

Browser-based Peer-to-peer Clients and Copyright Infringement

Herkko Hietanen
*HIIT and Lappeenranta
University of Technology*
herkko.hietanen@hiit.fi

Petri Savolainen
*Helsinki Institute for
Information Technology*
petri.savolainen@hiit.fi

Ken Rimey
*Helsinki Institute for
Information Technology*
ken.rimey@hiit.fi

Abstract

We have created a browser extension called FusionFox to integrate the BitTorrent file sharing protocol into the Firefox web browser. FusionFox adds support to the browser for a BitTorrent URL type, which can be used like any other URL. It thus enables the transparent use of BitTorrent to retrieve media content for HTML image tags or an embedded media player. This means that somebody viewing the content on a web site might also be redistributing that content to other people without being aware of it, which poses legal problems, as copying and making a work available to the public are exclusive rights of the copyright's owner. The paper surveys the legal issues that FusionFox thus raises.

1. Introduction

Until recently, web browsers have mainly utilized traditional client-server protocols such as HTTP and FTP in fetching images, music, videos, and other content embedded in web pages. Lately, some browsers have started to support peer-to-peer protocols, either as an internal feature or as an extension [3][4][5].

In BitTorrent-like peer-to-peer protocols [1], the downloader of a file automatically shares the downloaded content with other downloaders. If the content is embedded into web pages—using *img* or *object* tags, for instance—users might not be aware of what file transfer protocol the browser is using to retrieve the content.

With BitTorrent-like peer-to-peer protocols, somebody surfing a web site might not only be downloading and viewing the contents, but also sharing them with other people. This raises legal issues, as reproducing a work and making it available to the public are exclusive rights of the copyright's owner.

The rest of the paper is organized as follows. In

section 2, we briefly review the BitTorrent peer-to-peer protocol and BitTorrent web browser integration. We also introduce FusionFox, a web browser extension that enables the browser to use BitTorrent protocol to fetch content embedded in web pages. In section 3, we analyze the legal issues that the integration of the BitTorrent protocol into web browsers generates, and in section 4, we give recommendations on how to take the legal issues into account.

2. Technical background

2.1. BitTorrent

BitTorrent is a peer-to-peer data dissemination protocol that works by utilizing the uplink capacity of the downloaders [1][2]. In BitTorrent, files are split into pieces, and the peers downloading a file, in effect, trade the pieces that they have for the ones that they do not yet have.

BitTorrent uses small .torrent files as descriptors for the actual content files to be downloaded. A .torrent file contains the hashes of the content pieces and the addresses of one or more trackers, which are centralized servers that keep track of which clients are interested in which files.

The .torrent files are usually distributed on web sites, from which users download them using HTTP like any other downloadable file. Once the download of the .torrent file is complete, the .torrent file is typically opened in a BitTorrent client, which then starts downloading the actual content file(s) using the BitTorrent protocol. The BitTorrent client can be a separate program, a browser extension, or a built-in part of the web browser.

When the client is ready to start downloading the content file(s), it contacts a tracker, which provides a randomly selected list of IP addresses of other clients that are currently downloading or uploading the file in question. The client then initiates TCP/IP connections to these other clients and starts listening for incoming

connections.

The client uses these connections to request pieces of the content file(s) from its peers. The order in which a client requests the pieces is determined by a *piece selection algorithm*, the most important of which is the so-called “rarest-first algorithm”, designed to prevent the rarest pieces from becoming extinct.

The mechanism that, according to Cohen [1], forces the downloaders to share the pieces that they already have is called “tit-for-tat” and works as follows: If a downloader is not willing to upload to others or uploads at a slow rate, his connection will be blocked by other peers, resulting in a poor download rate for the one not willing to cooperate.

2.2. BitTorrent browser integration

Initially, BitTorrent clients were generally implemented as stand-alone client programs [1]. Recently, however, BitTorrent implementations integrated into web browsers have started to pop up. The Opera web browser [3] has had the ability to download files via BitTorrent since version 9, and recently, RedSwoosh released FoxTorrent [5], a BitTorrent extension for the Firefox web browser [4].

Both the Opera and FoxTorrent implementations make downloading files via BitTorrent as easy as downloading files over HTTP. Clicking on a link to a .torrent file downloads the .torrent file and starts the download of the actual content file(s) within the browser itself.

Currently, these implementations do not, however, enable the use of BitTorrent for transferring web pages, or content embedded inline into web pages.

2.3. FusionFox

To take the next logical step beyond allowing users to download files via BitTorrent from within the browser, we have implemented FusionFox [6], a Firefox BitTorrent extension that in effect makes BitTorrent just another protocol among the others available to Firefox for retrieving data. This includes loading content embedded into web pages—such as images, audio, and video—as well as loading the web pages themselves. We have achieved this by adding support for a new “torrentfile:” URL scheme into the browser. A torrentfile URL consists of two parts: the “torrentfile:” scheme name followed by another URL that points to or (in the case of a “data:” URL) encloses a .torrent metadata file. The formal syntax of the torrentfile URL scheme can be seen in Figure 1, and a full specification of the scheme can be found in [7].

```
<torrentfile_url> ::= "torrentfile:"<absolute-URI>  
                    | "torrentfile:"<relative-part>
```

Figure 1. The torrentfile URL scheme syntax

The extension handles the torrentfile URL in two phases. First it gets the .torrent metadata file referenced or enclosed by the latter part of the torrentfile URL. Then it interprets the .torrent metadata in the same way as any other BitTorrent client and downloads the data using the BitTorrent protocol. As the data arrives, the extension streams it to the web browser.

A torrentfile URL can be used like any other: It can be typed into the address bar, and it can, for example, serve as the value of a *src* attribute in an HTML *img* element, as presented in Figure 2, which may prove useful when dealing with full-resolution, megapixel-size images.

```

```

Figure 2. An example of an HTML image tag with a torrentfile URL

For those interested, the FusionFox extension along with full source code is available for download [6].

3. Legal issues

Peer-to-peer file sharing has typically required separate client programs for connecting to other peers. Today’s users’ participation in file sharing is active. BitTorrent requires users to download torrent files that are opened in separate BitTorrent clients.

When embedding of BitTorrent content into web pages becomes commonplace, people who are surfing a site will not just be downloading and viewing content, but also sharing it with other people. This poses legal problems, as reproducing a work and making it available to the public are exclusive rights of the copyright’s owner.

Copyright is not the only body of law that restricts distribution. Users might also be charged for distributing other illegal content.

3.1. Linking

Linking to a site with a *hyperlink*, which users can click on to move to the other site, is not considered to

be copyright infringement [8]. In *inline linking*, a web site designer embeds items such as music, pictures, or videos that are hosted on other websites into their own site, using HTML code. The inline link instructs the user's browser to retrieve the linked-to image from the source website and display it on the user's screen, without leaving the linking site. The bandwidth is charged to the website from which the content is actually retrieved. Inline linking requires no action on the part of the site visitor. Rather, the browser software automatically retrieves the content and displays a copy of it on the user's screen. A court decision in the USA has determined that inline linking and framing of full-sized images of the plaintiff's copyrighted photographs within the defendant's web site violated the plaintiff's public display rights [9].

BitTorrent users must find the torrent file by web search or other means. Torrent files are typically distributed on special websites such as thepiratebay.org [10]. Although torrent files do not include any copyrightable information, torrent websites have been the targets of rights owners' legal threats and litigation [11]. Torrent sites have reacted by closing their services [12] or by challenging the threats [13].

3.2 Embedded BitTorrent content

The webmaster of a site has thus far been responsible for the hosting of any infringing content on the site, while the users browsing the content have not been liable for the infringement. With the client-server structure, the person who publishes a web site controls what content is shared from the site. If infringing content is stored on the website's own server, the liability is direct, and in the case of inline linking, the liability is indirect.

In the case of FusionFox, the webmaster who embeds infringing content inline using a torrentfile URL is most likely indirectly infringing copyrights. Although he is not hosting the media file, his instructions are used by the browser software to retrieve the media and integrate it as part of the web page. The user's activity is limited to surfing to the web page with a FusionFox-enabled browser. The user does not need to take additional actions, such as clicking on a link, to view the media file.

3.3 Liability of a web surfer

With FusionFox, the webmaster is not the only one who has to decide what gets distributed. As FusionFox-like technology changes the client-server model, the liability questions also change. Users might not be aware that the website they are browsing includes

BitTorrent elements which get further distributed by their browsers. Users just see a web page with media elements appearing on it. With FusionFox, a casual web surfer could unwarily become a direct infringer, simply by surfing to a website that includes infringing elements shared with BitTorrent protocol. The risk of infringement is not limited to the time spent reading the site. FusionFox may also keep a file stored for seeding after the user has left the site.

With the growing use of mobile computers, the question of involuntary transport of illegal content across borders arises. Legal norms differ from country to country, especially when it comes to making content available. Consider a scenario where the user views an adult entertainment site with FusionFox, with the effect of saving the content to the laptop. If the laptop were later connected to the network during a trip to Saudi Arabia, the automated seeding of the file could lead to serious consequences. Similar situations could occur with caching in ordinary web browsers, but FusionFox also shares the files with other users.

Should the users be held accountable for what their computers do? Every day thousands of computers are polluted by malware and viruses. It is also common for such computers to further spread the malware. Yet people who become involuntary members of botnets as a result of virus infection are not considered criminals, because criminal liability requires intent.

Lack of intent does not automatically exempt people from copyright or general tort liability. For example, a person who is unaware of the real rights owner of a work is nevertheless liable for making the rights owner's work available to public. Still, it would be hard to argue that a computer user whose computer is taken over secretly by a virus should be responsible for the content that is secretly shared by the virus.

Would the user be accountable for browser-based BitTorrent sharing? The analogy with unintentional virus spreading is evident. A user who is not aware of the file sharing that his browser is doing should not bear liability. This would be the case if FusionFox-like technology were automatically enabled as a default in the browser. But as users gain knowledge of how BitTorrent works as part of web pages, the question gets more complicated.

4. Recommendations

How would a user react to a claim that she has violated somebody's copyright by visiting a web page? The first defense that naturally comes to mind is lack of knowledge. Users could claim that they were unaware that their computer was performing any kind of file sharing. Copyright law has a rule of strict

liability, which does not protect those of innocent mind. Being uninformed of the illegality of sharing certain content doesn't free one from civil liability. However, the strict liability may not extend to situations where users are not aware that they are sharing content at all.

Nevertheless, BitTorrent browser developers need to find ways to let users know when BitTorrent is used as a transfer protocol, and to let users determine what content they want to share. This could be done in several ways. The browser could inform the user that the site includes embedded BitTorrent files and ask her to approve the initiation of the transfer. An alternative to requiring the user to click Accept buttons could be to inform them of the presence of BitTorrent elements using visual hints. Such methods are used in secure protocols by online banks and other sites that require trusted file transfers. The browser displays a lock icon when a secure connection has been made.

The browser could also resolve the sharing issue by using a white list of trusted websites, which might be community-created. Users could also choose to participate only in sharing of files that have certain permissive licenses attached, such as a Creative Commons license [14] or the GFDL license used by Wikipedia. Finally, an audit trail connecting a file to the original person who shared it would create trust in those situations where rights owners want to permit peer-to-peer sharing.

This work has been supported by the P2P-Fusion project (EU FP6).

5. References

[1] B. Cohen. Incentives Build Robustness in BitTorrent, In *Workshop on Economics of Peer-to-Peer Systems*, Berkeley, USA, May 2003.

[2] BitTorrent Protocol Specification v. 1.0, <http://wiki.theory.org/BitTorrentSpecification>, May 2007.

[3] Opera browser home page, <http://www.opera.com/>, May 2007.

[4] Firefox browser home page, <http://www.mozilla.com/>, May 2007.

[5] FoxTorrent extension home page, <http://www.foxtorrent.com/>, May 2007.

[6] FusionFox extension home page, <http://www.fusionox.org/>, September 2007.

[7] Torrentfile URL scheme specification, <http://www.fusionfox.org/torrentfilescheme.txt>, September 2007.

[8] Ticketmaster Corp. v. Tickets.com, Inc., 2000 U.S. Dist. LEXIS 4553 (C.D. Cal. Mar. 27, 2000)

[9] Kelly v. Arriba Soft Corp. (9Cir'02) 280 F3d 934

[10] The Pirate Bay, <http://www.thepiratebay.org/>, May 2007.

[11] Drew Cullen; Finnish police raid BitTorrent site. The Register 14.12.2004 http://www.theregister.co.uk/2004/12/14/finnish_police_raid_bittorrent_site/, May 2007.

[12] M. Bordash "RIAA, MPAA rejoice as suprnova.org closes, file sharing goes underground" Internetdj.com <http://www.internetdj.com/article.php?storyid=514>, May 2007.

[13] Legal threats against The Pirate Bay, <http://thepiratebay.org/legal>, May 2007.

[14] Creative Commons home page, <http://www.creativecommons.org/>, May 2007.