Securing the Open Campus Network
Resisting Copyright Closure

Wendy Seltzer, wendy@seltzer.org
http://wendy.seltzer.org/
Berkman Center for Internet & Society at Harvard University
American University Washington College of Law
Securing the eCampus, Nov. 11 2008
Un ragazzo chiamato Bi, Flickr
Overload

- When copyright is conflated with security
  - Fewer resources remain to address other security threats
  - Students take security warnings less seriously
  - Neither security nor copyright benefits
Securing Openness
We the People

Article 1

Section 1. All legislative Powers herein granted shall be vested in a Congress of the United States, which shall consist of a Senate and House of Representatives.

Section 2. The Congress shall assemble at least once in every Year, and such Meeting shall lie on the 1st Day of January, unless they shall by Law prohibit the Meeting to be elsewhere.

Section 3. Every Bill, when passed by the Senate and House of Representatives, shall, before it becomes a Law, be presented to the President of the United States; if he approve, he shall sign it...
• Copyright holders overreach
  – Conflate copyright infringement with security
• Copyright holders err
National Cyber Alert System
Cyber Security Tip ST05-007

Risks of File-Sharing Technology

File-sharing technology is a popular way for users to exchange, or "share," files. However, using this technology makes you susceptible to risks such as infection, attack, or exposure of personal information.

What is file sharing?
File sharing involves using technology that allows internet users to share files that are housed on their individual computers. Peer-to-peer (P2P) applications, such as those used to share music files, are some of the most common forms of file-sharing technology. However, P2P applications introduce security risks that may put your information or your computer in jeopardy.

What risks does file-sharing technology introduce?

- **Installation of malicious code** - When you use P2P applications, it is difficult, if not impossible, to verify that the source of the files is trustworthy. These applications are often used by attackers to transmit malicious code. Attackers may incorporate spyware, viruses, Trojan horses, or worms into the files. When you download the files, your computer becomes infected (see Recognizing and Avoiding Spyware and Recovering from Viruses, Worms, and Trojan Horses for more information).

- **Exposure of sensitive or personal information** - By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been
Tuesday, July 24, 2007

Communications and Information Technology

Committee Holds Hearing on Inadvertent File Sharing over Peer-to-Peer Networks

On Tuesday, July 24, 2007, the Committee held a hearing on inadvertent file sharing over peer-to-peer (P2P) networks, the impact of such sharing on consumers, corporations, and government entities, and whether such sharing creates privacy or security risks for users. Witnesses included officials from the Federal Trade Commission (FTC), the U.S. Patent and Trademark Office (PTO), the Department of Transportation (DOT), as well as independent experts experienced in P2P issues. A preliminary transcript of this hearing is now available.

The PTO Report.

In 2003, the Committee held a hearing to investigate and understand the uses and risks of P2P networks, finding that highly personal data such as tax returns and financial information were being shared with millions of computer users without the knowledge of their owners. After the Committee’s 2003 hearing, the P2P industry adopted a voluntary Code of Conduct to prevent inadvertent disclosures of sensitive information. In March 2007, however, the PTO released a report suggesting that inadvertent file sharing may still be a serious problem and that the industry might not be living up to its promise to address this issue voluntarily.

The Committee’s Findings.

In response to the PTO report, the Committee staff conducted its own investigation into the question of whether...
NFL / DMCA
February 08, 2007

MY FIRST YOUTUBE: SUPER BOWL HIGHLIGHTS OR LOWLIGHTS

I snipped the copyright warning out of the weekend's Super Bowl broadcast as an example for my copyright class of how far copyright claimants exaggerate their rights.

This telecast is copyrighted by the NFL for the private use of our audience. Any other use of this telecast or of any pictures, descriptions, or accounts of the game without the NFL's consent, is prohibited.

Let's see whether the video, clear fair use, gets flagged by a copyright bot.
DMCA § 512. Limitations on liability relating to material online

• (c) Information Residing on Systems or Networks At Direction of Users.—
  – (1) In general.— A service provider shall not be liable for monetary relief...for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider, if the service provider—
    – (A)(i) does not have actual knowledge that the material or an activity using the material on the system or network is infringing;
    – ... (iii) upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;
MY FIRST DMCA TAKEDOWN

That didn't take long. On Feb. 8, I posted to YouTube a clip taken from the Super Bowl: not the football, but the copyright warning the NFL said they tell you it's forbidden even to share "accounts of the game" without the NFL's consent.

Their copyright bot didn't seem to see the fair use in my educational excerpt, so YouTube just sent me their boilerplate takedown. Time to be notified.

-------- Original Message --------
Subject: Video Removed: Copyright Infringement
Date: Tue, 13 Feb 2007 15:43:24 -0800 (PST)
From: DMCA Complaints
To: peppercornconsider

Dear Member:

This is to notify you that we have removed or disabled access to the following material as a result of a third-party notification by National Football League claiming that this material is infringing:

Super Bowl Highlights: (http://www.youtube.com/watch?v=a4uCWr1UJo)

Please Note: Repeat incidents of copyright infringement will result in the deletion of your account and all videos uploaded to that account. In order to avoid future strikes against your account, please delete any videos to which you do not own the rights, and refrain from uploading additional videos that infringe on the copyrights of others. For more information about YouTube's copyright policy, please read the "Copyright Tips" guide: http://www.youtube.com/t/howto_copyright.

If you elect to send us a counter notice, to be effective it must be a written communication provided to our designated agent that includes substantially the following (please consult your legal counsel or see 17 U.S.C. Section 512(g)(3) to confirm these requirements):

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

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

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

(D) The subscriber's name, address, and telephone number, and a statement that
October 13, 2008

Dear Mr. Hurley, and Ms. Levine, and Mr. Patry:

By providing a platform for political candidates and the American public to post, view, share, discuss, comment on, mash-up, re-mix, and argue over campaign-related videos, YouTube has played a prominent and overwhelmingly positive role in the 2008 election. YouTube is to be congratulated on the groundbreaking contributions it has made to the political discourse, including through the CNN/YouTube primary debates.

We write, however, to alert you to a problem that has already chilled this free and uninhibited discourse, and to propose a solution. First, the problem: overreaching copyright claims have resulted in the removal of non-infringing campaign videos from YouTube, thus silencing political speech. Numerous times during the course of the campaign, our advertisements or web videos have been the subject of DMCA takedown notices regarding uses that are clearly privileged under the fair use doctrine. The uses at issue have been the inclusion
Hearing: “An Update – Piracy on University Networks”

Thursday 03/08/2007 - 2:00 PM
2141 Rayburn House Office Building
Subcommittee on Courts, the Internet, and Intellectual Property
By Direction of the Chairman

Hearing Information

Hearing PDF (Serial No. 110-29)

Witness List

Jim Davis
Associate Vice Chancellor for Information Technology
University of California Los Angeles, CA (UCLA)

Gregory J. Marchwinski
President and Chief Executive Officer
Red Lambda
Longwood, Florida

Gary H. Sherman
President
Recording Industry Association of America (RIAA)
Washington, D.C.

John C. Vaughn
Executive Vice President
Association of American Universities
Washington, D.C.
Hearings :: June 5, 2007

The Role of Technology in Reducing Illegal Filesharing: A University Perspective

Witness Panel

From L-R: Dr. Wight, Dr. Sannier, Mr. Ikezoye, Ms. Elzy, & Dr. Jackson

For information on witnesses, use links at left.
DMCA§ 512. Limitations on liability relating to material online

• (a) Transitory Digital Network Communications. — A service provider shall not be liable for monetary relief ... for infringement of copyright by reason of the provider’s transmitting, routing, or providing connections for, material through a system or network controlled or operated by or for the service provider, or by reason of the intermediate and transient storage of that material in the course of such transmitting, routing, or providing connections,

• (h) Subpoena To Identify Infringer.— NOT APPLICABLE to 512(a) providers (RIAA v. Verizon)
Copyright notifications and lawsuits

• DMCA takedowns
• Pre-litigation letters
  – Settlements
• John Doe complaints, followed by discovery subpoenas
  – University of Oregon, motion to quash on “undue burden” of identification
  – RIAA v. Tenenbaum
  – Capitol v. Thomas (making available)
Higher Education Act Reauth

INSTITUTIONAL AND FINANCIAL ASSISTANCE INFORMATION FOR STUDENTS.

...(P) institutional policies and sanctions related to copyright infringement, including--

- `(i) an annual disclosure that explicitly informs students that unauthorized distribution of copyrighted material, including unauthorized peer-to-peer file sharing, may subject the students to civil and criminal liabilities;
- `(ii) a summary of the penalties for violation of Federal copyright laws; and
- `(iii) a description of the institution's policies with respect to unauthorized peer-to-peer file sharing, including disciplinary actions that are taken against students who engage in unauthorized distribution of copyrighted materials using the institution's information technology system;
• PROGRAM PARTICIPATION AGREEMENTS.
• ... (29) The institution certifies that the institution—
• (A) has developed plans to effectively combat the unauthorized distribution of copyrighted material, including through the use of a variety of technology-based deterrents; and
• (B) will, to the extent practicable, offer alternatives to illegal downloading or peer-to-peer distribution of intellectual property, as determined by the institution in consultation with the chief technology officer or other designated officer of the institution.
Common Solutions Group report

- Audible Magic’s CopySense technology can most reliably identify only material that is registered with the vendor. Moreover, encryption can enable peer-to-peer traffic to bypass Audible Magic’s detection.
- Red Lambda’s cGrid technology detects traffic patterns rather than suppresses infringement. It requires considerable administrative expense and specific network architecture and management tools to translate identification of patterns into suppression of infringement.
- SafeMedia’s Clauseau technology blocks any communications its vendor deems undesirable. Network operators cannot override this blocking locally, even if the vendor blocks important non-infringing communications or otherwise disrupts network operations and effectiveness.

Current technologies can affect unauthorized sharing. However, their effectiveness is very limited, and they can suppress legitimate traffic along with infringing traffic. Fully deployed, they are also expensive. Although new approaches may yield effective, inexpensive, operationally benign infringement-suppression technologies in the future, implementing current technologies simply will increase tuition and research costs in higher education and degrade network performance while yielding only modest effects on unauthorized sharing.

It is important to note that the technology vendors do not necessarily agree with the views of CSG members. The logos below link to comments from the three vendors who participated in the workshop:

Business and policy challenges surrounding online media continue to evolve. So does the technology of online media distribution and sharing — both legal and illegal. Given the limited ability of technology to reduce unauthorized online sharing, which the CSG workshop made clear, effectively mitigating online copyright infringement requires much more than technological solutions. The challenge is fundamentally educational, and it must be addressed throughout formal and continuing education. The educational message will become far more effective as more appealing legal distribution mechanisms emerge. And the educational message must be reinforced by appropriate penalties for non-compliance that are fairly, diligently, and uniformly imposed, as is the case today within most research universities. CSG members remain eager to collaborate with other interested parties in a multi-faceted approach to the challenge.

2 June 2008
Copyright over-enforcement threatens security, privacy, innovation: Academic Freedom

- Financial costs are substantial, $150k/year
- Non-financial costs may be worse:
  - Monitoring deters exploration
  - Record retention risks breach
  - Deflection of security staff attention
  - Packet-filtering limits students’ and faculty’s ability to experiment without asking permission first
Float On

Rate: ★★★☆☆☆ 4,659 ratings
Views: 1,725,573

From: gothichik16
Added: October 29, 2006

Modest Mouse - Float On

URL: http://www.youtube.com/watch?v=HLkCBl3njo
Embed: Embedding disabled by request
Contains:
Content From: Sony/BMG

More From: gothichik16

Related Videos
Help Build The Commons

Join Jesse Dylan in supporting CC. Watch his new video about us, A Shared Culture.
Donate by November 21st and have the value of your gift doubled thanks to wikiHow.

$68,105 / $500,000 by Dec 31

Share, Remix, Reuse — Legally
Creative Commons provides free tools that let authors, scientists, artists, and educators easily mark their creative work with the freedoms they want it to carry. You can use CC to change your copyright terms from "All Rights Reserved" to "Some Rights Reserved."

We're a nonprofit organization. Everything we do — including the software we create — is free.

Learn More    FAQ
Collective Action

• Separately, we’re vulnerable. Together, we can change the law and tactics.
Responses

• Change the law
• Offer open access to your own copyrighted materials
• Hold the law’s drafters to their words, even as you educate
• Don’t keep records longer than necessary
Leave Openings for the Unexpected