MAJOR COURT DECISIONS, 2007

ACLU V. Gonzales, No. 98-5591, 2007 U.S. Dist. LEXIS 20008 (E.D. Pa. Mar. 22, 2007)

Issue: (1) Whether the Child Online Protection Act, 47 U.S.C. § 231 (2000), ("COPA") is constitutional and (2) whether this court should issue a permanent injunction against its enforcement due to its alleged constitutional infirmities?

Holding: (1) COPA is unconstitutional because it facially violates the First and Fifth Amendment rights of the plaintiffs, therefore, (2) a permanent injunction should be issued against the enforcement of COPA.

History: The first attempt by Congress to protect children from harmful material on the Web was the Communications Decency Act of 1996, 47 U.S.C. § 223 (2000) ("CDA"). The CDA was held unconstitutional by the Supreme Court because it was not narrowly tailored to serve a compelling state interest and because less restrictive alternatives were available. *See Ashcroft v. ACLU*, 542 U.S. 656, 661 (2004) (discussing *Reno v. ACLU*, 521 U.S. 844 (1997)).

The second attempt by Congress "to protect minors from exposure to sexually explicit materials on the Web deemed harmful to them" was COPA. COPA was signed into law October 21, 1998 to fix the deficiencies in the CDA. Within one day of its execution, however, the plaintiffs, a variety of Web site providers, filed a suit against the Attorney General of the United States seeking injunctive relief from the enforcement of COPA. This District Court granted the plaintiff's motion for a temporary restraining order and eventually granted the plaintiffs' motion for a preliminary injunction on February 1, 1999. *ACLU v. Reno*, 31 F. Supp.2d 473 (E.D. Pa. 1999). The government appealed this decision but it was affirmed by the Third Circuit Court of Appeals but on different grounds. *ACLU v. Reno*, 217 F.3d 162, 166 (3d Cir. 2000). The Court of Appeals found that the "community standards" language in the statute made it unconstitutionally overbroad. *Id.* at 166. The Supreme Court granted certiorari and reversed but only based on the limited finding that that particular language was not overbroad. *Ashcroft v. ACLU*, 535 U.S. 564, 585 (2002). The Court remanded to the Court of Appeals to determine whether the District Court was correct in granting the preliminary injunction. The Court of Appeals affirmed the District Court. *ACLU v. Ashcroft*, 322 F.3d 240 (3d Cir. 2003). The Court of Appeals agreed that the statute was overbroad, did not serve a compelling interest and was not the least restrictive means available to serve its purpose. *Id.* at 266-71. Once again the government sought review and the Supreme Court granted it. 540 U.S. 944 (2003). Finally on June 29, 2004, the Supreme Court affirmed the District Court's decision to

grant the preliminary injunction. The Court remanded the case to the District Court for a trial on the merits. Because of the many changes since Much had changed since the passage of COPA, so the Court directed the District Court to update the factual record to reflect upon any technological changes, note possible changes in the legal scope, and to determine the effectiveness of Internet content filters ("filters"). *Ashcroft*, 542 U.S. at 671-73.

Discussion: COPA imposes criminal and civil penalties that punish anyone who knowingly "by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors." 47 U.S.C. § 231(a)(1). COPA only applies to files that are publicly accessible over the Web via HTTP or a successor protocol, but does not protect harmful material transferred through email, newsgroups, chat, or peer-to-peer. COPA allows affirmative defenses against liability for a defendant who in good faith restricted access to minors. Ways to restrict access to minors include the requirement of a credit card, adult access code, digital certificate, or any other reasonable measures that verify age. 47 U.S.C. § 231(c)(1). Essentially, COPA tries to put sexually explicit images "behind the counter" by requiring the commercial pornographer to verify age before pornography is made available.

The plaintiffs in the case represent a wide array of individuals and entities who post sexual content on their Web sites. The content includes information about sexual health, safe sex, literary and artistic depictions of sex, and resources for homosexuals. Many of the Web sites involve interactive exchanges through chat rooms, discussion groups, and bulletin boards; all of which may contain language or images pertaining to sexually explicit conduct. Of the Web sites included, the majority of them provides free information and does not currently require a password, log-in, or any personal identifiable information to access the material.

The thrust of the plaintiffs' claim is that less restrictive means than COPA are available. Therefore, most of the opinion focused on the availability, effectiveness, and ease of filters. Filters block categories of material on the Internet and can prevent children from seeing unsuitable material. Filters are flexible and can be set up according to the age and maturity of the child, by specific words, Web site addresses, time of day, or day of the week. Filter software can be purchased or downloaded online however there are many that are offered for free. Filters can be used to block any Internet application for HTTP and other Internet applications like email, chat, peer-to-peer file sharing, and audio and video files. Furthermore, they block content regardless of the geographic origin of a Web page and apply to both non-commercial and commercial Web pages. Overall, filters are difficult for children to circumvent and block about 95% of sexually explicit material on the Web.

COPA does not rely on the use of filters; rather it puts the onus on Web site providers to prevent children from accessing specified material. COPA provides for an affirmative defense which requires the use of age verification technologies. With respect to the ease and availability of age verification technologies, the court found that no product accurately verifies age online. Credit and debit cards are prohibited uses of age verification since the Internet is faceless, and minors can obtain cards with the consent of their parents. Data verification services ("DVS") that assess the age of the individual based on public records like voting, property, and vehicle registration are easily circumvented by children who know the name, address, and zip codes of their parents. Not only is age verification an ineffective way to prevent children from accessing the information, but it hinders adults from lawfully accessing the same information. For example, DVS is slow to keep up with name changes, identifying residents outside of the United States, recent immigrants, and young adults who do not have much verifiable information. Another problem with DVS is the associated fees. Any adult who wishes to access a site, whether or not they want to purchase material, will be charged a fee to verify their age. If the Web site consumes the costs, it will face costs between $14,800,000 to $38,000,000 per year. Additionally, the requirement of personal identification or credit card information will take the anonymity out of online browsing and will in effect chill free speech for users who want to browse privately.

In addition to problems with the age verification element provided for in COPA's affirmative defense section, COPA is problematic in other ways as well. The court found COPA to be vague because of terms like "commercial purposes," "any person under 17 years of age," and "as a whole" create uncertainty. Although Congress only intended for COPA to apply to commercial pornographers, many of the plaintiffs in the case are not commercial pornographers yet still may face prosecution under the statute. The court found a lack of clarification in the terms will lead to a chilling effect on free speech because Web providers are wary as to what they are immune from. COPA is overbroad because the terms "communication for commercial purposes" and "engaged in business" restrict more than the statute intended. Congress only meant to regulate Web publishers who seek a profit; however, the broad language allows Web publishers who receive revenue indirectly through advertising or other means to fear prosecution as well. The broad definitions also make COPA overinclusive because its language prohibits more speech than necessary to serve Congress' interest. In addition to regulating more than just commercial pornographers, the language also regulates speech that is obscene to all minors instead of just to older minors. Lastly, COPA is underinclusive because it does not apply extra-territorially to a large portion of harmful material from overseas; rather COPA only applies to material in the United States "that is accessible over the Internet using HTTP or a successor protocol."

However, much of the harmful material that children access comes from sources like email, chat rooms, and peer-to-peer programs.

Above all, the defendant failed to meet his burden of proof that COPA is narrowly tailored to a compelling interest and that no less restrictive means are available. The defendant offered no proof that COPA will be effective, especially since it will not reach most of the foreign material. The abundance of proof pertaining to filters leads this court to hold that indeed filters are a less restrictive alternative to COPA. Filters do not impose fines or prison sentences, they apply to private or public uses, they can be encouraged by Congress in schools and training programs, and they cover formats other than just HTTP. As a result of the aforementioned conclusions of law, the court held that "COPA facially violates the First and Fifth Amendment rights of the plaintiffs."

Summarized by Megan Green

Twentieth Century Fox Film Corp. v. Cablevision Systems Corp., 2007 WL 867093 (S.D.N.Y. Mar. 22, 2007)

Issue: Whether Cablevision is "copying" plaintiffs' copyrighted programming or otherwise violating plaintiffs' rights under the Copyright Act of 1976, as amended, (the "Copyright Act"), 17 U.S.C. § 101, by introducing a new Remote-Storage DVR System ("RS-DVR") which would permit Cablevision customers to record programs on central servers at Cablevision's facilities and play the programs back for viewing at home.

Holding: The U.S. District Court for the Southern District of New York held that the operation of the proposed RS-DVR would "copy" plaintiffs' programming in two ways: (1) Cablevision makes unauthorized copies of plaintiffs' programming, in violation of plaintiff's right to reproduce their work; and (2) Cablevision makes unauthorized transmissions of plaintiff's programming, in violation of plaintiff's exclusive right to publicly perform their work.

The court found that Cablevision makes multiple unauthorized copies of programming in two respects: (1) a complete copy of a program selected for recording is stored indefinitely on the customer's allotted hard drive space on the Arroyo server, the server that programming is recorded and stored on for later playback, at Cablevision's facility; and (2) portions of programming are stored temporarily in buffer memory on Cablevision's servers.

Based on the court's conclusion that Cablevision, through its operation of the RS-DVR, would "copy" plaintiffs' programming both in the Arroyo servers and in buffer memory, in violation of plaintiff's exclusive right of reproduction under the Copyright Act, summary judgment was granted in favor of the plaintiffs, and Cablevision is enjoined from copying plaintiffs' copyrighted works, unless it obtains a license to do so.

Discussion: In these related cases, plaintiffs sued Cablevision and its parent, CSC Holdings, Inc. ("CSC"), for copyright infringement, seeking a

declaratory judgment that Cablevision's RS-DVR would violate their copyrights and an injunction enjoining defendants from rolling out the RS-DVR without copyright licenses. Defendants counterclaimed for a declaratory judgment holding that the RS-DVR would not infringe on plaintiffs' copyrights, and the parties' cross-motioned for summary judgment.

Under the Copyright Act, a plaintiff must establish (1) ownership of a valid copyright and (2) unauthorized copying or a violation of one of the other exclusive rights afforded copyright owners pursuant to the Copyright Act, to claim a copyright infringement. In this case, it was undisputed that plaintiffs were the valid owners of the television programming at issue. Therefore the only issues before the court was whether Cablevision was "copying" plaintiff's copyrighted programming in violation of the Copyright Act by implementing the RS-DVR technology.

A key question in determining the answer to this issue was "who makes the copies?" Cablevision sees itself as entirely passive in the RS-DVR's recording process; rather Cablevision contends that it is the customer that is doing the copying. The court disagreed with this argument for several reasons. The RS-DVR is a complex system that involves an ongoing relationship between Cablevision and its customers, payment of additional monthly fees by the customers to Cablevision would be required, ownership of the equipment remained with Cablevision (opposed to a stand-alone machine that sits on the top of a television), the use of numerous computers and other equipment located in Cablevision's private facilities was necessary for the RS-DVR to operate, and ongoing maintenance of the system required Cablevision personnel.

In addition, the RS-DVR's architecture and delivery method is most synonymous with Video-On-Demand ("VOD"), a service that Cablevision provides pursuant to licenses negotiated with programming owners. Like VOD technology, Cablevision decides which programming channels they want to make available for recording on the RS-DVR system, and the programming that they do make available for viewing is stored outside the customer's home at Cablevision's private facilities.

Thus, a reasonable factfinder could conclude that the copying of programming to the RS-DVR's Arroyo servers would be done not by the customer, but by Cablevision, albeit at the customer's request. This copying would, as a matter of law, constitute copyright infringement.

The Defendants went on to deny that the portions of programming temporarily stored in buffer memory during the RS-DVR's operation are "copies" for the purposes of the Copyright Act because the buffer copies are "not fixed" and are "otherwise de minimis," terms essential to the Copyright Act's definition of "copy." 17 U.S.C. § 101 (2000). However, the Copyright Act provides that a work is "fixed" if it is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration." In this case, portions of programming residing in buffer memory are used to make perma-

nent copies of entire programs on the Arroyo servers. Furthermore, numerous courts have held that the transmission of information through a computer's random access memory, as is the case with the buffering here, creates a "copy" for purposes of the Copyright Act. As a result, defendants were found to "copy" plaintiffs' programming in both the Arroyo servers and in buffer memory.

The final issue was whether or not the proposed RS-DVR would "copy" plaintiffs' programming when Cablevision makes unauthorized transmissions of plaintiff's programming, in violation of plaintiff's exclusive right to publicly perform their work. To "perform" a work, as defined by the Copyright Act, is "to recite, render, play, dance, or act it, either directly or by means of any device or process or, in the case of a motion picture or other audiovisual work, to show its images in any sequence or to make the sounds accompany it audible." 17 U.S.C. § 101. Cablevision again suggested that it was passive in this process, and that it was the customer that was "doing" the performing. Again, the court rejected this argument for the same reasons that they rejected the argument that the customer is "doing" the copying involved in the RS-DVR. The court held that Cablevision actively participates in the playback process, and that Cablevision would be engaging in public performance of plaintiff's copyrighted works in operating its proposed RS-DVR service, thereby infringing upon plaintiffs' exclusive rights under the Copyright Act.

Cablevision is permanently enjoined, in connection with its proposed RS-DVR system, from (1) copying plaintiff's copyrighted works and (2) engaging in public performance of plaintiffs' copyrighted works, unless it obtains licenses to do so.

Summary by Rebecca Magnone