SUMMARY AND HIGHLIGHTS OF THE PHILADELPHIA FEDERAL DISTRICT COURT'S DECISION IN

CENTER FOR DEMOCRACY & TECHNOLOGY V. PAPPERT
Case No. 03-5051 (E.D. Pa. Sept. 10 2004)

CENTER FOR DEMOCRACY & TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

On September 10, 2004, Judge Jan DuBois of the United States District Court for the Eastern District of Pennsylvania invalidated Pennsylvania's "Internet Child Pornography" law, finding that the law has blocked access to more than one million wholly innocent web sites, while having little if any effect on the few hundred child pornography sites that were targeted under the law. In one instance described by Judge DuBois, access to the web site of a rural Pennsylvania community recreation center was blocked as a result of an order issued to an Internet Service Provider (ISP) by the Pennsylvania Attorney General. Although targeted at a single child pornography site, the order resulted in the blocking of more than ten thousand innocent web sites.

The court decision came in a constitutional challenge filed in September 2003 by the Center for Democracy & Technology, the ACLU of Pennsylvania, and Plantagenet, Inc., a Pennsylvania ISP. The challenge argued that the Pennsylvania law was a prior restraint on speech that violates the First and Fourteenth Amendments and the Commerce Clause of the Constitution.

The challenged statute had authorized the state Attorney General or any county district attorney to apply unilaterally to a local judge for an order declaring that certain Internet content may be child pornography, and requiring any ISP serving Pennsylvania citizens to block the content. As Judge DuBois found, because of the technical design of the Internet, most ISPs can only comply with the blocking orders by also blocking a significant amount of wholly innocent web site content as well. Also, the court ruled, the statute violated the First Amendment's protection against prior restraints, since the court proceeding in response to the government's request occurred with no prior notice to the ISP or the web site owner.

The following are highlights of the court's decision striking down the law:

KEY FACTUAL FINDINGS:

- Over a 16-month period leading up to the lawsuit, Pennsylvania issued approximately 500 blocking orders targeting fewer than 400 alleged child pornography web sites. These orders led to the blocking of more than 1 million innocent web sites.
- Many ISPs complied with the blocking orders by using "IP filtering" to block access to the numeric "Internet Protocol" address of the targeted web site. In light of technical, economic, administrative, and legal considerations, the court concluded that it was reasonable for ISPs to use IP filtering.
- However, all web sites that are hosted on the same "web server" usually share the same IP address. Thus, if a child pornography web site happens to be operated on a

web server that also operates unrelated, innocent web sites, all of the web sites on the server would be blocked by IP filtering.

- Based on expert testimony presented by the Plaintiffs, the court found that more than 50% of all web sites share their IP addresses with at least 50 other web sites. In one example noted by the court, the IP address of a child pornography site was shared by hundreds of thousands of other web sites, all of which were blocked under the Pennsylvania law. Thus, there is a high risk that blocking by IP address will lead to the blocking of innocent web sites.
- Some ISPs used "DNS filtering" to comply with the blocking orders, whereby they changed entries in a "domain name system" database to interfere with requests for targeted web sites (designated by its domain name). The court found that this approach was less effective than IP filtering (and thus exposed the ISP to greater criminal risk). Moreover, the court found that even using the DNS filtering method resulted in the blocking of innocent web sites.
- As a result of the blocking orders challenged in the case, the court found that at least 1,190,000 non-targeted web sites were blocked. That figure did not include hundreds of thousands of web sites on the "terra.es" online community that the court found were blocked as a result of a challenged blocking order.
- A World Wide Web address (or URL) only refers to a location where content can be found, and does not refer to any particular piece of static content. Thus, blocking access to a particular URL effectively blocks access to whatever new or different content might appear at the URL in the future.
- Although the blocking orders interfered with more than a million innocent web sites, the court found very little evidence that the challenged Pennsylvania law furthered the legitimate fight against child abuse. The court concluded that child pornography web sites – and people seeking to access such web sites – could easily circumvent the blocks placed by the ISPs in response to the Pennsylvania statute.
- The impact of the Pennsylvania law reached far outside of Pennsylvania, and interfered with non-Pennsylvanians' access to lawful web sites located outside of Pennsylvania. In some cases, the blocking orders affected Internet communications wholly outside of the United States.

KEY LEGAL HOLDINGS:

- Applying Supreme Court precedent, the court concluded that Pennsylvania was constitutionally responsible for the blocking of innocent web sites even thought it was private ISPs that implemented the blocks. Pennsylvania was responsible for the consequences that flowed from the statute and the blocking orders it issued to ISPs.
- The court concluded that it did not need to decide whether "strict" or "intermediate" scrutiny applied under the First Amendment because the challenged law failed the more lenient intermediate scrutiny test. Under both strict and intermediate scrutiny, the government must demonstrate that the challenged law in fact furthers the goal of fighting child pornography. The court concluded that in this case Pennsylvania "has

not produced any evidence that the implementation of the Act has reduced child exploitation or abuse."

- Because the challenged law did not provide for prior notice to the affected web sites or the opportunity for an adversarial hearing before a web site is blocked, the blocked orders were an unconstitutional prior restraint under the First Amendment.
- The challenged law is also an unconstitutional prior restraint because it prevents future content to be displayed at a particular URL (such as http://www.example.com) based on the fact that the URL previously displayed illegal content. The court applied Supreme Court cases involving newspapers and movie theaters to conclude that a state cannot ban future speech on a particular Internet URL.
- The fact that the challenged law's intent was to target *child* pornography does not mean that fewer or weaker First Amendment protections apply when the statute results in the censorship of legal, non-pornographic content.
- The "informal" notice system used by the Pennsylvania Attorney General (which bypassed even the inadequate procedures found in the challenged law) also was an unconstitutional prior restraint. The blocking orders sent by the Attorney General to ISPs were coercive and threatening, and the ISPs were not realistically free to ignore them.
- Because the challenged law impacts speech that is wholly outside of Pennsylvania, and because any in-state benefit of the law is greatly outweighed by the harm to out-of-state speech on the Internet, the law violates the Commerce Clause of the U.S. Constitution.

Additional background and the important litigation documents (including the parties' expert witness reports) are available at http://www.cdt.org/speech/pennwebblock/. The court's decision itself is available at http://www.cdt.org/speech/pennwebblock/20040910memorandum.pdf.

For more information, contact John Morris or Lara Flint at (202) 637-9800.