MEMBERS OF CONGRESS DECLARE WAR ON P2P NETWORKS

Jonathan Band and Masanobu Katoh[1]

In June and July, 2003, members of Congress introduced three progressively more aggressive bills targeted at perceived evils of peer-to-peer (P2P) networks. None of the bills are as extreme as last year's P2P Piracy Prevention Act, H.R. 5211, which would have provided copyright owners with a safe harbor against legal liability that could result from engaging in self –help activities such as denial of service attacks.[2] Nonetheless, the bills contain serious legal, technical, and policy flaws that probably will prevent their enactment in the form introduced.

I. H.R. 2517.

The most benign of these bills is H.R. 2517, the Piracy Deterrence and Education Act of 2003, introduced by Congressman Lamar Smith (R-TX), Chairman of the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property.[3] Section 3 of the bill requires the FBI develop a program to deter members of the public from committing acts of copyright infringement by uploading works onto the Internet and downloading works from the Internet without the copyright owners' authorization. This program must include issuing appropriate warnings to individuals engaged in the unauthorized uploading and downloading of works that they could by the subject of criminal prosecution. Section 3 also requires the FBI to facilitate the sharing among law enforcement agencies, Internet service providers, and copyright owners of information concerning the uploading and downloading of works.

Section 3 has been criticized on several counts. First, Section 3(1) assumes that all unauthorized downloads are copyright infringements, when they might be fair uses in certain circumstances. For example, the owner of a CD might decide to download his favorite song from the Internet so that he can listen to it on his lap-top when he is traveling.[4]

Second, the scope of the deterrence "program" is completely undefined. Beyond the issuance of warnings, the bill gives the FBI no guidance concerning what the "program" should entail. The information sharing referenced in Section 3(2) could be

---

[1] Jonathan Band is a partner in the Washington, D.C., office of Morrison & Foerster, LLP. Masanobu Katoh is President of the Intellectual Property and Export Control Group of Fujitsu Limited. The views expressed in this article are those of the authors alone.

[2] *See* Jonathan Band, "Vigilantes on the Cyberspace Frontier: The Berman P2P Bill," AsianIP, Sept. 2002.

[3] Co-sponsors included Howard Berman (D-CA) and John Conyers (D-MI).

[4] Statement of Gary J. Shapiro, Chairman, Home Recording Rights Coalition, before the House Judiciary Subcommittee of Courts, the Internet, and Intellectual Property, July 17, 2003.

understood to suggest that the FBI should start monitoring P2P networks to acquire information to share. This raises serious privacy and civil liberties concerns.[5]

Third, the information sharing referenced in Section 3(2) suggests that the FBI and other law enforcement agencies should provide the fruits of their monitoring to the copyright owners. This, in essence, would constitute a government subsidy of a private entity's enforcement efforts.

Fourth, H.R. 2517 provides no additional funding for the FBI to carry out its deterrence program and the facilitation of information sharing. Presumably the FBI would have to divert resources from other law enforcement activities to meet this mandate.

Section 4 of H.R. 2517 requires the Attorney General to ensure that any Justice Department unit responsible for investigating computer hacking of intellectual property crimes have at least one agent trained in the investigation and enforcement of intellectual property crimes. Again, H.R. 2517 fails to provide the resources for this training and staffing.

H.R. 2517 likewise fails to provide the funds for the establishment of the education program required under Section 5. That section directs the establishment of an Internet Use Education Program in the Office of the Associate Attorney General. The purpose of the program is to "educate the general public concerning the value of copyrighted works and the effects of the theft of such works on those who create them." The program must also "educate the general public concerning the privacy, security, and other risks of using the Internet to obtain unauthorized copies of copyrighted works...." Additionally, the Associate Attorney General must work with the Department of Education and the Department of Commerce to improve compliance by educational institutions and corporations, respectively, "with applicable copyright laws involving Internet use."

But even if H.R. 2517 did provide additional funding to the FBI and the Department of Justice for these various programs, it is fair to ask whether this would be an appropriate expenditure when the annual federal budget deficit exceeds $450 billion and many important homeland security initiatives remain under-funded.

Section 7 directs the Attorney General to establish criteria under which copyright owners designated by the Attorney General will be able to use the FBI's seal as a warning on copyrighted works. The FBI has long permitted the Motion Picture Association of America to use the seal on videotapes and DVDs, and currently is negotiating a memorandum of understanding with the Recording Industry Association of America to permit RIAA members to use the seal on sound recordings. Section 7 would formalize this process for other copyright holders. Critics have noted that this provision could ultimately lead to foreign copyright owners using the FBI's seal, including organizations supporting terrorist attacks on the United States.

---

[5] *Id.*

Section 6 of H.R. 2517 heads in a completely different direction from the rest of the bill. Section 411(a) the Copyright Act currently requires that a United States work be registered with the Copyright Office before an infringement action can be initiated. Section 6(a) would amend Section 411(a) so as to permit the United States government to initiate a criminal proceeding even if the work is not registered. At the July 17, 2003, hearing on H.R. 2517, a photographer testified about the difficulty of instituting criminal proceedings concerning the infringement of photographs, because many photographers do not register their works.[6] Similarly, Sections 6(b) and (c) would clarify that a work need not be registered with the Copyright Office nor recorded with the Bureau of Customs and Border Protection prior to the Bureau seizing infringing copies at ports of entry to the United States.

While eliminating the registration requirement with respect to these federal enforcement actions may be a good idea, this issue is a subset of the larger questions of the benefits of registration and the need to register prior to bringing any infringement action concerning a United States work. In the early 1990s, the Library of Congress convened the Advisory Committee on Copyright Registration and Deposit ("ACCORD") to review the issue comprehensively. In its final report issued in September, 1993, ACCORD recommended against any amendments to the provisions regarding registration and deposit. Now that ten years have passed since the ACCORD report, it may be time to reexamine the issue. But it should be considered comprehensively, not on the piecemeal basis proposed in H.R. 2517.

In sum, although H.R. 2517 reflects questionable budget priorities, and could be construed as encouraging the FBI to monitor P2P networks, it does not propose seriously problematic substantive changes to the copyright law. H.R. 2752, by contrast, does.

II. H.R. 2752.

Congressman John Conyers (D-MI), the ranking Democrat on the House Judiciary Committee, along with several other Democrats on the House IP subcommittee,[7] introduced H.R. 2752, the Author, Consumer, and Copyright Owner Protection and Security ("ACCOPS") Act of 2003. Its very first provision appropriates $15 million to the Department of Justice for the investigation and prosecution of violations of the Copyright Act. Thus, from the outset, H.R. 2752 has more teeth than H.R. 2517.

Like H.R. 2517, H.R. 2752 also addresses information sharing. But unlike H.R. 2517's vague direction to the FBI to facilitate the sharing of information among law enforcement agencies, ISPs, and copyright owners, Title II of H.R. 2752 requires the Attorney General to provide evidence to a foreign authority to assist in the enforcement of

---

[6] *Hearing on H.R. 2517 Before the House Judiciary Subcommittee on Courts, the Internet, and Intellectual Property*, 108th Cong. (July 17, 2003)(testimony of David P. Trust, CEO of Professional Photographers of America).

[7] Howard Berman (D-CA), Adam Schiff (D-CA), Martin Meehan (D-MA), Robert Wexler (D-FL), and Anthony Weiner (D-NY).

foreign copyright laws. The bill then specifies examples of the type of evidence to be provided, including evidence that describes the nature of the violation, the technological means by which the violation occurred, the identity and location of the person who committed the violation, and the estimated financial loss caused by the violation. Title II evidently recognizes the international nature of P2P systems and the infringement they facilitate. However, the bill requires the Attorney General to provide assistance concerning activities that might not violate U.S. copyright law were they committed in the U.S. – for example, reproduction permitted under the fair use doctrine. Additionally, the information could be gathered prior to the filing of a criminal complaint. Thus, the provision could easily be abused to assist in the prosecution of foreign dissidents who quote from government or religious texts in order to criticize them.

While H.R. 2517 requires the Justice Department to educate the general public concerning the privacy and security risks of using the Internet to engage in infringing activity, H.R. 2752 prohibits the distribution of P2P software without notice concerning security and privacy risks. Specifically, Section 302 imposes criminal penalties on anyone who knowingly offers "enabling software for download" without providing clear and conspicuous warning to any person downloading the software that the software "could create a security and privacy risk for the user's computer...." Further, the distributor must obtain the downloader's consent to the download after providing the warning.

The fundamental flaw in this provision is the definition of "enabling software." The bill defines it to mean "software that, when installed on the user's computer, enables 3rd parties to store data on that computer, or use that computer to search other computers content over the Internet." This definition appears broad enough to include all instant messaging, email, and browser software, as well P2P programs such as KaZaa.[8] By requiring notice and consent on such a broad swath of software, Section 302 will simultaneously be burdensome on the software distributor and completely ineffectual to the user. The user will treat it as yet another window that must be clicked through to get the computer to perform basic functions.

Section 303 imposes criminal penalties on "[w]hoever knowingly and with intent to defraud provides material and misleading false contact information to a domain name registrar," registry, or registration authority. Similarly, Section 305 would amend the criminal copyright section, 17 U.S.C. § 506(a), to provide that "[t]he knowing and intentional provision of material and misleading false contact information to a domain name registrar," registry, or registration authority "shall be considered evidence of willfulness with respect to infringements committed by the domain name registrant through the use of that domain name." To be sure, many of the websites that disseminate infringing material have false contact information in their domain name registrations. At the same time, some registrants have legitimate reasons for remaining anonymous. A whistleblower, for example, may wish to post documents demonstrating his employer's

[8] Indeed, Judge Posner noted the similarity between the Aimster P2P system and AOL instant messaging in *In re Aimster*, 334 F.3d 643 (7th Cir. 2003).

wrongdoing, without revealing his identity. These provisions probably could be redrafted to address these free speech concerns.

Perhaps the most controversial provision of H.R. 2752 is its least understood: section 301, which would provide felony treatment for the uploading of works on the Internet. In the press this amendment has been described as imposing felony penalties for the uploading of even a single song. The provision in fact is far more complex, and a complete understanding of its operation requires a brief discussion of criminal copyright law.

The criminal copyright provisions are divided between two sections. 17 U.S.C. § 506 sets forth the basic standards for criminal copyright liability, while 18 U.S.C. § 2319 articulates the penalties for criminal infringement. Thus, 17 U.S.C. §506(a) imposes criminal liability on a person who infringes a copyright willfully either (1) for purposes of commercial advantage or private financial gain; or (2) by the reproduction and distribution, during a 180 day period, of one or more works, with a total retail value of over $1,000.

Once criminal liability is established, the penalties set forth in 18 U.S.C. § 2319 are applied. If the infringer reproduces or distributes more than ten copies with a total retail value of over $2500, the offense is treated as a felony. Otherwise, it is treated as a misdemeanor. Under 18 U.S.C.§ 2319(b), a felony conviction pursuant to 17 U.S.C. § 506(a)(1) – that is, an infringement for purposes of commercial advantage or private financial gain – is punishable for up to five years in prison (ten years for a second offense). Under 18 U.S.C. § 2319(c), in contrast, a felony conviction pursuant to 17 U.S.C. § 506(a)(2) is punishable for up to three years in prison (six years for a second offense).

Section 301 of H.R. 2752 would add a sentence to 17 U.S.C. § 506(a) that would state that for purposes of 18 U.S.C. § 2319(b), a single upload will be treated as meeting the $2,500 felony threshold, even if the existing $2,500 threshold is not in fact crossed. Contrary to the implication of press reports, Section 301 does not change the basic test for criminal liability in the first place -- willful infringement either for financial gain or by reproduction or distribution of $1,000 of copies. Section 301 would simply make it easier for a prosecutor to have felony penalties imposed *after* he establishes criminal liability.

Section 301 contains two serious drafting errors. First, Section 301 amends the wrong section of the U.S. Code. It would add the sentence discussed above to 17 U.S.C. § 506(a), but the sentence refers to 18 U.S.C. § 2319. Since the sentence does not change the 17 U.S.C. § 506(a) standards for liability, but it does create a non-rebuttable presumption with respect to 18 U.S.C. § 2319, the sentence should be placed in 18 U.S.C. § 2319 rather than in 17 U.S.C. § 506(a).

Second, the amendment appears incomplete. The added sentence refers only to 18 U.S.C. § 2319(b), but not 18 U.S.C. § 2319(c). As noted above, 18 U.S.C. § 2319(b) contains penalties only with respect to 17 U.S.C. § 506(a)(1), which refers to commercial

advantage or private financial gain, while 18 U.S.C § 2319(c) sets forth the penalties for violations of 17 U.S.C. § 506(a)(2), which refers to the distribution of copies with a retail value of over $1,000. By referring only to 18 U.S.C. § 2319(b), Section 301 appears to create the non-rebuttable presumption only with respect to 17 U.S.C. § 506(a)(1).

This makes little sense in a bill purportedly directed at P2P networks. Why lower the threshold for felony punishment only with respect to infringements for commercial advantage or private financial gain, when most file trading has no commercial nexus whatsoever? After all, Congress added § 506(a)(2) specifically to address the "LaMacchia Loophole," where an MIT graduate student who operated an electronic bulletin board that facilitated the distribution of large quantities of software could not be prosecuted because he received no compensation.

To be sure, one could fashion an argument that P2P file trading does meet the commercial advantage/private financial gain standard. The Ninth Circuit in *A&M Records v. Napster* held that the file trading by Napster users constituted a "commercial use" for purposes of the fair use analysis: "[r]epeated and exploitative copying of copyrighted works, even if the copies are not offered for sale, may constitute a commercial use."[9] Similarly, 17 U.S.C. § 101 defines "financial gain" as the "expectation of receipt, of anything of value, including the receipt of other copyrighted works." Arguably a person that uploads a work does so with the expectation of downloading something in return.

However, despite the use of the term "file trading" to describe activities on P2P networks, such networks do not operate on the barter system. Uploading and downloading are distinct functions performed by distinct people. Given the size of P2P networks, it is highly unlikely that any two individuals would actually exchange files.

Moreover, even if a court were to find that uploading content onto a P2P network met the commercial advantage/private financial gain standard, what would be the logic – from the sponsors' point of view -- of not lowering the threshold for felony punishment with respect to violations of 17 U.S.C. § 506(a)(2)? Under 17 U.S.C. § 506(a)(2), the prosecutor would already have to show that the defendant distributed copies with a retail value of $1,000. The amendment thus as a practical matter would be lowering the threshold for felony treatment from $2,500 to $1,000.

Further reinforcing the logic, from the sponsors' perspective, of applying the amendment to all of 18 U.S.C. § 2319 is Section 304 of H.R. 2752. Section 304 would amend 17 U.S.C. § 506(a) by adding the "unauthorized reproduction or recording of a motion picture as it is being performed or displayed in a motion picture theatre" as one of the forms of willful infringements deserving of criminal punishment. That is, the recording of a movie in a theatre would be a new § 506(a)(3), joining willful infringement for commercial advantage or private financial gain (§ 506(a)(1)) or the reproduction or distribution of copies with a total retail value of more than $1,000 (§ 506(a)(2)). Presumably the sponsors would want the reduced felony threshold to apply to the

[9] *A&M Records, Inc., v. Napster, Inc.*, 239 F.3d 1004, 1015 (9th Cir. 2001).

uploading of a movie copied in a movie theatre. (The hurried drafting of H.R. 2752 is evident in Section 304. It does not provide for any conforming amendments to 18 U.S.C. § 2319. Thus, 18 U.S.C. § 2319 does not set forth the punishments for a violation of this new criminal offense.)

As noted above, while section 301 does reduce the threshold for felony treatment, it does not amend the basic standard for criminal copyright liability. Hence, the uploading of a work will not automatically constitute a felony. A prosecutor will still need to prove that the uploader 1) infringed the work 2) willfully 3) either for a) purposes of commercial advantage or private financial gain or b) by reproduction or distribution of copies with a total retail value of over $1,000. A prosecutor should have little difficulty with the first two elements. Every court to consider file trading has concluded that the typical file trader is a direct infringer.[10] To the extent a plausible fair use defense can still be mounted, it would apply most strongly to the downloader, not the uploader.

With respect to the willful element, Professor Goldstein in his treatise states that to show willfulness the government must "prove that the defendant knew that his acts constituted copyright infringement or, at least, knew that there was a high probability that his acts constituted copyright infringement."[11] After the *Napster*, *Grokster*, and *Aimster* decisions, it will be difficult for most uploaders to argue that they were not aware, at a minimum, of the high probability that their conduct was unlawful.

Given the dearth of criminal copyright precedent, it is hard to predict whether a prosecutor will have difficulty proving the third element (commercial advantage/private financial gain or $1,000 of copies) with respect to an uploader. A court may very well conclude that a prosecutor has not proven this element beyond a reasonable doubt if the prosecutor only shows that the defendant has uploaded a small number of copyrighted sound recordings. The court may require evidence of the number of downloads of these uploads, or that the defendant also downloaded enough other works to meet the definition of "private financial gain."

If enacted, Section 301 would represent a continuation of the dramatic criminalization of copyright law over the past twenty years. For the first 100 years of federal copyright law, "copyright infringement was exclusively a civil matter."[12] In 1897, Congress imposed misdemeanor penalties for willful infringement for profit. The 1909 Copyright Act continued to treat willful infringement for profit as a misdemeanor.

---

[10] *See A&M Records, Inc., v. Napster, Inc.*, 239 F.3d 1004 (9th Cir. 2001); *In re Aimster*, 334 F.3d 643 (7th Cir. 2003); *MGM Studios, Inc. v. Grokster, Ltd.*, 259 F. Supp.2d 1029 (C.D. Cal. 2003).

[11] 2 Paul Goldstein, Copyright, § 11.4.1(b) at 11:51—52 (2d ed. 2002). It should be noted, however, that courts have not always applied the term "willfully" in a consistent manner. *See* Lydia Pallas Loren, *Digitization, Commodification, Criminalization: The Evolution of Criminal Copyright Infringement and the Importance of the Willfulness Requirement*, 77 Wash. U. L. Q.835 (1999).

[12] *Id*. at 840.

Similarly, the 1976 Copyright Act imposed misdemeanor penalties on infringements done "willfully and for purposes of commercial advantage or private financial gain."

In 1982, 192 years after the adoption of the first federal copyright law, Congress designated certain acts of infringement as felonies. Specifically, the reproduction or distribution of 100 copies of sound recordings, or seven copies of motion pictures or other audio-visual works, could be punished by two years imprisonment.[13] In 1992, Congress passed the Copyright Felony Act, which expanded the scope of the felony provisions to all works, and lowered the threshold for felony treatment to the reproduction or distribution of ten copies with a total retail value of $2,500. Finally, in 1997, Congress enacted the No Electronic Theft (NET) Act, which created 17 U.S.C. § 506(a)(2). The NET Act, therefore, imposed criminal sanctions on the reproduction or distribution of copies with a total retail value of $1,000, even in the absence in any profit motive.[14]

In short, the fifteen years between 1982 and 1997 saw a radical expansion of criminal copyright law. For the first time, Congress imposed criminal sanctions on infringement without a profit motive, and felony penalties on infringements in excess of certain thresholds. Section 301 of H.R. 2752 would significantly reduce these thresholds with respect to the uploading of works on to the Internet.

The expansion of criminal copyright law since 1982 has been effective in combating large scale commercial infringement. Infringing copies of computer software or CDs are not sold openly in stores in the U.S. as they are in many Asian countries. This is because commercial infringers and their distributors know that they face a significant risk of prosecution, conviction, and imprisonment.

At the same time, the non-commercial infringers – the high school and college students engaged in file trading and other forms of infringement over the Internet – know that the likelihood of prosecution is remote. Indeed, the NET Act – § 506(a)(2) --has hardly been used by prosecutors since its enactment in 1997. *See U.S. v. Rothberg*, 222 F. Supp. 2d 1099 (N.D. Ill. 2002). Enforcement of the criminal copyright provisions against non-commercial infringers simply has not been a priority for the Justice Department. The Justice Department correctly perceives that the public has little interest in seeing college students sent to prison merely because they traded songs on the Internet. Making it easier for prosecutors to bring felony charges by lowering the thresholds will not change the Justice Department's priorities.

III. H.R. 2885

While H.R. 2517 and H.R. 2752 focus on reducing copyright infringement over P2P networks, H.R. 2885, introduced by Congressman Joseph Pitts (R-PA), targets

[13] The reproduction or distribution had to occur within a 180 day period. Reproduction or distribution of 1000 copies of sound recordings or 65 copies of motion pictures was punishable by five years imprisonment. *Id.* at 843-44.
[14] *Id*. at 845-49.

children's access to pornography over P2P networks.[15] It is stimulated in part by a March, 2003 General Accounting Office study that found that pornography is readily available to children over P2P networks.[16]

Section 4 of the bill directs the Federal Trade Commission to promulgate regulations relating to P2P software. The FTC is to develop a definition of peer-to-peer file trading software that encompasses "software that enables the transmission of computer files or data over the Internet" and that has as its "primary function" the capability 1) to enable a computer to transmit data to another computer; 2) to enable the user of one computer to request transmission of files or data from another computer; and 3) to enable the user of one computer to designate data available for transmission to another computer. The definition is to exclude "software products legitimately marketed and distributed primarily for the operation of business and home networks, the networks of Internet access providers, or the Internet itself."

Once they define peer-to-peer file trading software, the FTC regulations would require any person who distributes such software to provide recipients with notice that use of the software "may expose the user to pornography, illegal activities, and security and privacy threats." The regulations would further require the distributor, prior to providing the software, to receive verification that the recipient is 18 or older, or, if the recipient is under 18, to receive verifiable parental consent. Verification that the recipient is 18 or older would include accepting and verifying a credit card number. Parental consent would include efforts constituting parental consent under the Children's Online Privacy Protection Act.

The regulations would set forth additional requirements on the P2P distributor. The software must have "the capability to be readily disabled or uninstalled by a user...." The software must not cause a user's computer to function as a supernode without notifying the user and the user taking affirmative steps to activate that capability. Similarly, the software must not disable a firewall or other protective software without notifying the user and the user taking affirmative steps to cause that result.

Finally, under H.R. 2885 the FTC must develop "functional requirements for standard 'do not install' beacons" for parents to install on their computers to prevent the installation and use of P2P software. The FTC must also provide to the public a list of do-not-install beacon products that have been certified by their producers as conforming to the functional requirements. P2P software would then have to comply with the do-not-install beacon.

A violation of the FTC's regulation would be considered an unfair or deceptive act or practice under the Federal Trade Commission Act. H.R. 2885 would authorize the

---

[15] Co-sponsors include Chris John (D-LA), John Sullivan (R-OK), Mike Pence (R-IN), and Jim DeMint (R-SC).

[16] General Accounting Office, Rpt. No. 03-537T, *File Sharing Programs: Child Pornography Is Readily Accessible Over Peer-to-Peer Networks* at 11-12 (March 13, 2003).

FTC to bring enforcement actions against violators. Additionally, a State attorney general could bring a civil action in federal district court if he believes a State resident has been adversely affected by a violation of the FTC regulations.

H.R. 2885 contains several serious flaws. First, the FTC will have great difficulty crafting a definition of "peer-to-peer file trading software." As noted above with respect to the definition of "enabling software" in H.R. 2752, from a technical point of view there is little difference between P2P software and instant messaging software. Thus, the definition runs the risk of being very over-inclusive. On the other hand, the exclusion for "products legitimately markets and distributed primarily for the operation of" the home, business, and Internet access provider networks is so broad that it threatens to swallow the basic definition, particularly if P2P vendors market their products properly.

Second, the FTC does not possess the technical competence to develop functional requirements for a "do-not-install" beacon. Even if the FTC did possess the technical competence, the software and Internet industries, which have generally operated without government regulation, would view the FTC developing functional requirements as a dangerous precedent.

Third, the software industry probably will object to the requirement that P2P software be easy to disable or possess functionalities that require affirmative acts by the user. The industry will likely argue that such requirements interfere with the software design process and retard innovation. This particularly would be the case if the FTC's definition of P2P software was overbroad.

Fourth, H.R. 2885 places a heavy burden on software companies with little benefit to the public. Children under the age of 18 will still have ready access to pornography over the Internet via regular search engines or chatrooms. Additionally, offshore distributors of P2P software may chose not comply with the FTC regulations. While the regulations would require a non-U.S. distributor to designate a resident agent for service of process, see section 4(b)(I), there could be no effective enforcement mechanism against an offshore distributor willing to flout the law.

IV. Prospects for Enactment

Although the companies that distribute P2P software have established two lobbying coalitions in Washington, D.C., they still do not possess significant political power on Capitol Hill. Nevertheless, none of these bills are likely to be enacted in their present form. The absence of companion legislation in the Senate demonstrates these bills' lack of traction.

- H.R. 2517 imposes heavy burdens on the FBI and the Justice Department without providing them with additional resources. Given the looming budget deficit, Congress is unlikely to appropriate additional funds for copyright education. And given the war on terrorism, Congress is unlikely to direct the FBI and the Justice Department to divert existing resources to infringement prevention efforts. Thus,

H.R. 2517 probably will not find significant support in Congress or in the Administration.[17]

- H.R. 2752 probably will also run into significant opposition. The mainstream software and Internet companies such as Microsoft and AOL that distribute "enabling software" will oppose the bill's notice requirement. Public interest groups likely will object to the lowering of thresholds for felony sanctions for the uploading of works onto the Internet. These groups also will oppose the imposition of criminal penalties for misleading domain name registration because of the chilling effect the penalties may have on whistle-blowers and political speech.

- H.R. 2885 almost certainly will encounter strong resistance from information technology companies opposed to the government regulation of software products. They will view H.R. 2885 as a dangerous precedent for FTC involvement in the development and distribution of software products.

At the same time, it is possible that some of the less controversial provisions of these bills will get appended to other pieces of legislation that are moving through Congress. Moreover, these bills reflect a real hostility to P2P systems by important members of Congress. These members are likely to continue attacking P2P software distributors so long as the P2P systems facilitate conduct to which these members of Congress object.

[17] Jana Monroe, the Assistant Director of the FBI's Cyber Division testified at the July 17, 2003 hearing before the House IP subcommittee concerning H.R. 2517. She described the bill as a "positive step toward making Americans aware of the security, privacy and criminal issues related to trafficking in copyrighted works," but she did not support its enactment.