

EFF Wins Landmark Ruling Freeing Promo CDs for Resale

(EFF.org Updates)

Submitted at 1/4/2011 6:15:44 PM

San Francisco - The U.S. Court of Appeals for the 9th Circuit has shot down bogus copyright infringement allegations from Universal Music Group (UMG), affirming an eBay seller's right to resell promotional CDs that he buys from secondhand stores and rejecting UMG's attempt to claim that a sticker on a CD created a license agreement forbidding resale.

Troy Augusto, represented by the Electronic Frontier Foundation (EFF) and the law firm Durie Tangri LLP, was sued by UMG for offering promo CDs for auction on eBay. At issue was whether the labels on the CDs, some of which stated that they were "promotional use only, not for sale," trumped Augusto's right to resell the CDs that he bought. Copyright's "first sale" doctrine prevents a copyright owner from restricting further sales or

uses of a work once title has passed.

In an opinion issued today, the appeals court held: "UMG transferred title to the particular copies of its promotional CDs and cannot maintain an infringement action against Augusto for his subsequent sale of those copies." The court noted that UMG did not maintain control of the CDs once it mailed them out, did not require the recipients to agree to the "conditions" it sought to impose with the not-for-sale label, and did not require return of the CDs if the recipient did not consent.

"This ruling frees promotional CDs from the shadow of copyright infringement claims, which is good news for music lovers," said EFF Intellectual Property Director Corynne McSherry. "But it also has broader ramifications. The court flatly rejected the argument that merely slapping a notice on a copyrighted work prevents the work

from ever being sold. It eliminates the risk of copyright infringement claims against later recipients -- regardless of whether they paid for the work." "The Ninth Circuit recognized an important principle: that you can't eliminate consumers' rights just by claiming there's a 'license agreement,'" said Joe Gratz of Durie Tangri, lead counsel for Mr. Augusto. "Once a copyrighted work is freely given, the copyright holder isn't in charge anymore. The copyright owner can't stop you from selling it or lending it to a friend."

For the full opinion in UMG v. Augusto:

<https://www.eff.org/files/filenode/umgvaugusto/UMGvAugusto9thCircuitOp...>

Contact:

Corynne McSherry
Intellectual Property Director
Electronic Frontier Foundation
corynne@eff.org

When Bad Patents Hurt Good People: Patent Threat Shuts Down Flight Planning Site

(EFF.org Updates)

Submitted at 1/5/2011 5:39:10 PM

In another example of using patents to stifle rather than promote innovation, a company called FlightPrep has come out fighting, threatening online flight planning sites with its newly obtained patent, and going so far as to sue at least one of those sites. [That patent](#), originally filed in 2001, allegedly covers a system for generating flight plans online, hardly a novel concept. And FlightPrep is now using its patent to attempt to extract royalty payments from small companies that have been providing such a service for years or put them out of business.

A FlightPrep lawsuit has already caused a well-established site, RunwayFinder, [to go dark](#) possibly permanently. Started in 2005, RunwayFinder allowed users to check out runway layouts and gather other information about airports, such as current weather, to help them make flight plans. The site's developer ran RunwayFinder out of his home and relied on ad revenue and [paypal donations](#) to keep the site up.

For now, RunwayFinder [continues to fight](#) the FlightPrep patent, but patent lawsuits can be long and incredibly expensive. Like many that have come before it such as the infamous [entertaining-a-cat-with-a-laser patent](#) this dispute is emblematic of a patent system that has lost sight of its purpose. Instead of spurring innovation by encouraging folks to invent new and better ways to do things, the system is often used to impede the development and use of interesting and valuable new tools and services.

Part of EFF's work to fight the chilling effects of bad patents on the public and consumer interests is our ongoing [Patent Busting Project](#). So far nine patents targeted by EFF have been busted, invalidated, narrowed, or had a reexamination granted by the Patent Office.

EFF Calls for Court to Affirm Downsized Copyright Damages

(EFF.org Updates)

Submitted at 1/4/2011 10:37:38 AM

San Francisco - The Electronic Frontier Foundation (EFF) urged a federal court Monday to affirm downsized damages in Sony v. Tenenbaum, a file-sharing case in which a jury originally ordered a college student to pay \$675,000 for infringing copyright in 30 songs. EFF was represented by the Stanford Fair Use Project and the Samuelson Law, Technology & Public Policy Clinic in filing the amicus brief.

A federal judge reduced the jury award to \$67,500 last July, citing constitutional concerns and basic fairness. The record companies appealed the judge's decision to the 1st U.S. Circuit Court of Appeals. In Monday's brief, EFF argues that the judge was right to try to ensure that

damages in infringement cases bear a reasonable relationship to actual harm.

"The Supreme Court has ruled that courts should review statutory damage awards to ensure they are not grossly excessive," said EFF Intellectual Property Director Corynne McSherry. "But unfortunately, courts have often failed to do so. This is an opportunity for the appeals court to clarify copyright law for creators and guarantee they have their due process rights."

Right now, it is difficult to predict copyright damages. Any creator who relies on an untested theory of fair use or other copyright exemption could be forced to pay up to \$150,000 per work if she loses in court. This threat chills start-up companies and online artists as well as libraries and

digital archives that may need to enter uncharted areas of copyright law in order to innovate.

"The fundamental purpose of copyright law is to encourage innovation, creativity, and the dissemination of information," said McSherry. "But the fear of crushing liability chills vital experimentation and creativity. Due process review can help bring damage awards back in line with copyright's purpose."

For the full amicus brief:

<https://www.eff.org/files/filenode/infresonybmgetal/EFFamicustenenbaum.pdf...>

Contact:

Corynne McSherry
Intellectual Property Director
Electronic Frontier Foundation

First 2011 Windows vulnerability

by F-Secure Antivirus Research Team
(<mailto:weblog@PLEASE-REMOVE-THIS.f-secure.com>)
(F-Secure Antivirus Research Weblog)

Another year, another vulnerability in Windows. Yesterday Microsoft confirmed it was investigating a 'recently discovered' vulnerability.

Exploit code for this is [reported](#) to be already available.

According to the [Security Advisory](#), the vulnerability involves the Windows Graphics Rendering Engine. Affected Windows versions are various flavors of XP, Vista, Server 2003 and Server 2008. Windows 7 is not affected.

Exploiting the vulnerability requires a specially-crafted thumbnail image (say of a folder or program).

Successful exploitation can lead to the attacker pretty much taking control of said computer.

One note: whether the booby-trapped thumbnail is on a site or sent in an e-mail, the user still has to actively visit the site or click a link in the e-mail (or open an attachment) to be affected, so standard precautions about safe surfing and computer usage still apply.

For users on affected versions, the

Advisory has a workaround that will at least "help block known attack vectors", until a patch is released. Or since the new year is a time for fresh starts, this might be a good time to consider upgrading to Windows 7.

No out-of-band update release seems to be forthcoming, so the soonest a patch might be available is January 11. Stay tuned.

On 05/01/11 At 01:34 AM

Korean DDoS arrests - be warned, you can be caught

(Hack In The Box)

Submitted at 1/11/2011 4:16:51 AM

The Korean Times reports the arrest of a pair of hackers over the weekend on DDoS charges. According to prosecutors, the pair, Lee and Park, operated a gambling website on behalf of a crime gang. In an effort to boost traffic to their own site, they used a 50,000-strong botnet to overload 109 rival sites during November and December 2010. A botnet, of course, is a collection of malware-infected computers (often called "zombies") which can remotely

be instructed to initiate network-related activity. Sending spam is a common criminal task for which zombies are used; visiting targeted websites deliberately to waste their bandwidth is another. Since most web requests look alike, distinguishing the web hits of malevolent time-wasters from those of potential customers can be tricky. Sites which don't usually get a large number of simultaneous requests often aren't built to sustain heavy load.

Microsoft Internet Explorer 8 use-after-free Vulnerability

by US-CERT (US-CERT Current Activity)

Submitted at 1/7/2011 7:27:20 AM

US-CERT is aware of a vulnerability affecting Microsoft Internet Explorer 8. This vulnerability is due to improper handling of circular memory references. Exploitation of this vulnerability may allow an attacker to execute arbitrary code in the context of the user or cause a denial-of-service condition.

At this time, the vendor has not released a fix or a workaround to

address this vulnerability. Users and administrators are encouraged to consider implementing the mitigations provided in Microsoft's [Enhanced Mitigation Experience Toolkit \(EMET\)](#). These mitigations will not rectify the vulnerability but will make exploitation of the vulnerability more difficult.

Additional information can be found in US-CERT Vulnerability Note [VU#427980](#). US-CERT will provide updates as further details become available.

Network IPS security improving

(Hack In The Box)

Submitted at 1/10/2011 6:00:00 PM

Independent security research and testing firm NSS Labs today released its most recent Network Intrusion Prevention System (IPS) Comparative Group Test Report for the fourth quarter of 2010. The previous NSS Labs network IPS report was released in September 2009. In that study, NSS Labs found

that security effectiveness ranged from a dismal 17.3 percent to a high of 89.5 percent. Many of those failures a year ago resulted from the failure of network IPS vendors to stop techniques used by attackers to simply evade the defensive properties of IPS security gear, explains Rick Moy, president of NSS Labs. Since that time, NSS Labs has found significant improvements.

Microsoft Releases Security Advisory

by US-CERT (US-CERT Current Activity)

Submitted at 1/5/2011 6:48:41 AM

Microsoft has released security advisory [2490606](#) to alert users of a vulnerability affecting the Windows Graphics Rendering Engine. Exploitation of this vulnerability may allow an attacker to install programs; view, change, or delete data; or create

new accounts with full user rights.

US-CERT encourages users and administrators to review Microsoft security advisory [2490606](#) and the suggested workarounds to help mitigate the risks until a fix is available from the vendor.

US-CERT will provide additional information as it becomes available.

Apple Releases Mac OS X v10.6.6

by US-CERT (US-CERT Current Activity)

Submitted at 1/6/2011 11:58:43 AM

Apple has released Mac OS X v10.6.6 to address a vulnerability affecting PackageKit. Exploitation of this vulnerability may allow an

attacker to execute arbitrary code or cause a denial-of-service condition.

US-CERT encourages users and administrators to review Apple article [HT4498](#) and apply any necessary updates to help mitigate the risks.

Include Wi-Fi among security risks at airports, FBI warns

(Hack In The Box)

Submitted at 1/11/2011 4:15:40 AM

Not all potential security breaches at an airport can be captured on a cell phone and posted as a YouTube video. One such danger lurks in the form of free wireless Internet access offered by many airports throughout the nation and in other public places. Authorities warn travelers to beware of hackers setting up fake wireless

fidelity or Wi-Fi connections to steal passwords, credit card and bank account numbers, and other personal information. Experts say the threat is not new, but it's not clear how prevalent it has become over the years because tracking where information was initially compromised in most identity theft cases is often difficult.

Microsoft to probe Windows Phone 7 data problem

(Hack In The Box)

Submitted at 1/11/2011 4:06:57 AM

Microsoft said it is investigating why some mobile handsets running its Windows Phone 7 software are sending and receiving "phantom data". The software maker's spokesman was quoted by BBC News as saying the company will determine the root cause and will update with

information and guidance as it becomes available. The mobile operating system aimed at the consumer market was launched in October 2010. Many users in the US have posted complaints on several online forums saying that their phones are automatically sending about 30MB to 50MB of data every day.

WordPress.org has released WordPress 3.0.4

by US-CERT (US-CERT Current Activity)

Submitted at 1/3/2011 7:10:55 AM

WordPress.org has released WordPress 3.0.4 to address a vulnerability in the HTML sanitation library. Exploitation of this

vulnerability may allow an attacker to insert arbitrary HTML and script code into the browser session.

US-CERT encourages users and administrators to review the WordPress.org [blog entry](#) and apply any necessary updates to help mitigate the risks.

Microsoft Releases Advance Notification for January Security Bulletin

by US-CERT (US-CERT Current Activity)

Submitted at 1/6/2011 12:08:42 PM

Microsoft has issued a [Security Bulletin Advance Notification](#) indicating that its January release will contain two bulletins. These bulletins will have the severity ratings of critical and important and will be for Microsoft Windows. Release of these bulletins is scheduled for Tuesday, January 11, 2011.

US-CERT will provide additional information as it becomes available.