Plan

Date: Wednesday, March 24, 2010 4:46:48 PM
Attachments: CDT comments for IPEC.pdf
ATT227860.htm

The Center for Democracy and Technology is pleased to submit the attached comments regarding the development of the Administration's Joint Strategic Plan for intellectual property enforcement.

Please let me know if you encounter any problems receiving the attachment.

Thank you for your consideration,

Andrew McDiarmid

Andrew McDiarmid
Policy Analyst

CDT
1634 I Street, NW • Suite 1100 • Washington, DC 20006
E andrew@cdt.org • **P (**202) 637-9800 x305 • **F** (202) 637-0968

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

WRITTEN SUBMISSION OF THE CENTER FOR DEMOCRACY & TECHNOLOGY
Re: Intellectual Property Enforcement Joint Strategic Plan

March 24, 2010

The Center for Democracy & Technology (CDT) submits these comments in response to the February 23, 2010, Federal Register notice requesting written submissions regarding the Joint Strategic Plan for intellectual property enforcement.[1] CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet.

While the Federal Register Notice seeks comment on the full range of intellectual property enforcement matters, our comments here will specifically address copyright, which with the growth of the Internet and new digital technologies, has been the site of novel factual disputes and considerable legal uncertainty for users and innovators. This stands in contrast to other intellectual property concerns such as counterfeit products, where the law is reasonably clear and there are potential risks to health and safety.

On copyright matters, CDT seeks balanced approaches to policy and enforcement that respect the rights of content creators without curtailing the Internet's tremendous potential for fostering innovation and free expression. This means that CDT supports vigorous enforcement of existing copyright laws. There is no substitute for bringing enforcement cases against bad actors – both individuals who infringe copyright and companies that actively encourage infringement.[2] At the same time, copyright enforcement should not target technologies or providers of multipurpose online services, because that would risk throwing out the baby with the bathwater; new digital and Internet-based media and communications tools are of great value to consumers, the economy, and society in general.

I. Analyzing the Costs of Violations

CDT welcomes the Federal Register Notice's insistence that submissions directed to economic costs of violations clearly explain the methodology,

---

[1] *Coordination and Strategic Planning of the Federal Effort Against Intellectual Property Infringement: Request of the Intellectual Property Enforcement Coordinator for Public Comments Regarding the Joint Strategic Plan*, 75 Fed. Reg. 35 (Feb. 23, 2010) at 8137-8139 (hereinafter "Federal Register Notice").

[2] *See* Center for Democracy & Technology, *Protecting Copyright and Internet Values: A Balanced Path Forward*, 2005, at 5-6, http://www.cdt.org/copyright/20050607framing.pdf.

assumptions, and data sources behind any calculations or estimates.[3] This is an area in which numbers merit careful scrutiny. Parties commissioning studies often have vested interests in the results, and simplistic methodologies or assumptions can significantly skew the numbers.

For example, it clearly is not the case that each infringing copy of a work means a lost sale.[4] There is no way to know with certainty that all who possess infringing copies would have otherwise purchased legitimate copies. Any methodology equating the two should have little credibility.

Similarly, any reliable calculation would need to avoid assumptions that equate correlation with causation. Showing that a trend correlates with a rise in large scale infringement says little about whether that trend was *caused* by infringement. This is especially true in the Internet context, because the Internet and digital technologies are highly disruptive of existing business models and markets for many reasons other than their possible use for infringement, making this a time of great flux and transition in media and entertainment markets. For example, the rise of the Internet may have enabled increased infringement of music recordings, but it also has enabled a shift to selling songs individually, new marketplace options like podcasts and music streaming services, and changing patterns in the way people consume and enjoy music. With so much in flux, there is no easy, controlled experiment to isolate the impact of infringement.

In addition, the Joint Strategic Plan should be extremely cautious in its assessment of claims of "emerging or future threats" to the economy.[5] The VCR was viewed at first as the scourge of the movie industry. Industry advocates produced impressive calculations based on the amount of unauthorized copying the technology would facilitate once widely adopted.[6] But these dire predictions about the cost to the U.S. economy were wrong; the technology eventually offered tremendous new growth opportunities, and any *costs* associated with infringement the VCR made possible were dwarfed by the *benefits* of those opportunities. In short, for forward-looking analyses, especially of emerging technologies, a myopic focus on threats and costs can paint a dramatically misleading picture.

II. Recommendations

1. In the area of copyright in particular, the Joint Strategic Plan needs to target enforcement against true bad actors. Ratcheting up copyright protections across-the-board would impair legitimate business activity and chill technological innovation and fair use.

It is easy to think of "copyright enforcement" as simply a question of catching and punishing bad actors. There is indeed lots of "plain vanilla" infringement – practices that are clearly illegal, and pirate enterprises that are clearly culpable. If this were the only kind of activity affected, there would be little downside to efforts to ratchet up copyright enforcement and remedies.

In practice, however, copyright enforcement in the information age affects a wide range of entities and behaviors. In a digital economy, many common activities and many well-intentioned

[3] Federal Register Notice at 8137.

[4] Indeed, one empirical study found that "downloads have an effect on sales which is statistically indistinguishable from zero." *See* Felix Oberholzer-Gee and Koleman Strumpf, *The Effect of File Sharing on Record Sales: An Empirical Analysis*, June 2005, http://www.unc.edu/~cigar/papers/FileSharing_June2005_final.pdf.

[5] Federal Register Notice at 8137.

[6] *See, e.g.*, Brief Amicus Curiae of Creators and Distributors of Programs in *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984), at 10, http://w2.eff.org/legal/cases/betamax/betamax_amicus_progcreate.pdf.

parties can face tricky and contentious copyright challenges. In short, there are many gray areas.

This is true for individuals. Any time a consumer forwards an email, or moves content from one device to another, or uses digital tools to create what has become known as "user-generated content," it can raise copyright questions.[7] The legal boundaries separating lawful and unlawful activity often are not clear, especially when fair use is involved.

Even more acute, however, are the challenges facing innovating companies in the Internet and information technology sectors. In today's world, all kinds of devices and services boast computing power, memory, and network connectivity. They enable users to store, transmit, and manipulate data in new ways. Inevitably, they make copies and/or enable users to do so. As a consequence, they often raise novel questions of copyright law. Those questions lead to business disputes and lawsuits.

It is essential for the Joint Strategic Plan to recognize, therefore, that copyright law implicates legitimate innovative companies, not just pirate enterprises. Strong copyright enforcement tools, such as the large statutory damage awards available under 17 U.S.C. § 504, are often brandished against upstart companies in business disputes. Strengthening such tools can significantly increase the leverage of copyright interests in negotiating and trying to obtain settlements, even where it is highly unclear that the law is on their side.

The concern that copyright enforcement can affect innovative businesses operating in good faith is by no means theoretical. Technologies that have been targeted in copyright disputes include the following:

- **VCRs.** Movie studios famously sued Sony, the maker of the original Betamax VCR, for providing users with the ability to record copyrighted television programs. Outcome: The Supreme Court held in 1984 that non-commercial copying for private "time-shifting" is a fair use and that Sony was not liable for the potential infringing behavior of some users.[8] The home video market has since grown into a major source of revenue for the entertainment industry.

- **Network-Based Digital Video Recorder.** Owners of cable television programming sued Cablevision for proposing to offer a digital video recorder – the digital equivalent of a VCR – that would record programs on a central server instead of on a device in the user's home. Outcome: A 2007 court ruling stalled the technology by finding it to violate copyright; a year-and-a-half later, an appeals court reversed, finding no copyright infringement.[9]

- **Family-Friendly DVD Player.** Film directors sued a company that marketed a DVD player designed to skip portions of movies containing sexual or violent content, as well as a company that edited and redistributed lawfully purchased DVDs to achieve the same

[7] *See* Tehranian, John, *Infringement Nation: Copyright Reform and the Law/Norm Gap*, 2007 Utah Law Review 537, http://ssrn.com/abstract=1029151.

[8] *Sony Corp. of America v. Universal City Studios, Inc.*, 464 U.S. 417 (1984).

[9] *The Cartoon Network LP, et al., v. CSC Holdings, Inc. and Cablevision Sys. Corp.*, 536 F.3d 121 (2d Cir. 2008), *cert. denied* 129 S. Ct. 2890.

result. Outcome: Congress stepped in to give family-friendly DVD players a legislative exemption. The company making edited DVDs, however, was ruled to infringe.[10]

- **Portable mp3 Players.** The recording industry sued Diamond Inc., the maker of an early portable mp3 player, arguing that it was required to include copy-protection technology specified in the Audio Home Recording Act. Outcome: The Ninth Circuit Court of Appeals ultimately ruled that devices with multi-purpose computer hard drives were not covered,[11] paving the way for iPods and the rest of the now-booming digital music player industry.

- **Search Engines for Images.** Perfect 10, an adult entertainment company, sued Amazon, Google, and Microsoft for providing online search engines that index and display "thumbnail" versions of images they find posted on third-party websites. A photographer sued an early, smaller provider of image search as well. Outcome: After extensive litigation, the Ninth Circuit Court of Appeals held that the copying and display necessary to operate image search engines constitutes fair use.[12]

- **Full-Text Search for Books.** Major publishers sued Google for its Book Search project, which involves scanning books into an index to enable a full-text search engine. Outcome: After years of uncertainty and litigation, the parties are currently awaiting a court ruling on a complicated settlement that could have far-reaching effects on the book industry and digital licensing.[13]

- **Video-Sharing Websites.** Viacom is currently engaged in a blockbuster suit against YouTube, demanding $1 billion in damages based on infringing videos uploaded by YouTube users.[14] Other video-sharing sites that have been sued on similar grounds include Veoh,[15] MySpace,[16] VideoEgg,[17] Grouper,[18] and Bolt.[19] Outcome: While some cases have been settled or resolved, the YouTube suit remains a major test of the liability safe harbor contained in section 512(c) of the DMCA. Without such safe harbor protection, user-generated content sites like YouTube likely could not exist in anything like their current form.

- **Auction Sites.** Tiffany and Co. brought trademark claims against eBay for the sale by users of counterfeit Tiffany goods through the auction website. Outcome: A court dismissed the trademark claims, but Tiffany is currently appealing.[20] The case could have significant ramifications for intermediary liability and e-commerce.

---

[10] *Clean Flicks of Colo., LLC v. Soderbergh*, 433 F. Supp. 2d 1236 (D. Colo. 2006).

[11] *RIAA v. Diamond Multimedia Systems, Inc.*, 180 F.3d 1072 (9th Cir. 1999).

[12] *Perfect 10, Inc. v. Amazon.com, Inc.*, 508 F.3d 1146 (9th Cir. 2007); *Kelly v. Arriba Soft Corporation*, 336 F.3d 811 (CA 2003).

[13] *The Authors Guild, et. al., v. Google, Inc.*, 05 CV-8136 (DC) (S.D.N.Y 2005).

[14] *Viacom International, Inc. et al v. Youtube, Inc. et. al.*, 07 CV-2103 (LLS) (S.D.N.Y 2007).

[15] *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132; *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099.

[16] *UMG Recordings, Inc. v. MySpace, Inc.*, CV 06-7361 AHM (AJWx) (C.D. Cal. 2008).

[17] *Capitol Records, LLC., et. al. v. VideoEgg*, 08 CV-5831 (S.D.N.Y. 2008).

[18] *UMG Recordings, Inc. v. Grouper, Inc.* CV 06-06561 (C.D. Ca. 2006).

[19] *UMG Recordings, Inc., et al. v. Bolt, Inc., et. al.*, CV 06-06577 (C.D. Cal. 2006).

[20] *Tiffany (NJ) Inc. v. eBay Inc.*, 04-CV-4607 (RJS) (S.D.N.Y. July 14, 2008).

- **Cell Phone Ringtones.** ASCAP sought performance royalties from wireless phone companies for the ringtones that play when users' phones ring. Outcome: A court declined to hold wireless companies liable for royalties every time a user's ringtone rings in public.[21]

- **Garage Door-Opener Remote Controllers.** A maker of garage-door openers sued a maker of a universal remote controller, alleging unlawful circumvention of a technological protection measure protecting the code that operated the garage-door opener. Outcome: After years of litigation, a court rejected this claim.[22]

- **Replacement Printer Cartridges.** Lexmark, a printer manufacturer, sued a maker of replacement ink cartridges for circumventing code designed to bar the use of non-Lexmark cartridges. Outcome: A lower court held for Lexmark, but the Sixth Circuit Court of Appeals eventually overturned that ruling.[23]

- **Computer Equipment Maintenance Services.** StorageTek, a maker of digital storage equipment, argued that an independent company providing maintenance services for StorageTek equipment unlawfully circumvented technological protections restricting access to the software controlling the equipment. Outcome: A court found no DMCA violation because the circumvention was not connected to any act of infringement.[24]

The point here is not that copyright disputes involving new technologies always should be resolved in favor of the technology providers and against the copyright holders. Reasonable people can and do disagree about the optimal legal outcomes from case to case. But it should be clear that mechanisms for enforcing copyright are often brought to bear against technologies that may well be lawful, resulting in substantial uncertainty and delay in the rollout of new or competitive products.

The key lesson is that the Joint Strategic Plan should not aim to tip the scales on tricky legal and policy questions that arise in commercial disputes between legitimate businesses over unsettled questions of copyright law. The Plan should refrain from recommending steps that would have such an effect, either directly or by giving copyright holders powerful new leverage in settlement discussions. Rather, the Plan should focus squarely and exclusively on bad actors and clear-cut cases.[25]

There are several things the Joint Strategic Plan could do to keep a narrow focus on bad actors and avoid creating legal landmines for bona fide businesses.

First, the Plan should concentrate on improving *federal* enforcement efforts – efforts that target true criminal behavior. Thus, in the White House blog post issued concurrently with the Federal Register Notice, the Intellectual Property Enforcement Coordinator (IPEC) cited "counterfeit car

---

[21] *U.S. v. ASCAP (In re Application of Cellco Partnership d/b/a/ Verizon Wireless),* 663 F. Supp. 2d 363 (S.D.N.Y 2009).

[22] *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, 381 F.3d 1178 (Fed. Cir. 2004).

[23] *Lexmark International, Inc. v. Static Control Components, Inc.*, 387 F.3d 522 (6th Cir. 2004).

[24] *Storage Tek v. Custom Hardware*, 421 F.3d 1307 (Fed. Cir. 2005).

[25] This approach is consistent with Federal guidelines on prosecuting intellectual property crimes, which note that "Federal criminal prosecution is most appropriate in the most egregious cases," and "Federal prosecution is most appropriate when the questions of intellectual property law are most settled." U.S. Department of Justice Computer Crime & Intellectual Property Section, *Prosecuting IP Crimes Manual* at chapter IX.B.2, http://www.justice.gov/criminal/cybercrime/ipmanual/09ipma.html.

parts, illegal software, pirated video games, knockoff consumer goods, [and] dangerous counterfeit medicines" as examples of the kinds of behavior that the IPEC aims to fight.[26] All of these examples appear to be products of deliberate wrongdoing rather than of good-faith disputes over unsettled legal questions.

The title of the statute creating the IPEC indicates Congress's focus on "Prioritizing Resources and Organization," rather than reconsidering copyright policy.[27] The provisions concerning the IPEC's Joint Strategic Plan and annual report emphasize setting priorities,[28] preventing duplication,[29] coordinating the work of relevant agencies,[30] improving efficiency in the allocation and use of Federal resources,[31] and ensuring the sharing of information between agencies and with foreign law enforcement.[32] The description of the contents of the Joint Strategic Plan calls for a general analysis of the threats and costs of intellectual property violations, but otherwise focuses exclusively on how to improve the efforts and activities of the "Federal Government" and the relevant "departments and agencies."[33]

All of this argues for a Plan that sets out how the federal agencies involved in copyright enforcement can better do their job of prosecuting serious intellectual property crimes. The Plan should not make controversial policy recommendations regarding the *civil* side of copyright enforcement – the side that often leads to lawsuits involving bona fide businesses. The Plan should particularly steer clear of recommendations that could affect the scope of liability for civil infringement. As should be apparent from the bullet point list above, questions regarding when and whether copyright liability should extend beyond individual infringers to the providers of technology and services is a highly complicated issue with major implications not just for copyright holders, but for multiple sectors of the U.S. economy and for the public.

Second, in coordinating the development of the Joint Strategic Plan, the IPEC should make sure that each proposed action or recommendation is subject to rigorous cost-benefit analysis. The IPEC should be particularly alert to the risk that, where the benefits and costs of a measure accrue to different parties, it can be in the interest of the beneficiaries (likely the rightsholders) to lobby strongly even for a measure that offers relatively minor private gains at high social cost. In short, careful, independent consideration and balancing of the true costs and benefits of suggested measures for inclusion in the Plan will be essential. This kind of cost-benefit analysis needs to be incorporated in a formal and systematic way into the process for developing the Joint Strategic Plan. If, as discussed in the next section, the reduction is likely to be of marginal size or fleeting duration while imposing significant burdens on (for example) legitimate innovators or online free expression, then the proposal should not be included in the Plan.

Third, if the Joint Strategic Plan delves into legislative recommendations relating to civil copyright laws and private copyright litigation, it should include measures to protect legitimate companies from being subject to the same tough enforcement tools as true piracy rings. As

---

[26] Victoria Espinel, *Intellectual Property and Risks to the Public*, The White House Blog, Feb. 23, 2010, http://www.whitehouse.gov/blog/2010/02/23/intellectual-property-and-risks-public.

[27] Prioritizing Resources and Organization for Intellectual Property Act of 2008, Pub. L. No. 110-403 (2008) (hereinafter "PRO IP Act").

[28] *See* PRO IP Act § 303(e)(1), (e)(2), (f)(2), (f)(3).

[29] *See* PRO IP Act §§ 303(a)(2), 303(f)(1), 304(b)(6), 304(b)(10).

[30] *See* PRO IP Act §§ 301(b)(1)(D), 303(e)(7), 304(b)(4).

[31] *See* PRO IP Act § 303(e)(2), (e)(3),(f)(1).

[32] *See* PRO IP Act §§ 303(a)(3), 303(a)(7), 304(b)(4), 304(b)(8).

[33] *See* PRO IP Act § 303(e)(1), (2), (6), (7), (8).

discussed above, and also below under recommendation #3, CDT does not believe that the Plan should expand its focus beyond improving the effectiveness of *Federal* enforcement mechanisms. But if it does, the Plan should recognize that the litigation risks that copyright law imposes on legitimate businesses is already a significant problem. In the digital age, statutory damages of anywhere from $750 to tens of thousands of dollars per work infringed[34] quickly reach astronomical levels that could break the backs of most companies. A company that believes with 98 percent certainty that its activity is lawful (that it falls within fair use, for example) still needs to consider whether it would be wise to take a two percent risk of bankrupting the company.

Thus, current copyright law can chill innovation, and further changes to expand or strengthen enforcement tools could exacerbate the problem. One way the Plan could try to help address this issue would be by recommending legislation to amend 47 U.S.C. § 504(c)(2) to eliminate statutory damages for companies that believed their behavior to be lawful based on a reasonable interpretation of copyright law.[35] Actual damages would still be available, protecting any rights holder that suffers identifiable harm. Representatives Boucher, Doolittle, and Lofgren introduced a bill in 2007 that provides a possible model.[36]

2. The Plan should not call for imposing a new network-policing role on Internet Intermediaries.

Congress has expressly rejected the notion that Internet service providers (ISPs) should be held responsible for policing user behavior. 47 U.S.C. § 230(c)(1) states that ISPs and other "interactive computer services" shall not be treated as the publishers or speakers of "any information" provided by users. 17 U.S.C. § 512(a) directs that ISPs shall not be held liable for any copyright damages when users transmit infringing material. These legislative safe harbors reflect a deliberate policy choice – a choice to allow ISPs to focus on empowering communications by and among users *without* the ISPs monitoring, supervising, or playing any other kind of "gatekeeping" role with respect to such communications.

That policy choice has yielded significant benefits, creating an Internet environment that fosters a tremendous amount of innovation, speech, collaboration, civic engagement, and economic growth. The Plan should not take the myopic approach of endorsing an IP enforcement strategy that is inconsistent with that broader policy.

Requiring or encouraging ISPs to assume a new network-policing role would also conflict with U.S. foreign policy regarding Internet freedom. The PRO IP Act makes clear that the Joint Strategic Plan should focus substantial effort on assisting, coordinating with, and influencing foreign governments.[37] At the same time, as Secretary of State Clinton explained in January, promoting Internet freedom in foreign countries is now a major U.S. foreign policy goal.[38] The United States intends to urge other countries to allow the provision of Internet access as an open communications platform without centralized supervision or monitoring. Indeed, Secretary

---

[34] *See* 47 U.S.C. § 504(c)(1).

[35] Current law provides for a reduction in statutory damages if an infringer can prove that there was "no reason to believe" that the actions constituted infringement. 47 U.S.C. §504(c)(2). But this is a difficult standard, and damages cannot be reduced below $200 per work infringed in any event, which could still multiply quickly for an entity offering a digital product or service.

[36] H.R. 1201 § 2(a), 110th Cong., 1st Sess. (2007).

[37] *See* PRO IP Act §§ 303(a)(5)-(7), 303(f), 304(b)(3), 304(b)(7).

[38] Secretary of State Hillary Rodham Clinton, Remarks on Internet Freedom, address at The Newseum, Jan. 21, 2010, http://state.gov/secretary/rm/2010/01/135519.htm.

Clinton said that the U.S. State Department is urging private sector companies "to take a proactive role in challenging foreign governments' demands for censorship and surveillance."[39]

It would be difficult if not impossible to square this policy, calling on companies to resist government calls for censorship and surveillance, with a U.S. Government mandate that ISPs police the content of Internet communications for purposes of ferreting out copyright infringement. To be clear, CDT does not in any way suggest that copyright enforcement is the moral equivalent of censorship. But there is a clear tension in pressing ISPs to resist the demands of foreign governments to monitor, filter, or otherwise police the content of Internet communications while at the same time insisting that ISPs should accept direction from the U.S. Government to police Internet communications at home. Repressive regimes that outlaw certain kinds of speech would say their restrictive Internet policies were really no different than U.S. copyright policy: in both cases, governments would be calling on ISPs to police user behavior to prevent certain unlawful communications.

In short, as CDT recently told the Senate Subcommittee on Human Rights and the Law, "we must take care not to set precedents can be used by authoritarian regimes to justify their own acts of censorship and surveillance."[40] The Joint Strategic Plan should not set such a precedent by calling on ISPs to assume a new role as copyright police.

This is not to say that there is no room for cooperation between ISPs and copyright holders. It has been widely reported that many ISPs, on a voluntary basis, work with copyright holders to forward warning notices to subscribers that copyright holders identify as suspected infringers.[41] The notices make it clear that the subscribers' behavior is not as anonymous as they may have believed. In the case of families sharing a computer, a notice may alert the parents that a child is engaged in unlawful filesharing, which may prompt the parents to put a stop to it. Given the potential for very large statutory damages, such warning notices may be quite effective in prompting recipients to cease infringement.[42]

Policies to enlist ISPs more broadly, however, raise significant concerns. The Plan should steer clear of two kinds of policies in particular: "three strikes" or "graduated response" policies calling on ISPs to terminate the Internet access of subscribers that copyright holders claim are infringers; and automatic filtering policies calling on ISPs to install technical systems that purport to identify and block transmissions of copyrighted material on an automated basis.

"Graduated Response" Policies

Rightsholders are increasingly promoting policies by which ISPs would penalize alleged infringers through a series of escalating warnings and sanctions, potentially including disconnection from the Internet. The most widely known example of this approach is a controversial law passed in France in 2009, which established Internet cutoff as a supplemental

---

[39] *Id.*

[40] Statement of CDT before the Senate Judiciary Committee, Subcommittee on Human Rights and the Law: *Global Internet Freedom and the Rule of Law II*, 111th Congress, 2nd Sess. Mar. 2, 2010, at 8, http://www.cdt.org/files/pdfs/20100302_cdt_global_net_freedom.pdf.

[41] *See, e.g.,* Sarah McBride and Ethan Smith, "Music Industry to Abandon Mass Suits," *Wall Street Journal*, December 19, 2008, http://online.wsj.com/article/SB122966038836021137.html.

[42] A 2007 Canadian study found notices effective at deterring infringement. *See* "E-mail warnings deter Canadians from illegal file sharing," *CBC News*, February 15, 2007, http://www.cbc.ca/consumer/story/2007/02/14/software-warnings.html.

penalty for online copyright offenses.[43] The British parliament is considering legislation that contemplates similar penalties.[44] And while CDT is aware of no concrete proposals in the U.S. yet, major U.S. copyright interests appear to be pushing for ISPs to take a more active role in policing infringement.[45]

CDT urges the IPEC and others within the administration to reject the enlistment of ISPs in copyright enforcement through Internet disconnection. As explained above, any endorsement of this approach would be at odds with longstanding U.S. policy. Moreover, graduated response policies have proven extremely controversial, and raise a number of concerns with respect to proportionality, due process, and free expression. Even in Europe, where these policies have gained some traction, they have recently encountered serious opposition from the European Parliament and the European Data Protection Supervisor based on similar concerns.[46] Given the growing necessity of Internet access to full participation in modern society, these measures should not be taken lightly, and may indeed raise serious constitutional problems if enacted in the United States.

Disconnection of Internet access would generally be a disproportionate response to copyright infringement. The Internet has become a core component of the right to free speech and access to information; it is vital to all aspects of life, including personal communication, employment, health care, education, and civic participation. It has become increasingly difficult if not impossible to conduct research, search for a job, or locate indispensable commercial and government services without some sort of Internet connection. Simply put, being online is now an essential part of the day-to-day lives of many in American society. The Obama administration has recognized the importance of this medium, and made the expansion of broadband Internet access a national priority.[47]

Given this importance, courts have been reluctant to impose Internet bans on wrongdoers, even in extreme cases. Courts have imposed restrictions on convicted child predators, for example,

---

[43] French Parliament, Law number 2009-669, enacted June 12, 2009, http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000020735432&categorieLien=id (in French).

[44] United Kingdom Parliament, Digital Economy Bill [HL] 2009-10, http://services.parliament.uk/bills/2009-10/digitaleconomy/documents.html.

[45] Parties in recent proceedings at the Federal Communications Commission have urged endorsement of graduated response. *See, e.g.*, Comments of the Motion Picture Association of America in the matter of A National Broadband Plan for our Future, FCC GN Docket No. 09-51, http://fjallfoss.fcc.gov/ecfs/document/view?id=7020244174. In addition, the confidential Anti-Counterfeiting Trade Agreement (ACTA) being negotiated by the U.S. Trade Representative reportedly endorses it. *See* Michael Geist, "ACTA Internet Chapter Leaks: Renegotiates WIPO, Sets 3 Strikes as Model," February 21, 2010, http://www.michaelgeist.ca/content/view/4808/125/. Lastly, there have been widespread reports of private negotiations between content producers and ISPs, as well as reports of discussions of the controversial policy within the Obama administration. *See* Josh Gerstein, "Web piracy, 3-strikes and Biden: what Ari said," *Politico Under the Radar Blog*, http://www.politico.com/blogs/joshgerstein/0310/Web_piracy_3strikes_and_Biden_what_Ari_said.html.

[46] European Data Protection Supervisor Peter Hustinx denounced ACTA and "three strikes Internet disconnection" in a recent opinion. *See* Opinion of the European Data Protection Supervisor on the current negotiations by the European Union of an Anti-Counterfeiting Trade Agreement, February 22, 2010, http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2010/10-02-22_ACTA_EN.pdf. In addition, the European Parliament overwhelmingly passed a resolution condemning the secrecy of ACTA negotiations and questioning disconnection penalties' consistency with human rights. *See* Motion for a resolution – Anti-Counterfeiting Trade Agreement (ACTA), March 10, 2010, http://votewatch.eu/cx_vote_details.php?id_act=456&lang=en.

[47] Federal Communications Commission, *Connecting America: The National Broadband Plan*, GN Docket No. 09-51, March 17, 2010, http://broadband.gov/download-plan.

but judges there have taken an individualized, narrowly tailored approach in approving the restrictions. Courts have struck down permanent bans on access[48] and opted for supervised access rather than no access.[49] One court, in overturning a ban, wrote:

> "Computers and Internet access have become virtually indispensable in the modern world of communications and information gathering. The fact that a computer with Internet access offers the possibility of abusive use for illegitimate purposes does not, at least in this case, justify so broad a prohibition."[50]

Disconnection is a penalty best reserved for the most egregious offenses, and even then courts impose it only upon careful consideration of the individual circumstances.

It is important to note that where courts have approved Internet access restrictions, they have done so only as part of sentencing or supervised release agreements – that is, following full criminal trial and conviction. In contrast, graduated response proponents in the U.S. advocate the development of private agreements between major copyright holders and ISPs, under which it is not at all clear that users will possess sufficient due process and appeal rights.[51]

Concerns about due process and proportionality are only exacerbated by the importance of the Internet to free expression. Courts have time and again recognized the significance of the Internet as a vital platform for speech and political participation – extending the highest level of First Amendment protection to this medium.[52] Any government action that results in cutting off a person's Internet access would therefore raise serious First Amendment problems. Such action would severely curtail the exercise of core speech rights and impact a person's ability to participate in many aspects of social, economic, and political life. The Plan should not invite constitutional jeopardy by putting the weight of the Federal Government behind disconnection policies.[53]

In light of the foregoing serious concerns raised by the prospect of Internet disconnection penalties, the Joint Strategic Plan should not endorse the adoption of "three strikes" or "graduated response" policies by ISPs.

Automated Content Filtering

A second troubling potential avenue for ISP copyright enforcement is automated content filtering. In recent years, major content producers have openly expressed their support for

---

[48] *See, e.g., U.S. v. Voelker*, 489 F.3d 189 (3rd Cir. 2007).

[49] *U.S. v. Boston*, 494 F.3d 660 (8th Cir. 2007).

[50] *United States v. Peterson*, 248 F.3d 79 at 83 (2d Cir. N.Y. 2001) (striking a condition of probation that would have restricted computer ownership and Internet access as unreasonably broad given the defendant's crime and the impact on the defendant's ability to work in his profession).

[51] *See, e.g.,* MPAA Comments, *supra* note 44.

[52] *Reno v. ALCU*, 521 U.S. 844 (1997).

[53] CDT will soon release a paper detailing the constitutional concerns that would be raised by any government policy directing ISPs to implement a "three strikes" regime resulting in Internet disconnection.

filtering technologies and their interest in seeing ISPs install them.[54] However, while filtering may seem attractive for reasons of scalability and comprehensiveness, the Joint Strategic Plan should avoid encouraging or endorsing its use by ISPs. In addition to contravening U.S. policy as described above, content filtering at the ISP level carries significant costs, both in terms of the core values of free expression and privacy, and in terms of the financial and performance burdens associated with filters' installation and operation.

Foremost among the downside risks to network-level filtering is its potentially significant adverse impact on free expression and fair use online. Filtering inevitably involves some risk of overblocking, the unintended filtering of constitutionally protected material. Even a low-percentage error rate will impact innumerable legal transmissions, given the speed and scale of Internet communication.[55] This should be unacceptable in a medium for global communication and commerce on which people increasingly depend in their personal, professional, and civic lives.

Moreover, as discussed above with respect to "graduated response" and Internet disconnection, the impact on legitimate speech can raise serious First Amendment concerns. To the extent the government mandates or encourages the use of filters that can impede legal speech, such regulations may well be met with strong constitutional challenges.

Filters' impact on free expression is exacerbated by the fact that even some communications *correctly* identified by an automatic filter will nonetheless be perfectly legal. This would be true in cases of fair use, or cases in which the user has an otherwise valid license for the recognized content. For instance, the transmission of a legal documentary film making fair or licensed use of other video footage might be unduly filtered and blocked simply because the filter recognizes the incorporated footage.

Making fair-use determinations is simply impossible to automate. Fair use is a notoriously fact-specific gray area of copyright law involving a complex balancing of factors. Software designed to find matches and apply firm rules to them is ill-suited to making such determinations. Given the fact-specific nature of fair use, a perfect filter is impossible; whatever rules one might distill from fair use case law, certain edge cases would inevitably be unduly caught or ignored by the filter. Importantly, fair use is not some minor or fringe concept; it is a critical limitation to copyright that facilitates creativity and protected expression. The Supreme Court has said that fair use guarantees "breathing space within the confines of copyright"[56]; it prevents copyright protection from unduly conflicting with free speech. Any form of automated copyright enforcement that diminishes the protections fair use provides should therefore be discouraged.

The use of filters would also come at considerable cost to Internet users' privacy. In order to be comprehensive – a feature filtering proponents tout – a filtering system must be "always on." To catch all acts of infringement, all traffic must be scrutinized and checked against the filter.

---

[54] *See* Saul Hansell, "Bits Debate: Should Internet Providers Block Copyrighted Works?" *New York Times Bits Blog*, January 15, 2008, http://bits.blogs.nytimes.com/2008/01/15/bits-debate-should-internet-providers-block-copyrighted-works; *See also* "Internet Copyright Filters: Finding the Balance," panel discussion at State of the Net conference, January 30, 2008, http://www.netcaucus.org/conference/2008/audio-copyright.shtml.

[55] *See* Australian Communications and Media Authority (ACMA), *Closed Environment Testing of ISP-Level Internet Content Filters: Report to the Minister for Broadband, Communications and the Digital Economy*, June 2008, http://www.acma.gov.au/WEB/STANDARD/pc=PC_311316; *See also CDT v. Pappert*, 337 F.Supp.2d 606 (E.D. Penn. 2004) (noting the effects of overblocking on protected speech).

[56] *Campbell v. Acuff-Rose Music, Inc.*, 510 U.S. 569 (1994).

Pervasive surveillance of this sort would run counter to users' expectations of privacy and the traditional roles of ISPs, and could lead to major abuses.

Constant monitoring of Internet traffic would necessitate the use of deep-packet inspection (DPI) technology, which allows ISPs to examine the contents of users' communications in ways not ordinarily necessary to route traffic to its intended recipients. Widespread and indiscriminate use of DPI would give ISPs unwarranted access to customers' legal, but personally sensitive, information.[57] Users quite simply do not expect such surveillance. If consumers come to learn that their ISPs are monitoring and perhaps recording every step they take online, DPI runs the risk of damaging consumer confidence in the medium. This could have a chilling effect on the use of the Internet for beneficial purposes, including academic, financial, and health services. In addition, this would compromise speakers' ability to remain anonymous, a valuable aspect of online free expression.[58]

Surveillance on the scale necessary to implement copyright filtering would also be out of step with carefully considered U.S. policy under which ISPs are under no obligation to actively monitor their networks, as described above. More specifically, in the context of privacy, full-time monitoring might run afoul of applicable laws. The Electronic Communications Privacy Act prohibits service providers' interception of electronic communications except as necessary to the rendition of the service or with user consent.[59] Full-time interception for the purpose of enforcing third-party copyrights likely does not, in our view, meet this standard. Given existing U.S. policy and the risks to consumer privacy, the Joint Strategic Plan should not endorse policies that would lead to this kind of surveillance.

Implementing filtering also would carry significant financial and performance costs for ISPs. ISPs would have to add hardware and software to their networks, requiring upfront investment and additional ongoing maintenance and support costs.[60] No matter how fast or sophisticated this equipment becomes, adding the additional steps of examining and recognizing content in transit can introduce significant latency within a network, which can have significant costs to network operations. For example, as part of its proposed national filtering scheme, the Australian government conducted a closed-network test of various filtering products in 2008. While the results showed some improvement over earlier tests, five of six products tested degraded network performance significantly, two by more than 75 percent.[61] Similarly, in evaluating fingerprinting-based copyright filtering for a university network, one university researcher testified to Congress that "there is no practical way to do full-file comparison without seriously degrading network performance."[62] Even small delays can have substantial

---

[57] *See* Statement of Leslie Harris, CDT, before the House Committee on Energy and Commerce, Subcommittee on Communications, Technology and the Internet: *The Privacy Implications of Deep Packet Inspection*, April 23, 2009, http://cdt.org/privacy/20090423_dpi_testimony.pdf.

[58] *See* Julie Cohen, *A Right to Read Anonymously: A Closer Look at 'Copyright Management' In Cyberspace*, 28 Conn. L. Rev. 981 (1996), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=17990.

[59] 18 U.S.C. § 2511(2)(a)(i); (2)(c).

[60] See, e.g., *ACLU v. Gonzales*, 478 F. Supp. 2d 775 (E.D. Pa. 2007) (estimating the cost of web-based geographic filtering services); *see also* Statement of Dr. Adrian Sannier, Arizona State Univ., before the House Committee on Science and Technology, *The Role of Technology in Reducing Illegal Filesharing: A University Perspective,* June 5, 2007, http://democrats.science.house.gov/Media/File/Commdocs/hearings/2007/full/05june/sannier_testimony.pdf.

[61] ACMA, *Closed Environment Testing*, *supra* note 54.

[62] Statement of Dr. Greg Jackson, University of Chicago, before the House Committee on Science and Technology, *The Role of Technology in Reducing Illegal Filesharing: A University Perspective,* June 5, 2007, http://democrats.science.house.gov/Media/File/Commdocs/hearings/2007/full/05june/jackson_testimony.pdf.

consequences. Recent evidence shows that even a few milliseconds' delay can have a significant financial impact on websites' usage and associated revenue.[63] Furthermore, the investment required to maintain a robust filtering system is likely to increase over time as increases in the amount Internet traffic will necessitate more and faster filters.

Finally, addressing infringement through the use of filters would likely provoke an ongoing and ultimately futile arms race with infringers. Increased sophistication of filters will be met with increased ingenuity in infringers' efforts to avoid them.[64] Before long, widespread filtering by ISPs would likely cause infringement networks to encrypt traffic, rendering filters wholly unable to identify content. The prospect of such escalation raises serious questions as to whether automated filtering indeed offers the potential benefits its proponents suggest.

Especially in light of these questions about their ultimate effectiveness, network-level filters must be evaluated by weighing their potential benefits with the serious costs described above. Over time, any benefits would likely diminish significantly, while would likely costs rise. The Joint Strategic Plan should refrain from recommending such a tenuous approach.

3. For copyright, the Plan should focus on effective and efficient use of existing legal tools. It should not focus on trying to increase penalties, expand the scope of copyright liability, or otherwise make substantive changes to the copyright regime.

In the area of copyright, the Joint Strategic Plan should aim to ensure that relevant Federal agencies and authorities make the most of the legal tools at their disposal. As discussed above, the pertinent portions of the PRO IP Act contain numerous references to setting priorities, eliminating duplication, coordinating activities, and sharing information.[65] Again as discussed above, such activities could improve enforcement against true bad actors without negatively impacting lawful behavior by bona fide companies or members of the public.

By contrast, the Plan should not take on the very different task of trying to reshape substantive copyright law or policy by making significant legislative recommendations regarding such matters as what remedies are available or when parties may be held liable for infringement committed by others under the doctrine of secondary liability. Substantive changes to copyright law, especially civil law enforced largely by private lawsuits, would have serious repercussions for many activities and parties with no connection to any behavior that is clearly unlawful.

In this context, it is important to recognize that Congress has already provided rights holders with a powerful set of copyright enforcement tools, including a number or recent additions and updates:

- Rights holders can bring lawsuits against infringers.
- Rights holders can bring secondary liability lawsuits against companies that actively induce infringement, following the Supreme Court's 2005 *Grokster* decision.[66]

---

[63] *See* Mehan Jayasuriya et. al. (Public Knowledge), *Forcing the Net Through a Sieve: Why Copyright Filtering is Not a Viable Solution for U.S. ISPs*, 2009, at 42, http://www.publicknowledge.org/pdf/pk-filtering-whitepaper-200907.pdf.

[64] *See* Peter Biddle et. al., *The Darknet and the Future of Content Distribution*, Microsoft Corp., 2002, http://msl1.mit.edu/ESD10/docs/darknet5.pdf.

[65] *See supra* notes 26–32.

[66] *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913 (2005).

- Rights holders benefit from a generous statutory damages regime that allows them to recover from $750 to $150,000 per work infringed, without having to make any showing regarding actual damages suffered. The threat of such statutory damages gives rights holders considerable leverage in settlement or cease-and-desist discussions with actual or potential defendants.

- The "notice-and-takedown" regime created by section 512(c) of the DMCA enables rights holders to demand the removal by online content hosts (Web site hosting companies, user-generated content sites, etc.) of any material the rights holders identify as infringing.

- The anticircumvention provisions of section 1201 of the DMCA give the force of law to any technological protection measures that individual rights holders choose to deploy. Whenever a rights holder employs "digital rights management" technology to limit access to a copyrighted work – whatever form such DRM may take – violating the limits becomes not just technologically more difficult, but illegal as well.

- The 2005 Family Entertainment and Copyright Act created tough new penalties for using camcorders in movie theaters and for copyright infringement involving works that have not yet been commercially released.

- The recently enacted PRO-IP Act, in addition to creating the IPEC and providing additional resources for intellectual property law enforcement efforts, provides for civil forfeiture of any property used to commit or facilitate copyright violations.

The continued existence of infringement should not be taken as evidence that these tools are too weak. As discussed below, eliminating infringement entirely is an impossible goal, so it will *always* be possible to argue that legal remedies should be further expanded and that penalties and damages should be further ratcheted up. But this kind of never-ending, one-way ratchet, resulting in copyright enforcement tools of ever-increasing reach and severity, would carry major costs. Rather than launch a highly contentious debate about the substance of the current copyright law legal regime, the Joint Strategic Plan should strive to ensure that the range of existing legal tools on the civil side is buttressed and complemented by effective and efficient Federal enforcement against criminal violations.

4. The Plan's goal for copyright should be realistic: making participation in widespread infringement relatively unattractive and risky, compared to participating in lawful markets.

Eliminating copyright infringement completely is likely an impossible task. The goal of policy needs to be more realistic: not to prevent infringement entirely, but rather to make it relatively unattractive and risky compared to participating in legal markets. Some people will no doubt continue to engage in large-scale infringement no matter what. But the software industry has managed to be quite profitable despite stubbornly high rates of infringement, demonstrating that a content business does not need to eliminate all illegal infringement in order to succeed.

In short, the Plan's goal for copyright should be to make infringement risky and unattractive compared to lawful alternatives. This goal is echoed in the PRO IP Act, which characterizes the Plan's objective as "[r]educing" infringing goods in the supply chain, not eliminating them.[67] It is

[67] PRO IP Act § 303(a)(1).

also worth noting that this goal cannot be achieved by enforcement efforts alone; it also requires that copyright industries provide legal offerings that are compelling and convenient.

Efforts to pursue a more ambitious goal – such as complete or near-complete elimination of large-scale infringement – would risk taking the Plan in a harmful direction. Copying and disseminating data are core functions of computers and the Internet. Any law or policy aiming to curtail the *technical* capability of people to engage in copyright infringement, therefore, has to go down the radically dangerous path of restricting access to or hobbling the very technologies that are central to the information economy. In the computer and Internet age, there simply is no good policy option for making infringement technically infeasible.

Framing the goal in a realistic way should help clarify that the Plan need not and should not issue recommendations targeting multipurpose technologies or multipurpose online services in a vain attempt to restrict the public's access to technological tools that have the potential to be employed for infringement. Rather, the Plan, and Federal copyright policy generally, should focus on deterring and punishing the illegal *use* of digital technologies and services.

III. Responses to Supplemental Comment Topics Listed in Notice

Question 7: Technologies for Identifying Infringement

In the Internet context, CDT believes the Joint Strategic Plan should be wary of the limitations and costs associated with automatic filtering technologies. Automatic filters cannot readily separate infringing uses from licensed uses or fair uses. Furthermore, widespread adoption of network-level filtering technologies would likely drive infringement onto encrypted networks, negating the technologies' potential benefits. Meanwhile, network-level filtering technologies carry significant costs to free expression and user privacy. We address these issues in detail as part of recommendation 2 above.

Question 14: Methods to Limit or Prevent Internet-based Infringement

Preventing all online infringement is an unrealistic goal, and efforts to achieve an Internet with no infringement will come at significant cost to Internet openness and legal, beneficial innovation. Enforcement efforts should instead focus on truly bad actors, in concert with the development of lawful alternatives and educational efforts to reduce demand for infringing copies of creative works. The importance of crafting achievable goals that focus on truly bad actors is discussed in recommendations 1 and 4, above.

Question 15: Types of Entities Involved in Infringement

CDT strongly recommends that the Joint Strategic Plan avoid recommending that ISPs play a greater role in policing or enforcing online copyright infringement. Increased monitoring for and enforcement of third-party copyrights would be a radical departure from the way U.S. policy has traditionally approached Internet intermediaries, and such measures would likely have a damaging impact on free expression and user privacy. Furthermore, to the extent that measures limiting online free speech are encouraged or incentivized by the government, they would likely raise serious constitutional problems. Lastly, increased policing of online activity by

intermediaries may frustrate the U.S. foreign policy goal of preserving online free expression globally. These issues are discussed in detail as part of recommendation 2, above.

Question 19: Strategies for Reducing Demand for Infringing Goods

The best way to decrease demand for infringing creative works online is to increase the availability of lawful alternatives that are convenient and attractive to consumers. The Joint Strategic Plan should endorse the continued development of such alternatives, while recognizing that market forces and not government intervention are the preferable means to guide their development.

CDT appreciates the opportunity to comment in the development of the Joint Strategic Plan for intellectual property enforcement. We are available for further discussion on these and other digital copyright issues as the IPEC develops the Plan.

Respectfully submitted,

Leslie Harris, lharris@cdt.org
David Sohn, dsohn@cdt.org
Andrew McDiarmid, andrew@cdt.org