Before the
COMMISSION OF THE EUROPEAN COMMUNITIES

In the Matter of	)	
	)	COM(2007) 836
Communication on Creative Content	)	
Online in the Single Market	)	

COMMENTS OF PUBLIC KNOWLEDGE

Introduction

Public Knowledge submits these comments in reference to the Communication on Creative Content Online in the Single Market dated January 3, 2008. In that Communication, the Commission requested comments on eleven separate issues. Here, Public Knowledge limits its comments to issues 10 and 11, regarding measures to limit piracy, either according to the model of the French Memorandum of Understanding (MOU), or via filtering technologies. Public Knowledge believes that neither of these models is an effective means of combating piracy, and that each will result in negative unintended consequences for a large number of lawful users of the Internet.

Public Knowledge is a non-profit organization based in the United States and dedicated to promoting innovation and consumers rights in the emerging digital culture. The organization has been involved in a variety of issues at the intersection of technology, telecommunications, intellectual property, and the law. Recently, Public Knowledge has submitted reply comments to the United States Federal Communications Commission (FCC) regarding broadband practices in the United States, and specifically addressing proposals by content industries to mandate network providers to filter their networks for copyrighted content. Public Knowledge has also followed and participated in a variety of legislative, administrative, and judicial proceedings surrounding the Digital Millennium Copyright Act (DMCA), including its notice-and-takedown procedures regarding online infringement.

Given these experiences, Public Knowledge believes that the system proposed in the MOU, as well as any automatic filtering technologies, are flawed models that would result in innocent consumers suffering adverse effects on their ability to communicate and participate as citizens and consumers online.

The French Memorandum of Understanding is a Flawed Model Which Should Not be Adopted

One of the most troubling proposals outlined in the MOU is that infringement should be penalized by the termination of Internet access. This proposal represents a

completely disproportionate response to alleged infringement, and displays a markedly narrow conception of the importance and uses of the Internet.

The Internet is not merely a conduit through which consumers access copyrighted content, whether legally or illegally. It is also a vital means of communication for millions, who otherwise would be unable to speak to a global audience or participate in a global exchange of ideas. Internet access therefore is a vital outlet for citizens to both provide and receive civic and political information. The Internet allows, as never before, individuals to provide insight into a local crisis, make public revelations of governmental or corporate misdeeds, and mobilize other citizens on critical issues.

Aside from the importance of the speech that users might exchange via the Internet, the Internet also provides a vital communications link for individuals. Growing numbers of individuals are foregoing traditional wireline telephony in favor of voice over Internet protocol (VoIP) applications, whether they connect to traditional telephone exchanges or exist solely on a computer-to-computer network. For such individuals, Internet access is more than a luxury—it is a communications lifeline that must be used in emergencies. The importance that VoIP connections have to their users was recognized by the FCC when it required interconnected VoIP services to interoperate with existing emergency dispatch systems.

Given the myriad ways in which the Internet is of crucial importance to individuals, terminating access should not be a penalty for individuals merely because they are liable for infringement via the Internet. While it is entirely appropriate that infringers compensate copyright holders for their losses, depriving users of a forum for speech and expression is a uniquely disproportionate penalty divorced from any relationship to the losses suffered by the copyright holder or the unjust enrichment of the infringer. Violations such as in-person defamation do not bar the violator from speaking in public; a finding of fraud over a telephone does not prohibit a defendant from using the telecommunications system—basic needs and proportionality of punishment require that these resources be open to all. After all, each of these forms of communication will and must be used for a wide variety of purposes other than the commission of offenses—even by a convicted offender.

Adding to these concerns with the MOU is the nature of its structure and operation. A large-scale operation with the oversight of a single judicial official does not suggest a robust means of redress for those subjected to this system. Since rightsholders, and not the authority itself, will initiate the process, the tendency will be for complaints to be sent in on any evidence of potential infringement, without regard to the likelihood that this infringement can eventually be proved. Without a robust process for screening out meritless complaints or for deterring frivolous or malicious actions, the system could easily find itself faced with a large number of erroneously accused users. Any system should require those making complaints to subject themselves to penalties for recklessly or negligently false or malicious complaints. Accused individuals should also have effective redress procedures in case of wrongful complaints.

Past examples show the need for robust appeal procedures and penalties for abuse of the system. In the United States, the safe harbor provisions of the DMCA[1] require online service providers to expeditiously remove infringing material from their sites upon notification by a copyright owner. However, this procedure has been subject to a number of abuses, with copyright owners insisting upon, and often receiving, takedowns of material that is not infringing. Frequently, such notices targeted competitors[2], and in many cases these provisions have been used to unfairly target criticism of the complainant. These abuses exist even in the presence of a penalty for certain misrepresentations in requests.[3]

The types of penalties suggested by the MOU particularly require a process with more oversight and representation for the accused, as well as stronger and more definite methods for redress. Without Internet access, accused individuals face a major handicap in dealing with any process. Furthermore, compiling and publishing a list of alleged offenders puts the reputation, as well as the personal information, of such individuals at risk. Since private information, once disclosed, is nearly impossible to make private again, disclosure of individuals' identities to the world is a singularly poor remedy in a situation that lends itself to a large number of false positives. The reputational harm to falsely accused individuals, as well as the violations of their informational privacy, would indicate a greater need for caution in the process than there currently appears to be.

Filtering for Copyrighted Material is an Ineffective Measure with Detrimental Unintended Effects

Automated filtering is particularly poorly suited for finding determining copyright infringement online. Public Knowledge has commented at length upon the flaws in such systems in an FCC proceeding in 2007.[4] Those comments addressed suggestions that "network management" by Internet service providers might be used to prevent infringing copies of works from being transmitted across the Internet. These calls for network management amounted to requests for network filtering.

Network filtering may take the form of either content inspection or traffic analysis. Content inspection technologies look at the packets of data that are being transferred in order to determine whether those data are infringing. Traffic analysis technology looks not at the data, but at the kind and nature of the data traffic. By analyzing the traffic, the technology attempts to determine what application is sending the data. If the application appears to be one that the network operator has decided to block, the technology blocks the transfer.

---

[1] 17 U.S.C. § 512(c).

[2] For a quantitative study of takedown notices under the DMCA, including an analysis of abuses encouraged by the process, see Jennifer M. Urban & Laura Quilter, *Efficient Process or "Chilling Effects"? Takedown Notices Under Section 512 of the Digital Millennium Copyright Act*, 22 Santa Clara Computer & High Tech. L.J. 621 (2006), *available at* http://www.chtlj.org/pdf/22-4_Urban_quilter.pdf;

[3] *See* 17 U.S.C. § 512(f).

[4] Reply Comments of Public Knowledge, *et al.* in the Matter of Broadband Industry Practices, FCC, WC Docket No. 07-52, July 16, 2007, *available at* http://www.publicknowledge.org/node/1093.

Regardless of which form it takes, a network filtering system, by its nature, would be both over- and underinclusive. It would be overinclusive in that it would block, or mark as illicit, transfers of legitimate content. It would also be underinclusive, in that it would fail to stop traffic in infringing material. Any foreseeable filtration technology would suffer these defects.

The reasons for these defects are severalfold. In the case of traffic analysis, blocking particular applications that allow for infringement will necessarily also be overinclusive. For example, although peer-to-peer applications are often characterized as mere conduits for piracy, they are, like the Internet generally, frequently and most productively used to distribute legitimate content, in the form of free/open source software, public domain materials, or materials that the author wished to distribute efficiently. Blocking particular applications without regard to content would unfairly prejudice particular technologies, and deny all legitimate users of an efficient way to send and receive large files. Targeting any type of protocol runs this same risk.

Content inspection bears its own set of distinct problems. While matching a set of known files to a set of online files may be a trivial task for a computer, determining the context and the contours of that file's *use* are tasks requiring human judgment, if not legal expertise as well. An automated system might well recognize a portion of a copyrighted audiovisual work traversing the network, but the filtering technology would be unable to tell whether that portion was being sent from a library to a classroom for educational purposes; from a hearing impaired user to a transcription service; or from a legitimate buyer of the content to her own computer in another room. So long as lawful uses of copyrighted works are determined by uses, and not solely by the status of the work—in other words, so long as there are limitations and exceptions to copyright—content inspection will necessarily be overinclusive.

Meanwhile, filters will also be underinclusive, failing to find many infringements, due to determined infringers' use of encryption against content inspection, or traffic management applications against traffic analysis. Expanding the net to account for these tactics would only result in even more legitimate content being blocked.

Network filtering, especially content inspection, likewise necessarily implicates privacy questions. Inspecting the contents of all users' communications, for the comparatively limited benefit of locating some instances of copyright infringement, would appear to violate the principle of proportionality.

Conclusion

For the foregoing reasons, Public Knowledge strongly recommends against using the French MOU as a model for future action, and strongly recommends against any action that would mandate or encourage the use of automated network filters to curb online copyright infringement.