of materials on behalf of users (e.g., web hosting, remote file storage), and the provision of information location tools (e.g., providing links, directories, search engines).

Each of these functions, however, is narrowly defined by the statute (e.g., they don’t cover what you’d think) and reflects the state of the art in 1998. Because Congress did not anticipate peer-to-peer file sharing when it enacted the safe harbors, many P2P products may not fit within the four enumerated functions. For example, according to an early ruling by the district court¹ in the *Napster* case, an online service provider cannot use the “transitory network

¹ See *A&M Records v. Napster*, No. C 99-5183 MHP (N.D. Cal. filed May 5, 2000) (available at <http://www.eff.org/IP/P2P/Napster/DMCA_Ruling.php>)

transmission” safe harbor unless the traffic in question passes through its own private network. Many P2P products will, by their very nature, flunk this requirement, just as Napster did.

In addition to being limited to certain narrowly-circumscribed functions, the safe harbors are only available to entities that comply with a number of complex, interlocking statutory requirements:

- The online service provider (“OSP”) must (1) adopt, reasonably implement, and notify its users of a policy of terminating the accounts of subscribers who are repeat infringers; and (2) accommodate and not interfere with “standard technical measures” that have been widely adopted on the basis of industry-wide consensus.
- The OSP must designate a “copyright agent” to receive notices of alleged copyright infringement, register the agent with the Copyright Office, and place relevant contact information for the agent on its web site.
- The OSP must, upon receiving a notification of infringement from a copyright owner, expeditiously remove or disable access to the infringing material (“notice and takedown”).
- The OSP must not have known about the infringement, or been aware of facts from which such activity was apparent (i.e., if you take a “head in the sand” approach, you lose the safe harbor).
- The OSP must not receive a direct financial benefit from infringing activity, in a situation where the OSP controls such activity.

In the final analysis, qualifying for any of the DMCA safe harbors requires careful advance attention to the legal and technical requirements and obligations that the statute imposes. As a result, any P2P developer who intends to rely on them should seek competent legal counsel at an early stage of the development process—an after-the-fact, “bolt on” effort to comply is likely to fail (as it did for Napster).

D. The DMCA ban on circumvention technologies.

One recent addition to the copyright landscape deserves special attention. Section 1201 of the Copyright Act, enacted as part of the Digital Millennium Copyright Act (“DMCA”), makes it unlawful to “circumvent” any technology aimed at protecting a copyrighted work. In addition, the development, distribution or use of circumvention technology or devices is, with only narrow exceptions, also unlawful. For example, if a copyright owner uses a digital rights management (“DRM”) solution to protect a song, it would be unlawful for anyone to crack the encrypted file without the copyright owner’s permission, or to build or distribute a software tool designed to crack the file.

Of course, circumvention technology is not a necessary part of a P2P file-sharing network. Today’s P2P protocols, such as FastTrack and gnutella, simply facilitate file transfers, leaving the file itself, whether encrypted or not, unaltered. Nevertheless, as copyright owners begin to deploy DRM and watermarking systems, there may be interest in integrating circumvention tools with file-sharing tools. In particular, any “spoofing” of authentication handshakes between applications can create concerns (*see, e.g., Real Networks v. Streambox*, 2000 U.S. Dist. LEXIS 1889 (W.D. Wash. Jan. 18, 2000)).

V. Lessons and guidelines for P2P developers.

A few general guidelines for P2P developers can be derived from the discussion above. These are steps you can take that may: (1) reduce the chance that your project will be an easy, inviting target for copyright owners; and (2) minimize the chances that your case will become the next legal precedent that content owners can use to threaten future innovators.

Of course, because the relevant legal principles are still in flux, these guidelines represent merely one, general analysis of the legal landscape. Please consult with an attorney regarding your precise plans.

1. Make and store no copies.

This one may be obvious, but remember that if you make or distribute any infringing copies (even if only in RAM) of copyrighted works, you may be held liable as a direct infringer. In that case, a plaintiff need not prove “control” or “knowledge” or “financial benefit” or “material contribution”—the fact that copies were made on your equipment can be enough to establish direct infringement liability.

Of course, this shouldn't be a problem for most P2P developers, since the great insight of peer-to-peer architectures is that the actual resources being shared need not pass through any central server. Nevertheless, be careful where caching or similar activities are concerned.

2. Your two options: total control or total anarchy.

In the wake of recent decisions on indirect copyright liability, it appears that copyright law has foisted a binary choice on P2P developers: either build a system that allows for thorough monitoring and control over end-user activities, or build one that makes such monitoring and control impossible.

Contributory infringement arises when you have “knowledge” of, and “materially contribute” to, someone else's infringing activity. The chief battleground for contributory infringement in the P2P cases so far has been the “knowledge” issue, with copyright owners dumping box-loads of infringement notices on software developers, hoping to create “knowledge” of the infringing activities of end-users. The Ninth Circuit ruling in *MGM v. Grokster* makes it clear that if there is nothing you can do to stop the infringing activities when the notices arrive (because the software enables you to control neither access to the network nor end-user activities, for example), then you will not be held liable for contributory infringement based on those after-the-fact notices. (After all, merely notifying Xerox that one of its photocopiers is being misused at a neighborhood Kinko's would not suddenly make Xerox a contributory infringer—Xerox has no ability to disable, repossess, or remotely control its photocopiers once they have been sold.)

The law of contributory infringement therefore presents a developer with a binary choice: you can either include mechanisms that enable monitoring and control of user activities (and use them to stop allegedly infringing activity when you receive complaints), or choose a truly decentralized architecture that will convince a judge that such monitoring and control is impossible without extensive redesign. (Copyright owners have begun arguing that you must at redesign future versions of your software to prevent infringement. This remarkable argument was firmly rejected by the Ninth Circuit in *Grokster*.)

The *Napster* and *Grokster* courts' vicarious liability analyses also counsel for either a total control or total anarchy approach. Vicarious liability requires that the plaintiff demonstrate that the defendant you "control," and receive "benefit" from, someone else's infringing activity. The "benefit" element will be difficult to resist in many P2P cases (at least for commercial products)—so long as the software permits or enables the sharing of infringing materials, this will serve as a "draw" for users, which can be enough "benefit" to result in liability according to some precedents.

So the fight will likely center on the "control" element. The *Napster* court found that the right to block a user's access to the service was enough to constitute "control." The court also found that Napster had a duty to monitor the activities of its users "to the fullest extent" possible. In contrast, the *Grokster* court found that where a P2P software vendor has no ability to control access to the network, or to control what users search for, share or download, it cannot be held vicariously liable for their infringements. These decisions taken together suggest that, in order to avoid vicarious liability, a P2P developer would be wise to choose an architecture that will convince a judge that control over end-user activities is impossible.

3. Better to sell stand-alone software products than on-going services.

Vicarious liability is perhaps the most serious risk facing P2P developers. Having the power to terminate or block users from accessing the network can constitute enough "control" to justify imposing vicarious liability. Add "financial benefit" in the form of a business model that depends on a large user base, and you're well on your way to joining Napster as a vicarious infringer. This is true even if you are completely unaware of what your users are up to—the pairing of "control" and "financial benefit" can be enough.

Of course, most "service" business models fit this "control" and "benefit" paradigm. What this means is that, after the *Napster* decision, if you offer a service, you may have to monitor and police your users if you want to escape liability. If you want to avoid monitoring obligations, you'll have to give up on anything that smacks of "control."

Vendors of stand-alone software products may be in a better position to resist monitoring obligations and vicarious liability. After Sony sells a VCR, it has no control over what the end-user does with it. Neither do the makers of photocopiers, optical scanners, or audio cassette recorders. Having built a device with many uses, only some of which may infringe copyrights, the typical electronics manufacturer has no way to "terminate" end-users or "block" their ability to use the device. They also have no ability to repossess or remotely modify the device after purchase. The key here is to let go of any control you may have over your users—no remote kill switch, automatic update feature, contractual termination rights, or other similar mechanisms. (Although the *Grokster* court found that the ability to update software already deployed to end-users is irrelevant to establishing "control" for vicarious liability, prudence suggests that vendors give anything that smacks of "control" a wide berth.)

4. What are your substantial noninfringing uses?

If your product is intended to work solely (or best) as a mechanism for copyright piracy, you're asking for legal trouble. More importantly, you're thinking too small. Almost all peer-to-peer systems can be used for many different purposes, some of which the creators themselves fail to appreciate.

So create a platform that lends itself to many uses. Actively, sincerely, and enthusiastically promote the noninfringing uses of your product. Gather testimonials from noninfringing users. The existence of real, substantial noninfringing uses will increase the chances that you can invoke the *Betamax* defense if challenged in court.

5. Do not promote infringing uses.

Do not promote any infringing uses. Be particularly careful with marketing materials and screenshot illustrations—attorneys are very good at making hay out of the fact that Beatles songs were included in sample screenshots included in marketing materials or documentation. Have an attorney review these materials closely.

6. Disaggregate functions.

Separate different functions and concentrate your efforts on a discrete area. In order to be successful, peer-to-peer networks will require products to address numerous functional needs—search, bootstrapping, namespace management, security, dynamic file redistribution, to take a few examples. There's no reason why one entity should try to do all of these things. In fact, the creation of an open set of protocols (or at least APIs), combined with a competitive mix of interoperable, but distinct, applications is probably a good idea from a product-engineering point of view.

This approach may also have legal advantages. If Sony had not only manufactured VCRs, but also sold all the blank video tape, distributed all the TV Guides, and sponsored clubs and swap meets for VCR users, the *Betamax* case might have turned out differently. Part of Napster's downfall was its combination of indexing, searching, and file sharing in a single piece of software. If each activity is handled by a different product and vendor, on the other hand, each entity may have a better legal defense to a charge of infringement.

A disaggregated model, moreover, may limit what a court can order you to do to stop infringing activity by your users. As the *Napster* court recognized, you can only be ordered to police your own "premises"—the smaller it is, the less you can be required to do.

Finally, certain functions may be entitled to special protections under the "safe harbor" provisions of the DMCA. Search engines, for example, enjoy special DMCA protections. Thus, the combination of a P2P file sharing application with a third party search engine might be easier to defend in court than Napster's integrated solution.

7. Don't make your money from the infringing activities of your users.

Avoid business models that rely on revenue streams that can be directly traced to infringing activities. For example, a P2P file-sharing system that includes a payment mechanism might pose problems, if the system vendor takes a percentage cut of all payments, including payments generated from sales of bootleg Divx movie files.

8. Give up the EULA.

Although end-user license agreements ("EULAs") are ubiquitous in the software world, copyright owners have attempted to use them in P2P cases to establish "control" for vicarious liability purposes. On this view, EULAs represent "contracts" between vendors and their users, and thus give software vendors legal control over end-user activities. EULAs that permit a vendor to terminate at any time for any reason may raise particular concerns, insofar as they may leave the impression that a vendor has the legal right to stop users from using the software.

P2P software vendors should consider distributing their code without a EULA. Even without a EULA, a software developer retains all of the protections of copyright law to prevent unauthorized duplication and modifications. (After all, books, DVDs, and music CDs are all sold without any EULA, and copyright law certainly protects them.)

9. No direct customer support.

Any evidence that you have knowingly assisted an end-user in committing copyright infringement will be used against you. In the P2P cases so far, one source for this kind of evidence is from customer support channels, whether message board traffic, instant messages or email. A user writes in, explaining that the software acted strangely when he tried to download *The Matrix*. If you answer him, copyright owners will make it seem that you directly assisted the user in infringement, potentially complicating your contributory infringement defense.

So let the user community support themselves in whatever forums they like. (This will be easier if you are open source, of course.) Your staff can monitor forums and create FAQs that assist users with common problems, but avoid engaging in one-on-one customer support.

10. Be open source.

In addition to the usual litany of arguments favoring the open-source model, the open source approach may offer special advantages in the P2P realm. It may be more difficult for a copyright owner to demonstrate "control" or "financial benefit" with respect to an open source product. After all, anyone can download, modify and compile open source code, and no one has the ability to "terminate" or "block access" or otherwise control the use of the resulting applications. Any control mechanisms, even if added later, can simply be removed by users who don't like them.

"Financial benefit" may also be a problematic concept where the developers do not directly realize any financial gains from the code (as noted above, however, the *Napster* court has embraced a very broad notion of "financial benefit," so this may not be enough to save you). Finally, by making the most legally dangerous elements of the P2P network open source (or relying on the open source projects of others), you can build your business out of less vulnerable ancillary services (such as search services, bandwidth enhancement, file storage, meta-data services, etc.).

* * *

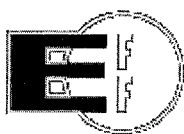
About the Author: Fred von Lohmann is a senior staff attorney with the Electronic Frontier Foundation, specializing in intellectual property issues. He is counsel to StreamCast Networks in the *MGM v. Grokster* litigation, one of the leading cases addressing copyright and peer-to-peer file sharing. In addition to litigation, he is involved in EFF's efforts to educate policy-makers regarding the proper balance between intellectual property protection and the public interest in fair use, free expression, and innovation.

Copyright Information: This work licensed under the Creative Commons Attribution-NoDerivs-NonCommercial License.² Contact the author (google: "fred von lohmann") for all other permissions.

© 2004 EFF v. 4.0

² Terms available at: <<http://creativecommons.org/licenses/by-nd-nc/1.0/>>.

EXHIBIT E



About EFF	Cases	Press Room	DeepLinks	Action Center	Join EFF	Sitemap Calendar
---------------------------	-----------------------	----------------------------	---------------------------	-------------------------------	--------------------------	--

[> Home](#) [> About](#) [> EFF's History](#)

Enter search terms

Search EFF

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 a 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 Kapur, 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

Contents

[EFF in the News](#)
[miniLinks](#)
[Pioneer Awards](#)
[EFF Victories](#)
[EFF White Papers](#)

EFFector

Subscribe to EFFector!
 [our free email newsletter]

Email:

Zip / Postal Code
(optional)

Subscribe!

» [EFFector Archive](#)

Topics

[Anonymity](#)
[Biometrics](#)
[Bloggers' Rights](#)
[Broadcast Flag](#)
[CALEA](#)
[CAPPS II](#)
[Censorship](#)
[Copyright Law](#)
[Digital Rights](#)

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 ecommerce, 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

[Management](#)
[DMCA](#)
[Domain names](#)
[E-voting](#)
[File-sharing](#)
[Filtering](#)
[FTAA](#)
[Intellectual Property](#)
[International](#)
[Internet governance](#)
[ISP legalities](#)
[Licensing/UCITA](#)
[Linking](#)
[Patents](#)
[Pending legislation](#)
[Privacy](#)
[Public records/FOIA](#)
[Reverse engineering](#)
[RFID](#)
[Spam](#)
[States](#)
[Surveillance](#)
[USA PATRIOT Act](#)
[Wireless](#)
[WIPO](#)

EFF en Español

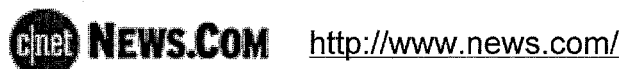
[Recursos e información de EFF en Español](#)

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.

Find out more about our current hot cases and issues on our [home page](#) or at <http://www.eff.org/about/>

[HOME](#) | [CASES](#) | [ACTION CENTER](#) | [PRESS ROOM](#) | [ABOUT THE EFF](#) | [DONATE](#) | [VOLUNTEER](#) | [PRIVACY POLICY](#)

EXHIBIT F



Google cache raises copyright concerns

By Stefanie Olsen

http://news.com.com/Google+cache+raises+copyright+concerns/2100-1032_3-1024234.html

Story last modified Wed Jul 09 13:28:00 PDT 2003

Like other online publishers, The New York Times charges readers to access articles on its Web site. But why pay when you can use Google instead?



[Read more about search engines' reach](#)

Through a caching feature on the popular Google search site, people can sometimes call up snapshots of archived stories at NYTimes.com and other registration-only sites. The practice has proved a boon for readers hoping to track down Web pages that are no longer accessible at the original source, for whatever reason. But the feature has recently been putting Google at odds with some unhappy publishers.

"We are working with Google to fix that problem--we're going to close it so when you click on a link it will take you to a registration page," said Christine Mohan, a spokeswoman at New York Times Digital, the publisher of NYTimes.com. "We have established these archived links and want to maintain consistency across all these access points."

Google offers publishers a simple way to opt out of its temporary archive, and scuffles have yet to erupt into open warfare or lawsuits. Still, Google's cache links illustrate a slippery side of innovation on the Web, where cool new features that seem benign on the surface often carry unintended consequences.

The issue is particularly relevant at Google, a company that prides itself on creativity and routinely floats trial balloons for new features and services. Its culture of innovation may become increasingly risky as Google, which draws millions of visitors to its site daily and redirects them to others through secretive search formulas, cements its position as one of the most popular and powerful companies on the Web.

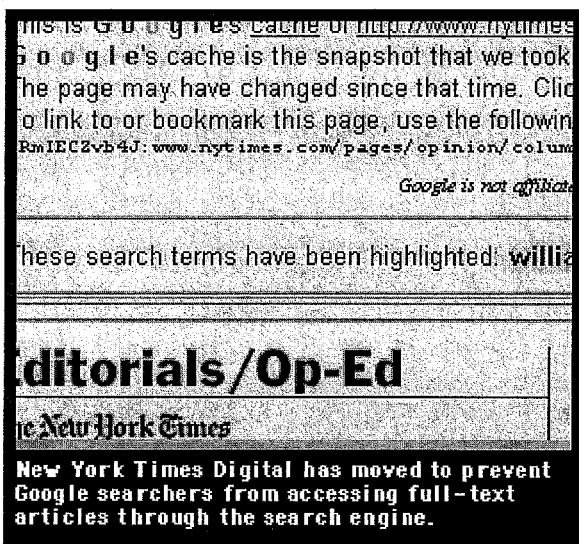
At the heart of Google's caching dilemma lies a thorny legal problem involving a core Web technology: When is it acceptable to copy someone else's Web page, even temporarily?

A phantom life for dead pages

Google's cache, a feature introduced in 1997, is unique among commercial search engines, but it's not unlike other archival sites on the Web that keep digital copies of Web pages. Google's relatively little-known feature lets people access a copy of almost any Web page, within Google's own site, in the form it was in whenever last indexed by the search giant. That could mean the page accessed is either minutes or months old, depending on when Google last crawled it.

Unlike formal Web archive projects, Google says its cache feature does not attempt to create a permanent historical record of the Web. Rather, the company actively seeks to delete dead links; once a Web page disappears, the search engine seeks to purge that record and any related cached page as quickly as possible.

Still, Google's cached pages have proven to be a treasure trove for investigators seeking to recover data pulled from public Web sites. In one high-profile example, security and privacy expert Richard Smith copied Web pages detailing the backgrounds of Dr. John Poindexter, head of the Pentagon's Information Awareness Office (IAO), and other officials, from the Google cache days after they were removed from the IAO Web site. The pages were deleted after public reports surfaced on the office's development of a massive computer system to spy on Americans and potential terrorists.



"When something's been yanked, Google cache is a good place to grab it and save for posterity, because you don't know how long Google will have it," said Smith.

Google claims its caching feature benefits Web surfers by letting them access a site that may be malfunctioning or offline. Also, its cached pages highlight terms that match a search query "to make it easier for users to find relevant information," according to a spokesman at the Mountain View, Calif.-based company.

Lawyers, start your search engines

As seemingly benign and beneficial as it is, some Web site operators take issue with the feature and

digitally prevent Google from recording their pages in full by adding special code to their sites. Among other arguments, they say that cached pages at Google have the potential to detour traffic from their own site, or, at worst, constitute trademark or copyright violations. In the case of an out-of-date news page in Google's cache, a Web publisher could even face legal troubles because of false data remaining on the Web but corrected at its own site.

For this reason, search experts and copyright lawyers expect the issue to come up in a court of law, joining the leagues of copyright disputes that have surfaced because of technology innovation.

"It's very much an issue that has yet to be tested, and I fully expect that it will be," said Danny Sullivan, industry pundit and editor of Search Engine Watch.

Admittedly, Google's cache is like any number of backdoors to information on the Web. For example, proxy servers can be the keys to a site that is banned by a visitor's hosting Web server. And technically, any time a Web surfer visits a site, that visit could be interpreted as a copyright violation, because the page is temporarily cached in the user's computer memory.

The digital universe is constantly changing, but its content can be either fleeting or permanent. Several Web sites, including the Internet Archive Wayback Machine and the Sept. 11 Digital Archive, have surfaced to preserve information on the Web and to keep permanent historical

accounts of events and Web pages. Yet, many more pages, and even those in Google's cache, are eventually lost in the digital ether. The average lifespan of a Web site is 100 days, according to estimates by the Internet Archive.

Still, copyright lawyers and industry experts say that there are legally uncharted waters around a commercial caching service.

"Many of us copyright lawyers have been waiting for this issue to come up: Google is making copies of all the Web sites they index and they're not asking permission," said Fred von Lohman, an attorney at the Electronic Frontier Foundation. "From a strict copyright standpoint, it violates copyright."

Most search engines make a statistical record of a Web page when they "spider" it, or use "robots" to scan the page for meaning or context to related queries. For example, the engine can point to specific information contained on a page that's related to a search term, but it often doesn't have the complete picture of the page. Google goes one step beyond, however, by taking a digital picture of pages and making it available to visitors in cached links. Those pictures exist temporarily on its site until the next time Google crawls that particular page, which can happen in a few days or in six weeks or more.

Legally, what could differentiate Google from other archival sites that record pages is that it is a commercial site and that it has enormous scope and influence on the Web.

Special Report

The Google gods ▶

Does the search engine's power threaten the Web's independence?

But what's kept the feature off most Web sites' radar is that, anecdotally, most people don't click on the cache. Even Google says people only "occasionally" click its cached links. If more people did, Web publishers might lose visitors--and potentially advertising dollars, which no one can afford to lose as Web publishing gets back on its feet.

Practically speaking, Web sites can "opt out," or include code in their pages that bars Google from caching the page. A tag to exclude "robots" such as "www.nytimes.com/robots.txt" or "NOARCHIVE" typically does the job. And that's largely what's kept the cache feature from being controversial.

Search Engine Watch's Sullivan said that, even though some publishers are wary of the caching feature, many don't block Google's robots for fear of losing favor in the company's powerful search rankings. He said some Webmasters believe there's a stigma associated the "no cache" tag, because many sites that use it have been accused of attempting to use banned methods to manipulate Google's rankings. Google said the "no cache" tag does not affect rankings.

Cache now, pay later?

Some legal experts say Google may be on shaky ground by caching first and asking questions later.

A provision in the Digital Millennium Copyright Act (DMCA) includes a safe harbor for Web caching. The safe harbor is narrowly defined to protect Internet service providers that cache Web pages to make them more readily accessible to subscribers. For example, AOL could keep a local copy of high-trafficked Web pages on its servers so that its members could

access them with greater speed and less cost to the network. Various copyright lawyers argue that safe harbor may or may not protect Google if it was tested.

"Most people agree that the caching exception in the DMCA is obsolete," von Lohman said. "I don't think it would cover Google's cache. Google is not waiting for users to request the page. It spiders the page before anyone asks for it."

Still, other lawyers argue that Google's practice would be protected by fair-use laws. A judge might look at the market impact of Google's caching and find that it's valuable, given that it could ultimately drive traffic to the cached site. Or the reverse could be true, depending on the nature of the page.

For its part, Google is confident that the service is within the law. "We've evaluated this from a legal perspective, including copyright law, and have determined that Google's cached page service complies with the law," a Google spokesman said.

A similar issue has played out in the courts in an image-searching case, *Kelly v. Arriba Soft*, filed in April 1999. Leslie Kelly, a photographer, sued the company for copyright infringement when its visual search finder cataloged thumbnails and full-sizes of his digital photos and made them accessible via its own search engine.

The court initially ruled against Kelly based on the "established importance of search engines," but Kelly appealed and won. In Feb. 2002, the 9th U.S. Circuit Court of Appeals held that Arriba's use of thumbnail images of Kelly's photos was fair use, but its display of full-size images was not fair use, because it was likely to harm the market for Kelly's work by reducing visits to his Web site and by allowing free downloads. But the opinion on full-size images was remanded by the 9th Circuit Court this week and is set to go to trial in the lower court of central California.

Judith Jennison, defense lawyer for Arriba Soft, said that one of the issues in the case is that Arriba Soft, in its process of indexing the Web, made copies of Kelly's photos and saved them for 24 hours in its servers. The 9th Circuit Court agreed that creating that copy is fair use under copyright law, she said, adding that there would be a slightly different analysis in a case related to Google. Also, the fact that the search site has an opt-out program would likely illustrate that the market for original copyrighted works can be protected, which is a significant factor in fair-use analysis.

"In Google's case, the result would likely be the same, because the temporary caching for indexing purposes would be fair use per *Kelly v. Arriba Soft*," Jennison said.

While it seems that many Net publishers haven't formed an official policy on Google caching, they say they are examining how it affects their business.

Randy Stearns, executive producer for ABCNews.com, said he's somewhat concerned about his company's news pages being archived temporarily on Google, because readers might access information that is not up-to-date or, in the worst case for a daily news outlet, is inaccurate. Theoretically, if a news report was issued with errors and was subsequently fixed on the publisher's site, but the erroneous report still existed in a cached version, it could raise legal issues for the publisher, he said.

Other publishers dismiss any threat, saying that not enough people actually click on those links to be a detriment to traffic. "People who find objection to what Google does likely spend enormous amounts (of time) on their content and refresh it regularly," said Harry Lin, head of ABC.com.

Special report

Search and destroy ▶

Microsoft's path to expanding Windows empire leads to search king Google.

In contrast with the priorities of some news publishers, Web archivists say preserving pages as they first appeared can offer important documentary records for historians and others.

Brewster Kahle, head of the Wayback Machine, said many people use its archive for patent research, or "prior art" searches. Designers and students have used the archive to see the evolution of Web site design and display, he added, and the Smithsonian has used subsets of the collection in the Presidential Election memorabilia room.

News publishers agree that Google's cache is also valuable if, for example, their site was inaccessible because of technical difficulties.

"It's a great, wonderful feature, and I don't know that copyright laws would protect them," said Search Engine Watch's Sullivan. "But most people are concerned about getting into Google, not getting out of it."

Copyright ©1995-2005 CNET Networks, Inc. All rights reserved.

1 **PROOF OF SERVICE**

2 STATE OF CALIFORNIA, COUNTY OF LOS ANGELES

3 I am employed in the county of Los Angeles, State of California. I am over the age of 18,
4 and not a party to the within action; my business address is Mitchell Silberberg & Knupp LLP, ,
Los Angeles, California 90064-1683.

5 On October 24, 2005, I served the foregoing document(s) described as **DECLARATION**
6 **OF ELENA SEGAL IN OPPOSITION TO MOTION OF ELECTRONIC FRONTIER**
7 **FOUNDATION FOR LEAVE TO FILE BRIEF AMICUS CURIAE** on the parties in this
action by placing a true copy thereof enclosed in sealed envelopes addressed as follows, and
taking the action described below:

8 Andrew P. Bridges, Esq.
9 Winston & Strawn
10 101 California Street, Suite 3900
San Francisco, CA 94111-5882

Mark T. Jansen, Esq.
Townsend and Townsend and Crew LLP
Two Embarcadero Center, 8th Floor
San Francisco, CA 94111

11 Fred Von Lohmann
12 Electronic Frontier Foundation
454 Shotwell St.
San Francisco, CA 94110

13 ☐ **BY MAIL:** I deposited such envelope in the mail at Los Angeles, California. The
14 envelope was mailed with postage thereon fully prepaid.

15 ☐ **BY FAX:** Instead of placing a copy of the document in a sealed envelope, I sent a copy
16 of the above-described document(s) via telecopier to each of the individuals set forth
above, at the following facsimile telephone numbers:

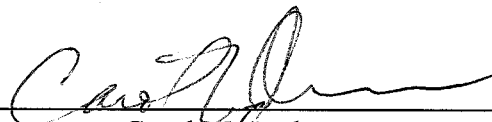
17 ☐ **BY OVERNIGHT MAIL:** I deposited the above-described document(s) with ___ in the
18 ordinary course of business, by depositing the document(s) in a box regularly maintained
by ___ or delivering the document(s) to an authorized driver for the carrier, in an
19 envelope designated by the carrier with delivery fees provided for, addressed as shown
above.

20 ☐ **BY PERSONAL DELIVERY:** I caused personal delivery by _____ of the
document(s) listed above to the person(s) at the address(es) set forth above.

21 ☒ **BY PLACING FOR COLLECTION AND MAILING:** I sealed and placed the
22 envelope(s) for collection and mailing following ordinary business practices. I am readily
familiar with the firm's practice for collection and processing of correspondence for
23 mailing with the United States Postal Service. Under that practice it would be deposited
with the U.S. Postal Service on that same day with postage thereon fully prepaid at , Los
24 Angeles, California 90064-1683 in the ordinary course of business.

25 Executed on October 24, 2005 at Los Angeles, California.

26 I declare that I am employed in the office of a member of the bar of this court at whose
direction the service was made.


Carol McAndrew