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

# COMMENTS OF THE CENTER FOR DEMOCRACY & TECHNOLOGY

## In Response to the Department of Commerce Internet Policy Task Force's Inquiry on Copyright, Creativity, and Innovation in the Internet Economy

**November 19, 2010**

The Center for Democracy & Technology (CDT) submits these comments in response to the October 5, 2010 Notice of Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy.[1] CDT is a non-profit, public interest organization dedicated preserving and promoting openness, innovation, and freedom on the decentralized Internet.

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.

In short, there is no inherent conflict between copyright protection and enforcement on the one hand and Internet innovation on the other; indeed, better respect for copyright and reduced levels of infringement would promote and enable innovation and expressive activity in a number of ways. But the *means* chosen to pursue copyright goals matter a great deal. Some potential tactics could be attractive from a copyright protection perspective, but would carry significant costs to innovation.

---

[1] Department of Commerce, *Inquiry on Copyright Policy, Creativity, and Innovation in the Internet Economy,* 75 Fed. Reg. 192 (Oct. 5, 2010) at 61419-61424.

[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.

CDT believes that the Internet Policy Task Force, in preparing its report in this area, should take care to observe the following principles.

**1. Copyright enforcement should target 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 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.[3] 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 policymakers to recognize, therefore, that copyright law implicates legitimate innovative companies, not just pirate enterprises. Strong copyright enforcement tools, such as the large statutory damages 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 is it 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 have been targeted in copyright disputes including 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.[4] The home video market has since grown into a major source of revenue for the entertainment industry.

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

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

- **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.[5]

- **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 result. Outcome: Congress stepped in to give family-friendly DVD players a legislative exemption. The company making edited DVDs, however, was ruled to infringe.[6]

- **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,[7] 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.[8]

- **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.[9]

- **Video-Sharing Websites.** Viacom is currently engaged in a blockbuster appeal against YouTube, demanding $1 billion in damages based on infringing videos uploaded by YouTube users.[10] Other video-sharing sites that have been sued on similar grounds include Veoh,[11] MySpace,[12] VideoEgg,[13] Grouper,[14] and Bolt.[15] Outcome: While some

---

[5] *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.

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

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

[8] *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).

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

[10] Viacom Int'l v. YouTube, 2010 U.S. Dist. LEXIS 62829 (S.D.N.Y. June 2010)*, appeal docketed,* No. 10-3270 (2nd Cir. 2010).

[11] *Io Group, Inc. v. Veoh Networks, Inc.*, 586 F. Supp. 2d 1132; *UMG Recordings, Inc. v. Veoh Networks, Inc.*, 665 F. Supp. 2d 1099 (C.D. Cal. Sept. 2009), *appeal docketed*, No. 09-56777 (9th Cir. 2009).

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

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

cases have been settled or resolved, the YouTube and Veoh suits are on appeal to the Second and Ninth Circuits, respectively, after the video-sharing sites prevailed at the district court level. These appeals constitute major tests 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.[16] The case could have significant ramifications for intermediary liability and e-commerce.

- **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.[17]

- **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.[18]

- **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.[19]

- **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.[20]

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 when and whether copyright liability should extend beyond individual infringers to the providers of technology and services is a highly complicated issue with major

---

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

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

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

[17] *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).

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

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

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

implications not just for copyright holders, but for multiple sectors of the U.S. economy and for the public. Law and policy in this area should be careful to keep a narrow focus on bad actors and avoid creating legal landmines for bona fide businesses.

Any new copyright enforcement policies, therefore, should include measures to protect legitimate companies from being subject to the same tough enforcement tools as true piracy rings. Indeed, 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[21] can 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 if 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, copyright law can chill innovation, and further changes to expand or strengthen enforcement tools could exacerbate the problem. One option for addressing this problem 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.[22] 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.[23]

**2. Existing policies establishing safe harbors for Internet intermediaries have been tremendously successful. Policymakers should avoid abandoning those policies in favor of imposing new network-policing roles on intermediaries.**

It is longstanding U.S. policy that intermediaries such as websites, hosting services, and Internet service providers ("ISPs") generally should not be liable for content created by their users. In section 230 of the Communications Act and section 512 of the Digital Millennium Copyright Act, Congress provided important statutory safe harbors from liability in such areas as defamation and copyright.[24] In the courts, the landmark 1984 case involving the Sony Betamax established the principle that making and distributing a product does not give rise to liability for infringements users may commit with that product, so long as the product is "capable of substantial noninfringing use."[25] The 2005 Grokster decision reaffirmed the "substantial noninfringing use" test: taking active steps to promote and encourage infringement can give rise

[21] *See* 47 U.S.C. § 504(c)(1).

[22] 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.

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

[24] 47 U.S.C. § 230(c)(1); 17 U.S.C. § 512.

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

to liability, but the mere act of distributing a multipurpose product does not – even if the product's maker knows that some infringing uses are certain to occur.[26]

These policy choices have been nothing short of a tremendous success. It is thanks to this legal framework that recent decades have seen an explosion of innovation in digital technologies and Internet-based products and services. Protection from potentially ruinous copyright liability risk has created an innovation environment in which technology providers can focus on developing tools that empower users and companies can grow from small start-ups to household names with unprecedented speed. Society benefits from the current innovation-friendly legal framework in the form of increased opportunities for speech, collaboration, civic engagement, and economic growth.

Protections from liability have been particularly essential in enabling interactive and "user-generated content" sites to flourish. If ISPs, hosts, and websites with no bad intent were instead made potentially liable for content posted by others, they would have no choice but to assume new gatekeeper roles and pare back on functions that empower communication by and among users. Entry barriers for new Internet services (and new competitors to existing services) would increase substantially, the platform's openness to innovation would be reduced, and service providers would be reluctant to host controversial but lawful speech.

In short, policymakers should avoid the myopic approach of departing from current policy principles to impose new, affirmative network-policing obligations on Internet intermediaries.

Requiring ISPs in particular to assume a new network-policing role would also conflict with U.S. foreign policy regarding Internet freedom. As Secretary of State Clinton explained in January, promoting Internet freedom in foreign countries is now a major U.S. foreign policy goal.[27] 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 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."[28]

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 between 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

---

[26] *See MGM Studios Inc. v. Grokster, Ltd.*, 545 U.S. 913 at, e.g., 932-933 ("the [staple article of commerce] doctrine absolves the equivocal conduct of selling an item with substantial lawful as well as unlawful uses, and limits liability to instances of more acute fault than the mere understanding that some of one's products will be misused"), 936 ("Evidence of 'active steps . . . taken to encourage direct infringement,' . . . show an affirmative intent that the product be used to infringe, and . . . overcomes the law's reluctance to find liability when a defendant merely sells a commercial product suitable for some lawful use" (first ellipsis in original) (quoting *Oak Industries, Inc. v. Zenith Electronics Corp.,* 697 F.Supp. 988, 992 (N.D. Ill. 1988))).

[27] 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.

[28] *Id.*

U.S. copyright policy: in both cases, government would be calling on ISPs to police user behavior to prevent certain unlawful communications. As CDT told a Senate subcommittee earlier this year, "we must take care not to set precedents that can be used by authoritarian regimes to justify their own acts of censorship and surveillance."[29]

**3. Rigorous cost-benefit analysis is essential in evaluating new policy proposals for addressing online copyright infringement. There needs to be a sober assessment of both how effective a policy is likely to be in reducing infringement and what collateral impact it may entail.**

Concern about copyright infringement is understandably high. But that does not mean that any and all proposals for reducing infringement are worthy of government endorsement. As in any area of policy, proposals for new anti-infringement measures must be subject to rigorous cost-benefit analysis, asking both how effective a proposed policy is likely to be in reducing infringement and what negative collateral impact it may entail.

Policymakers 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. Thus, careful, independent consideration and balancing of the true costs and benefits of suggested measures is essential. If a particular proposal's reduction in online infringement is likely to be of marginal size or fleeting duration and the proposal would impose significant burdens on (for example) legitimate innovators or online free expression, then the proposal should be rejected.

*Example: Automated Content Filtering by ISPs*

In recent years, major content producers have openly expressed their support for filtering technologies and their interest in seeing ISPs install them.[30] Any government action or policy regarding ISP-level filtering, however, would first need to assess the likely costs and benefits.

On the benefits side, there are strong reasons for skepticism. Policymakers would need to keep in mind that addressing infringement through filtering would almost certainly provoke an ongoing and ultimately futile arms race with infringers. Increased sophistication of filters would be met with increased ingenuity in infringers' efforts to avoid them.[31] 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.

Meanwhile, content filtering at the ISP level would carry significant costs, both to core American values of free expression and privacy, and in terms of the financial and performance burdens associated with filters' installation and operation.

---

[29] 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.

[30] *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.

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

Foremost among the downside risks of ISP-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.[32] Given that people increasingly depend on Internet communications in all aspects of their personal, professional, and civic lives, this has to be a serious consideration. Indeed, 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. And making fair-use determinations is simply impossible to automate.

Mandated use of filters would also come at considerable cost to Internet users' privacy. In order to be comprehensive – a feature filtering proponents often tout – a filtering system must be "always on." 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.[33] 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.[34]

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.[35] 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

---

[32] *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).

[33] *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.

[34] *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.

[35] 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.

degraded network performance significantly, two by more than 75 percent.[36] 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."[37] Furthermore, the investment required to maintain a robust filtering system is likely to increase over time as increases in the amount of Internet traffic will necessitate more and faster filters.

Given the serious questions about the ultimate effectiveness of network-level filters, it is highly doubtful that their benefits would warrant undertaking all of these costs. Over time, moreover, the "arms race" dynamic would make it likely that any benefits would diminish significantly, while costs would rise. Any policy discussion about filtering, therefore, should be clear-eyed in terms of the tenuous mix of costs and benefits.

*Example: DNS blocking*

The domain-name blocking contemplated in the "Combating Online Infringements and Counterfeits Act" (S. 3804, 111th Congress) offers another example. This bill, recently reported out of the Senate Judiciary Committee, would empower the Attorney General to seek court orders forcing domain-name registries and registrars to lock domain names connected to sites "dedicated to infringing activity," or forcing ISPs to filter and block resolution of DNS requests for these domains.

As in the case of automated content filtering, the effectiveness of such an approach would likely prove fleeting at best. DNS blocking is easily circumvented. First, third-party public DNS servers are widely available, and if blocking is implemented domestically, more would inevitably spring up outside the United States to avoid being subject to blocking orders. For Internet users, pointing DNS requests to these unfiltered servers would be simply a matter of updating a single parameter in their operating systems' Internet settings. Users who want to engage in infringement will thus easily be able to route their traffic around DNS providers that enforce the blacklist. Second, users could enter IP addresses manually into their browsers and bookmark those addresses, bypassing the DNS system entirely. Third, since most operating systems come with DNS server functionality built in, users could set up local DNS servers on their own computers, thus avoiding any DNS servers that have been ordered to block. Fourth, operators of blacklisted websites could distribute a small browser plug-in or other piece of software to allow users to retrieve the IP addresses of the operators' servers. Any combination of these circumvention techniques would dramatically limit DNS blocking's effect on online copyright infringement.

The negative consequences of DNS blocking, meanwhile, appear substantial. It would threaten online free expression, primarily because it would inevitably block some lawful speech in addition to targeted infringing material. Single domains can "house" thousands of distinct pages at the subdomain level. A domain registry or registrar taking blocking action against a domain would necessarily affect all subdomains – even non-infringing sites unaffiliated with the infringing site that gave rise to the blocking order.[38] The First Amendment requires that an order

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

[37] 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.

[38] *See*, e.g. *CDT v. Pappert*, 337 F.Supp.2d 606 (E.D. Penn. 2004) at 640 (citing evidence that DNS blocking led to the blocking of hundreds of thousands of innocent web pages).

against speech "be precise and narrowly tailored to achieve the pin-pointed objective of the needs of the case."[39] The only way to avoid overblocking when blocking domain names is if the *only* content associated with a particular name is 100% infringing, but in reality this is almost never the case.

DNS blocking as a means for combating copyright infringement would very likely also lead to cybersecurity problems. First, ordering ISPs not to resolve certain DNS requests is incompatible with DNSSEC, the security extensions to the DNS ten years in the making, which ISPs are just beginning to deploy.[40] Second, as discussed above, users seeking to circumvent such blocking can easily switch to third-party DNS providers. But by creating strong incentives for users to rely on potentially untrustworthy DNS providers, DNS blocking will create a new and very dangerous opportunity for security risks and crime online. Once a DNS server set up to facilitate the circumvention of blocking orders has a large base of regular users, the operator may well be tempted to take advantage of that traffic. It would be easy for that operator to, for example, re-route requests for banking websites not to the requested sites but to phishing sites set up specifically to steal unsuspecting users' personal information in order to gain access to financial accounts or perpetrate other fraud. Though they may be unaware of it, users place an enormous amount of trust in their DNS provider to route requests to the proper sites. ISPs have incentive to maintain that trust, but other DNS operators – especially those with an interest in evading the blocking of sites dedicated to commercial infringement – will likely not share that same incentive.

In short, DNS blocking carries risks to free expression and the security and reliability of the Internet. Given the ease with which the tactic can be circumvented by parties seeking to offer or access the targeted sites, the impact on speech and security would likely stand as the main lasting impact of a policy focused on DNS blocking.

**4. There may be opportunities for progress through voluntary, collaborative approaches that do not involve government mandates. Such approaches must, however, be developed in a manner that ensures that consumer and innovation interests are strongly represented and protected.**

There may be opportunities for progress in reducing copyright infringement through voluntary, collaborative efforts between copyright holders and other parties in the Internet ecosystem. Voluntary efforts carry less risk to innovation, because by definition they do not burden innovators with one-size-fits-all mandates that might prove too costly, awkward to implement, or simply effective in some contexts. To the extent that they are truly voluntary, rather than the product of government demands or pressure, such private sector efforts also avoid the constitutional questions (for example, due process, or inadvertent impact on lawful speech) that can arise when government action is involved. On the other hand, private deals by entities providing Internet services or online platforms can still have a substantial impact on their users. The lack of government involvement makes it all the more important that private parties working out voluntary arrangements take affirmative steps to ensure that the consumer and innovation interests of users are represented and protected as collaborative approaches are developed.

[39] Tory v. Cochran, 544 U.S. 734, 736 (2005) (internal quotes omitted).

[40] *See* Brenden Kuerbis, "COICA Amended, still threatens Internet security," Internet Governance Project Blog, October 6, 2010, http://blog.internetgovernance.org/blog/_archives/2010/10/6/4648186.html.

For example, many user-generated content sites have developed content-filtering tools to address uploads of copyrighted material.[41] From a user perspective, it is important that such filtering tools leave room for fair use, operate transparently, and allow users the opportunity to object if they believe a filter has wrongly blocked a lawful posting. Interestingly, some voluntary filters help minimize the impact on users by encouraging revenue-sharing partnerships between user-generated content sites and rightsholders as an alternative to blocking unauthorized postings.[42] This approach offers the promise of moving beyond content blocking and legal battles to focus instead on building new markets. *Mandating* filtering tools would likely stifle the development of such innovative licensing arrangements.

As another example, 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.[43] 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.[44]

Any attempt to move beyond warning notices to actual ISP-imposed sanctions, however – an idea often referred to as "three strikes" or "graduated response" – would implicate user interests in a much more fundamental way. The Internet has become essential for many aspects of personal, professional, and civic life. Disabling or restricting subscribers' Internet access, even in a temporary or limited way, can have significant consequences. Any such sanctions would need to take great care in ensuring due process for subscribers, including the opportunities to answer allegations and to appeal or otherwise take some recourse in case sanctions are applied wrongfully. In addition, the process would need to include consideration of such factors as potential hardship, unintentional violations, and impact on innocent members of an affected household. Finally, there would be substantial questions about proportionality; permanent termination, for example, generally would be difficult to justify.

In negotiating voluntary, cooperative agreements, therefore, private sector parties need to be sensitive a range of public interests beyond just those of the copyright holders and Internet or online service providers in question. This can best be accomplished by seeking input and participation from persons or groups focused on representing those interests before any final deal is cut.

### 5. Policy in this area should set a realistic goal: making participation in widespread infringement relatively unattractive and risky, compared to participating in lawful markets.

Eliminating copyright infringement completely is an impossible task. The goal of policy needs to be more realistic: not to prevent infringement entirely, but rather to make it relatively

---

[41] *See, e.g.*, YouTube's Content ID System, http://www.youtube.com/t/contentid.

[42] In August 2008, YouTube reported that rightsholders chose to allow their content to be uploaded, sharing in ad revenue, 90 percent of the time. *See* Brian Stelter, "Some Media Companies Choose to Profit From Pirated YouTube Clips," *New York Times*, August 15, 2008, http://www.nytimes.com/2008/08/16/technology/16tube.html?_r=1

[43] *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.

[44] 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.

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. The goal of making infringement less attractive and less common is echoed in the 2008 PRO IP Act, which characterizes the objective of the Federal Government's Joint Strategic Plan against counterfeiting and infringement as "[r]educing" infringing goods in the supply chain, not eliminating them.[45]

Efforts to pursue a more ambitious goal – such as complete or near-complete elimination of large-scale infringement – would risk taking the copyright policy in a harmful direction for innovation. 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 policy initiatives in this area need not and should not target 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, copyright enforcement efforts should focus on deterring and punishing the illegal *use* of digital technologies and services.

In that context, it is important to recognize that Congress has already created 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.[46]
- 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 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.

[45] Prioritizing Resources and Organization for Intellectual Property (PRO IP) Act of 2008, Pub. L. No. 110-403 (20008) § 303(a)(1).
[46] *MGM Studios, Inc. v. Grokster, Ltd.,* 545 U.S. 913 (2005).

- Criminal sanctions are available, under 17 U.S.C. § 506(a), for any willful infringement committed for commercial advantage or financial gain. Even where the motive is not financial, willful infringement is criminal so long as the infringed works have a total retail value over $1,000.
- 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 2008 PRO IP Act, in addition to creating the Intellectual Property Enforcement Coordinator 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. Since eliminating infringement entirely is an impossible goal, 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 for innovation and legitimate commerce. Policymakers aiming to improve copyright enforcement should look first to existing legal tools.

Importantly, however, the goal of making infringement less attractive compared to legal alternatives cannot be achieved by enforcement efforts alone. It also requires that copyright industries provide legal offerings that are compelling and convenient. Where government can promote the deployment of compelling legal offerings – for example, by streamlining existing statutes pertaining to music licensing – it should move aggressively to do so. And finally, as discussed in the next section, policymakers should look for opportunities to improve the public's understanding regarding the obligations of copyright law and the consequences of violating them.

**6. Public education remains an important component of policy in this area. Digital technologies will continue to put powerful tools in the hands of consumers, but consumers need to understand that using them to infringe copyright is illegal and wrong.**

Public education remains an important and underappreciated component of policy in this area. Modern information technology is here to stay and will continue to put powerful digital tools in the hands of the public. Inevitably, public attitudes and norms will play a major role in shaping how people choose to use the information-age tools at their disposal, including the extent to which they seek to engage in infringement.

Public education is needed, therefore, to help shape consumer expectations and norms concerning the use of copyrighted works in a digital world. Copyright law can be a technical area, and consumers' initial assumptions about what is and is not permitted are often not fully accurate. Education about copyright infringement and its potential legal consequences also can help increase the deterrent effect that the legal framework and enforcement campaigns have on the general population.

In the absence of effective education to help the public better understand its rights and responsibilities in the copyright realm, evolving technological capabilities may create their own "facts on the ground" with little regard for law or policy. For reasons discussed in the previous sections, trying to contain infringement by restricting the development of new technological capabilities would carry heavy costs to innovation and free expression; such a strategy requires hobbling the very technologies that are central to the information economy. By contrast, trying to help shape the public's understanding of what are and are not appropriate *uses* of new technologies would pose no risk to innovation.

Influencing public norms around copyright may not be easy or quick. But if the goal is to have a long-term impact on the scope of the infringement problem without depressing innovation, policymakers should make public education a key part of the discussion.

* * *

CDT appreciates the opportunity to comment on this crucial set of issues. We are available for further discussion on the intersection between copyright policy and Internet innovation as the Internet Policy Task Force continues its analysis and moves towards preparing its report.

Respectfully submitted,

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