Network Filtering: Limiting Cultural Industries, Damaging the Internet

EFF-Europe is very concerned with the recent opinion of the ITRE committee on the Guy Bono report on the Cultural industries in Europe, which calls upon "internet service providers [ISPs] to apply filtering measures to prevent copyright infringement", as well as other amendments that include language encouraging network filtering as a policy.

As an NGO focused on issues related to technology and consumers' rights, EFF's experience has been that filtering by ISPs is an overbroad, ineffective measure that will do little to practically address the concerns of major rightsholders while imposing serious costs on the individual rights of European citizens in their roles as consumers, artists and educators.

Filtering Would Curtail Existing Consumer and Artistic Rights

Users, both as consumers and as creators, have their own rights under copyright law to re-use and distribute content. These rights would be affected by filtering and blocking technology installed for detecting and removing major rightsholder content.

Many European countries, for example, have limitations on owners' exclusive rights for the purposes of private copying, or for the use of the disabled. Other exceptions permit the use of content for criticism, political use, or parody.

No technological system could determine whether these legitimate exceptions were in play during the transmission of content. Instead, all use not explicitly licensed by rightsholders would be banned from the network, severely restricting the exercise of existing exceptions and limitations designed to protect European artists, consumers and citizens.

This will have particularly strong ramifications in the growing online field of "user generated content" (UGC), which frequently relies on balanced copyright regimes that leave room for the creation of new cultural works.

To give an example of the kinds of content that would be trapped in such filters, consider EFF's own test suite for automatic recognition systems being considered in the United States of America for a far more limited, voluntary, deployment on individual websites: http://www.eff.org/pages/UGC-test-suite

This set of clips include creative and transformative use of copyrighted content that could be legal under national copyright limitations and exceptions, but would be automatically precluded by filters not capable of distinguishing the context. No recognition system is capable of making this subjective judgment. While not all of the clips are legal in every European country, they do give an illustration of the issues raised by automated filters when judging parody, pastiche, or caricature.

Filters could also interfere with private copying of content that is permitted as a practical matter. Many modern artistic works revolve around sampling or remixing existing content - for instance, popular dance music, or documentaries. Copyright clearance for these works is usually left until the work is finished and made available for sale.

In the production process, however, samples are frequently exchanged privately between co-creators. The Internet is increasingly allowing collaboration over long distances (for instance, David Pendragon, an award-winning Australian producer, mixes artists contributing from Europe, Singapore, and India at http://www.tribeworldensemble.com/), allowing Europeans to work with their fellow Europeans and others without needing to travel.

A filtering system at the ISP level cannot make a determination between a work that is being shared between two individuals privately or being more widely shared. Such collaboration will be hindered, and filters will therefore negatively affect the creative process itself.

Contact: Erik Josefsson on +32-484-082-063 or <erik@eff.org>

Filtering Would Place Burdens on Education and Research

Filtering is predicated on the notion that all unlicensed distribution of rightsholder content is infringing. Under European copyright, this is not the case. EU copyright law includes a number of limitations and exceptions to copyright, in particular those connected with uses for education and research. By pre-emptively interfering with all distribution, ISP filters would prevent educational institutions from using the Internet in the pursuit of their many legitimate uses of copyrighted material.

To give one example, a University of St. Gallen paper, "Teaching Exceptions in European Copyright Law", analysed the fictitious case of a professor who scans parts of a textbook, copies some digital articles, and uploads them to a web server which can be accessed by students enrolled in his class from home using a password. The authors concluded that such a practice is legal in a number of EU countries, and could become commonplace in the future as distance learning over the Internet becomes more popular. However, such a scenario would also be pre-emptively prohibited by filtering if any of the content was on an "infringing content" blacklist. (See Ernst, Silke, and Haeusermann, Daniel M., "Teaching Exceptions in European Copyright Law - Important Policy Questions Remain" (August 2006). Berkman Center Research Publication No. 2006-10 Available at SSRN: http://ssrn.com/abstract=925950).

Filtering Would Do Nothing to Prevent Copyright Infringement

Currently, most Internet communications are sent in a form that is easily examined by intermediaries such as ISPs. The exceptions to this are communications where there is a high risk of unwanted third parties seeking access to the confidential content, such as credit-card transactions or when accessing private web services. In these cases, communications are strongly encrypted so that third-party surveillance is not possible.

Introducing filtering technology at ISP facilities would simply cause infringing Net users to encrypt their communications in the same way, eliminating any chance that these filters could successfully target these transfers. Such encrypted content cannot be examined or blocked by third parties such as ISPs; if it could, the financial institutions would be equally at risk.

An example of the ease and speed of the adoption of encryption by end-users can be seen from the development of the BitTorrent protocol. BitTorrent is a file distribution system with substantial non-infringing uses (the United State's MPAA has worked with the parent company, and the protocol is used to distribute content for major media groups such as Fox and Viacom, as well as operating systems like Linux, and multi-million user games such as World of Warcraft). (See http://en.wikipedia.org/wiki/BitTorrent_Protocol)

Nonetheless, some ISPs have attempted to "throttle" or interfere with customer's use of BitTorrent to control high user bandwidth demands. Such interference has been widely-criticised by end-users. (See comments by U.S Congressman Rick Boucher and others, http://www.news.com/8301-10784_3-9804158-7.html)

Just as encryption would defeat filtering, it also defeats the protocol-throttling used by these ISPs. In reaction, the portion of traffic BitTorrent traffic measured by a large UK ISP which is encrypted rose tenfold from 4% of the total, to 40% in just 12 months. A concerted effort by ISPs to introduce blanket filtering would no doubt push this to close to 100% within a similar period of time. See: http://www.datacenterknowledge.com/archives/2007/Nov/09/more_p2p_traffic_using_ssl_encryption.html

Further details on the technical limits of filtering:

EFF's own technical analysis of "Audible Magic", a technology offered for use in filters: http://w2.eff.org/share/audible_magic.php

Testimony of Gregory A. Jackson, Vice President and CIO, University of Chicago to House Committee on Science and Technology on The Role of Technology in Reducing Illegal Filesharing, June 2007: http://democrats.science.house.gov/Media/File/Commdocs/hearings/2007/full/05june/jackson_testimony.pdf

Contact: Erik Josefsson on +32-484-082-063 or <erik@eff.org>

Filtering Would Limit European Innovation

It also has been proposed that some filtering take place at the "protocol level", which is to say some Internet services should be entirely blocked by ISPs because they may be used for infringing distribution.

While almost all Internet protocols, including email and the Web, may be used for infringement, the protocols that critics particularly target are "peer to peer" services on the assumption that these services carry the majority of the infringing materials.

But peer-to-peer services also provide unique, non-infringing uses. Indeed, many European companies, cultural institutions, and artists use these services to increase the innovation in the cultural industries. Some examples:

- AllPeers, a company based in the UK and Czech Republic, has adapted the BitTorrent protocol to allow low-cost sharing of personal files among small groups: http://www.allpeers.com/
- Miro, an "Internet television application" from the non-profit Participatory Culture Foundation, uses BitTorrent to allow video creators to distribute HD-TV works without the costs of traditional TV distribution:http://participatoryculture.org/ . A selection of European creators who use Miro can be seen at https://miroguide.com/tags/204
- The British Broadcasting Corporation uses peer-to-peer sharing to distribute its content within its iPlayer on-demand Internet service: http://www.bbc.co.uk/iplayer/
- Joost, the latest company from Skype's founders, uses encrypted peer-to-peer transmissions to create online TV channels. Joost's developers are based across the world, including London, Leiden, and Toulouse: http://en.wikipedia.org/wiki/Joost

A blanket protocol filter that blocked such peer-to-peer services would distort the market and reduce the effectiveness of European Net use.

Blanket protocol blocking also raises issues related to competition. The motives of those calling for such protocol filters should be examined closely. Many of these new services challenge the current market share of the present-day major rightsholders. Allowing these current industry leaders to determine what protocols and services can and cannot be allowed in the future would be to grant them an advance veto over new disruptive technologies -- even when those technologies improve the overall competitiveness and efficiency of the industry. Remember that the US music industry attempted to sue to stop the development of the first MP3 players -- which led to the iPod (See http://archive.salon.com/21st/feature/1998/10/28feature.html)

An example of such current innovations would be devices that facilitate "place-shifting": the private enjoyment of purchased content remotely over the Internet. Products such as the open source MythTV (See http://www.mythtv.org/ , also http://mythwiki.de/ and http://www.mythportal.be/) and commercial MP3 Tune Locker service (http://mp3tunes.com/) allow users to listen or watch their collection of legitimately obtained music or video over the Internet. There are few judicial decisions on what use of this technology is permissible using the private copying exception to copyright. With filters and protocol blocks in place, it would be possible for threatened industries with the ability to influence the implementation of protocol filters to eliminate these services before any judicial consideration has been made.

Filtering Would Weaken European Privacy Norms

In order to introduce filtering systems proposed by rightsholders, ISPs would have to install technology that would inspect the contents of every data packet passing through their networks - including private communications between individuals.

Giving blanket permission for third-parties to pry into communication data would set a disturbing precedent for privacy in the European Union. By creating not only the assumption that communication providers should analyse and block specific communications, but also encouraging building into every Internet peering center devices that would facilitate such surveillance, the safeguards provided by the

European Convention on Human Rights and the European Data Protection Directive would be seriously undermined.

A system that filters for infringing content would have to be programmable to examine and block any content. The dangers of creating and installing such equipment are best compared to the recent Telecom Italia/Greek mobile-phone tapping scandal. There, software designed to conduct lawful intercepts of telephone communications was misused to tap high-ranking ministers (See http://www.spectrum.ieee.org/print/5280).

A similar security threat exists for these filtering and blocking services - except that the risks are far greater and the protections far weaker. Lawful interception systems are held to the security standards of law enforcement; filtering systems will be held to the standards of a low-priced industry-led solution. Lawful intercepts have, by design, limited functionality. Filtering systems will have to be far-reaching to cope with the many different online protocols that might carry infringing content (from email to instant messaging, from webservers to peer-to-peer systems). In addition to surveillance, the proposed filtering systems are also expected to block or drop connections, allowing communications to be cut-off or permanently prohibited, as well as monitored.

Finally, at present, lawful intercepts of telephony are generally kept to a few major telecom companies. For filtering to be effective, it would have to be implemented by all ISPs, large or small (otherwise infringers would simply move to non-filtering ISPs). Such surveillance and interception systems would therefore have to be rolled out across Europe - and presumably work with a centralised database of offending content. Such a system would create a system of censorship and surveillance with a single control center for large-scale misuse and many vulnerable opportunities for unauthorized spying.

Real Solutions Foster the Balance of Copyright, Not Ignore It

The infringement we see online is a symptom of a rapidly changing environment for the cultural and creative industries: one that provides as opportunities as well as challenges. While some sectors of the industry see the low cost of reproduction and distribution that enables Internet infringement as a threat, other artists and producers are discovering that it provides novel business models which grant them new tools for collaboration and creation and access to new audiences, both as creators or distributors in their own right.

These new business models and cultural works rely just as much on a fair and responsive intellectual property policy as do older business models.

Network filtering would seek to bypass such subtlety, and in so doing dampen the experimentation and innovation that allow the cultural industries to constantly re-invent themselves and take advantage of change. EFF-Europe urges the rejection of such misguided and dangerous proposals in favor of a more nuanced approach, equitable to both established and newer members of the cultural and creative industries.

For further discussion, please do not hesitate to contact EFF's European Affairs Coordinator, Erik Josefsson, at the telephone or email address below.

Contact: Erik Josefsson on +32-484-082-063 or <erik@eff.org>