# TELECOMMUNICATIONS

## KILLING THE MESSENGER:
## PENNSYLVANIA'S NEW CHILD PORNOGRAPHY STATUTE IS AIMED AT THE WRONG PARTIES

*BY ANDREW G. MCBRIDE & KATHRYN L. COMERFORD**

The "network of networks" that is the Internet has proven an incredibly powerful medium for the organization and dissemination of vast amounts of information in a wide variety of formats. For many users, the Internet is library, theatre, mall, newspaper, and workplace all rolled into one. As the Supreme Court has recognized, "[i]t is no exaggeration to conclude that the content on the Internet is as diverse as human thought."[1] The dark side of this diversity is the use of the Internet to disseminate harmful and illegal material, such as child pornography. On February 21, 2002, the Commonwealth of Pennsylvania enacted a new section 7330 of the state criminal code, which requires an Internet service provider ("ISP"), upon five days' notice, to remove or disable access to content determined by the state officials to constitute "child pornography items."

Although the goal of eradicating child pornography is unquestionably a laudable one, the means Pennsylvania has chosen to pursue this goal conflict with provisions of the federal Communications Act, and are of dubious constitutionality. In this situation, the medium is not the message, and ISPs should not be forced to police content on the Internet in a manner that will suppress legitimate speech and constitute Pennsylvania as the nationwide arbiter of appropriate Internet content.

**The New "Internet Child Pornography" Law.** Pennsylvania's new Internet child pornography law is unprecedented in scope. At its core, the new statute provides:

> An Internet Service Provider shall remove or disable access to child pornography items residing on or accessible through its service in a manner accessible to persons located within this Commonwealth within five business days of when the Internet Service Provider is notified by the Attorney General . . . that child pornography items reside on or are accessible through its service.[2]

The law requires only an *ex parte* showing that information available on the Internet "constitute[s] probable cause evidence" of a violation of Pennsylvania's child pornography laws.[3] The statue provides for a series of graduated criminal penalties for ISPs that fail to block Internet content designated under the law, including felony treatment for a third offense.[4] As discussed below, a survey of the new law's key provisions demonstrates that it suffers a host of flaws that render its enforcement highly problematic under federal law and the Federal Constitution.

Section 7330 defines "Internet Service Provider" broadly to include any "person who provides a service that enables users to access content, information, electronic mail or other services offered over the Internet."[5] This definition reaches not only traditional commercial Internet access services (such as AOL or Verizon.net) but could easily extend to any physical location that provides Internet service, such as coffee shops, hotels, and non-profit entities, including universities and public libraries. Under the new Pennsylvania law, any of these businesses or organizations could be required to alter its services to preclude access to material that *might* violate Pennsylvania's child pornography law.

Even as applied to traditional commercial ISPs, the duties imposed by the Pennsylvania law are breathtaking. An ISP "must remove or disable the [alleged child pornography] items *residing on or accessible through* its services," *id*. at § 7330(g)(3)(iii) (emphasis added). This means the ISP is not only responsible for content it creates, or even content that its users create through web pages that are hosted on the ISP's own servers. Rather, the statute purports to require the ISP to disable or remove content "accessible through" its services, which includes every information storage device connected to the Internet. This is rather like making the Librarian of Congress responsible for the content of every copy of every book registered with that depository, wherever the copy is actually located.

Nor does Pennsylvania's new law contain any geographic limits on its reach. The only required geographic nexus to Pennsylvania is the requirement that the ISP make the items inaccessible to users located within the Commonwealth. Thus, under the new law, Pennsylvania could require a library located in Texas to disable its web page's search engine if that search engine would enable a Pennsylvania resident to access alleged child pornography created and uploaded to the Internet in Nebraska. Presumably, the law applies to content from other countries as well. Because ISPs do not possess the technology necessary to identify and selectively block content to Internet users located only in Pennsylvania, what Pennsylvania law enforcement officials ban under this law is banned nationwide (and perhaps even worldwide). With the emergence of wireless access to the Internet through readily portable devices, isolating "Pennsylvania Internet users" is impossible under current technology.

Finally, there is no mechanism for the Pennsylvania Attorney General to review and update the order based on the ever-changing landscape of the Internet. Thus, despite expressly disclaiming that Section 7330 "impos[es] a duty on an Internet Service provider to actively monitor its service or affirmatively seek evidence of illegal activity,"[6] it apparently places the onus on the ISP to determine whether a particular user or website has altered its content sufficiently that its dissemination would not violate a pre-existing notice under Section 7330. ISPs must thus become expert in identifying child pornography, with mistakes punishable by criminal sanctions.

**Federal Immunity and Preemption.** As part of the Telecommunications Act of 1996, Congress enacted Section 230 of the Communications Act. Section 230 grew out of a concern over individual states

holding ISPs liable for content created by others. Specifically, Section 230 broadly states that "[n]o provider or user of interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[7] Because enforcement of Pennsylvania's new law would, in effect, treat ISPs as publishers by holding them responsible for content created by others, it runs headlong into the federal immunity created by Section 230.

Numerous federal courts have held that Section 230 bars civil suits even where the plaintiff has previously notified the Internet service provider that allegedly unlawful content was stored or accessible through its service.[8] As the Fourth Circuit explained in the seminal opinion interpreting Section 230, as soon as an ISP receives notice of the allegedly unlawful content available on its service, "it is thrust into the role of a traditional publisher."[9] At this point, the ISP is in the same position as a publishing house that receives a threat of a libel or infringement suit based on the content created by one of its authors. This is exactly the situation that the federal immunity is meant to prevent. As the Fourth Circuit has put it, "[e]ach notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's [unlawful] character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information," which "would create an impossible burden in the Internet context."[10] The Pennsylvania law imposes exactly the kind of burden that Congress meant to eliminate in Section 230—ISPs are forced to police content created by the tens of millions of Internet users who can disseminate content directly or indirectly through their service.

While the broad immunity provided by Section 230 cannot be "construed to impair enforcement of . . . *Federal* criminal statute[s]," [11] there is no corresponding exception for state criminal laws. Indeed, Section 230 expressly references the federal child pornography laws, raising the inference that similar state laws are otherwise covered by Section 230's immunity provision unless expressly exempted. Federal courts have concluded that civil actions based upon the violation of state criminal laws, including state pornography laws, can be barred by the immunity created by Section 230.[12] Because Section 7330 treats ISPs as publishers of material and creates criminal liability on that basis, its enforcement is barred by the federal immunity created by Section 230.

Section 230 also contains an express preemption provision. That provision directs that "[n]o cause of action may be brought *and no liability may be imposed* under any State or local law that is inconsistent with [Section 230]."[13] Section 230 provides not only for immunity from republication liability, it also protects an ISP's voluntary decision to block (or to decline to block) access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable content." In these so-called "good Samaritan" provisions, Congress sought to place the decision whether to block content created by others in the hands of ISPs, to the exclusion of state or federal authorities. The goal of Section 230 is to create an environment where ISPs "self-regulate the dissemination of offensive material over their services."[14] Because the new Pennsylvania law supplants self-regulation in favor regulation by law enforcement authorities under penalty of criminal sanction, it is inconsistent with and frustrates the purpose of the federal law. [15]

**Constitutional Concerns.** In addition to raising serious questions under Section 230, Pennsylvania's new Internet child pornography law presents numerous constitutional problems, including concerns under the First Amendment and the Commerce Clause.

**The First Amendment.** Although child pornography is not protected speech,[16] the vast majority of content on the Internet is protected under the First Amendment. If access to the two—protected and unprotected speech—could be easily separated, there might be little cause for First Amendment alarm. Because they cannot be, enforcement of Pennsylvania's Section 7330 risks restricting access to protected speech and thus raises a serious threat of substantial overbreadth. This is particularly so where an *ex parte* showing of probable cause results in what appears to be a permanent ban of designated content from the Internet.[17] As the Supreme Court has explained, the probable cause standard is significantly lower than a preponderance of the evidence, and is best characterized as facts creating some probability that a proposition is true.[18] While temporary intrusions on liberty, such as search warrants or wiretaps might be based upon such a standard, Section 230 permanently bans content from the Internet based only upon this showing.

In addition, the new Pennsylvania statute ignores the reality that content stored at a single Uniform Resource Locator ("URL") or web address may be accessible through literally thousands of Internet avenues, including myriad search engines, newsgroups, electronic mail systems, and chat groups, that provide access to protected as well as unprotected speech. As the Supreme Court has noted, "these tools constitute a unique medium . . . located in no particular geographic location but available to anyone, anywhere in the world, with access to the Internet."[19] Furthermore, the "methods [of Internet retrieval] are constantly evolving and difficult to categorize precisely."[20] Because there is no simple way for an ISP to navigate through this labyrinth and isolate a single avenue to alleged unlawful content,[21] an ISP faced with a Pennsylvania order to cut off access to particular child pornography items will most likely be forced to shut down numerous avenues, which lead to protected as well as unprotected speech destinations.[22] Accordingly, although Pennsylvania's goal may be to "aim specifically at evils within the allowable area of government control," the means it chose to reach that goal—requiring an ISP to disable access to items beyond the ISP's control—is overbroad.[23]

Likewise, the statute shows no awareness on the part of Pennsylvania's legislators that a single URL address can contain numerous items, produced by independent authors, only one of which may be unprotected child pornography. This reality makes it difficult if not impossible for ISPs to comply with Section 7330 orders without the substantial risk of cutting off access to or removing protected speech. Although the underlying child pornography items created by individuals unconnected to the ISPs may provide a "core of easily identifiable and constitutionally proscribable conduct,"[24] the prohibited conduct of the *ISP* is not so easily identifiable. There is no explanation in the new law, for example, as to whether an ISP may maintain open access to a web site containing primarily protected speech even if it also contains a hyper-link to unprotected child pornography. Nor does the law make any allowance for an ISP to continue to offer access to a site that itself

contains a split screen, including separate child pornography and non-child pornography items. The Pennsylvania law shifts the burden to the ISP to devise a way to separate protected and unprotected speech. It is exactly this kind of blunderbuss approach to the regulation of speech that the First Amendment forbids. As the Supreme Court recently put it, "the possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted."[25]

**The Commerce Clause.** In addition to running afoul of the First Amendment, Pennsylvania's new Internet child pornography law raises serious Commerce Clause concerns.[26] Because communications over the Internet are themselves interstate commerce, because users of the Internet participate in interstate commerce as Internet consumers, and because the Internet, as a conduit, is an instrument of commerce, there is no question that "the Internet fits easily within the parameters of interests traditionally protected by the Commerce Clause."[27]

First, there is a need for uniformity in regulating, or not regulating, this unique international medium,[28] as Congress has recognized in identifying the federal policy to "preserve the vibrant and competitive free [Internet] market, . . . unfettered by Federal or State regulation."[29] Pennsylvania's own attempt to regulate ISPs which, by virtue of the ambiguous and potentially broad reach of the "disable access to" mandate, forces Internet service providers located anywhere in the world to conform to the Commonwealth's child pornography laws, thwarts this uniform approach.[30] Second, Pennsylvania's local interest in applying its tort law to Internet communications is far outweighed by the strong federal interest in maintaining the Internet free of state regulation, particularly as to content. Congress made this calculation when it chose, through Section 230, to preclude state attempts to hold ISPs responsible for the content of others. Indeed, Section 230 reflects a congressional decision to strike the balance between *incentivizing* ISPs to create better screening technology and *forcing* ISPs to develop new technology through the threat of civil or criminal sanctions; Congress has chosen the former approach as a nationwide policy. Finally, because Pennsylvania's new law threatens to upset this balance and, through overreaching in light of present technology, risks "directly control[ling] commerce occurring wholly outside the boundaries [of the Commonwealth]," enforcement of the new law could "exceed the inherent limits of [Pennsylvania's] authority."[31]

**Conclusion.** Like many aspects of modern technology, the Internet has magnified both positive and negative aspects of the human experience. The Internet's great potential for legitimate commerce and the dissemination of art, literature, and news is matched by its a possible abuse as a tool for trafficking in contraband such as child pornography. Rather than continuing to attack those who knowingly create and traffic in child pornography, Pennsylvania has chosen to attack the medium itself. This approach promises little in the way of law enforcement gains and substantial losses in the areas of personal freedom to create and receive expressive content over the Internet. Because Pennsylvania's new law conflicts with federal law and raises serious constitutional questions, no court should sanction its enforcement. Rather, Pennsylvania in particular, and the law enforcement community in general, should direct their efforts at the sources of the noxious content, rather than the new mode of delivery.

*Andrew G. McBride, Partner, Wiley Rein & Fielding LLP. Mr. McBride is a former law clerk to Justice Sandra Day O'Conner and Judge Robert H. Bork.
Kathryn L. Comerford, Associate, Wiley Rein & Fielding LLP. Ms. Comerford is a former law clerk to Justice Clarence Thomas and Judge J. Michael Luttig. The authors would like to thank Clint N. Smith, former Vice President and Chief Network Counsel at WorldCom, for his thoughtful comments on this article.

## Footnotes

[1] *Reno v. American Civil Liberties Union*, 521 U.S. 844, 852 (1997) (internal quotation marks omitted).
[2] Pa. Stat. Ann. tit. 18, § 7330(a).
[3] *Id.* at § 7330(f).
[4] *Id.* at § 7330(c)(1)-(3).
[5] *Id.* at § 7330(j).
[6] *Id.* at § 7330(b).
[7] 47 U.S.C. § 230(c)(1).
[8] *See, e.g.*, *Zeran v. America Online, Inc.*, 129 F.3d 327 (1997); *Doe v. America Online, Inc.*, 783 So.2d 1010 (Fla. 2001); *Stoner v. eBay Inc.*, 2000 WL 1705637 (Cal. Sup. Nov. 7, 2000).
[9] *Zeran*, 129 F.3d at 332.
[10] *Id.* at 333.
[11] 47 U.S.C. § 230(e)(1) (emphasis added).
[12] *See Doe*, 783 So.2d at 1011-12 (holding that plaintiff's negligence claim based on the service provider's alleged permitting of a third party to violate Florida's criminal child pornography distribution statute was barred by Section 230).
[13] 47 U.S.C. § 230(e)(3) (emphasis added).
[14] *Zeran*, 129 F.3d at 331; *see also Blumenthal v. Drudge*, 992 F. Supp. 44, 52 (D.D.C. 1998) (explaining that Congress created federal ISP immunity "as an incentive to [ISPs] to self-police the Internet for obscenity and other offensive material, even where the self-policing is unsuccessful or not even attempted").
[15] *See English v. General Elec. Co.*, 496 U.S. 72, 79 (1990).
[16] *See New York v. Ferber*, 458 U.S. 747, 764 (1982).
[17] *Cf. Blount v. Rizzi*, 400 U.S. 410, 420 (1971) ("[I]t is vital that prompt judicial review on the issue of obscenity—rather than merely probable cause—be assured . . . before the [Government's] severe restrictions . . . are invoked.").
[18] *See, e.g.*, *Illinois v. Gates*, 462 U.S. 213, 235 (1983); *United States v. Arvizu*, 122 S. Ct. 744, 751 (2002).
[19] *Reno*, 521 U.S. at 851.
[20] *Id.*
[21] Indeed, as a federal court in California recognized in refusing to enforce a French order that would force Yahoo! to restrict all access by residents of France to Nazi items available through its service, it was technologically impossible for Yahoo! to limit access by a geographically limited set of users to particular content and items available through its service. *See Yahoo!, Inc. v. La Ligue Contre le Racisme et L'Antisemitisme*, 169 F. Supp. 2d 1181 (N.D. Cal. 2001).
[22] For example, in order to block access to offending material, an ISP might have to restrict access to an entire website. It might also have to disable search engines' ability to lead to that website by blocking any combination of words that would uncover the website. Many of these word combinations could lead to legitimate speech as well as child pornography.
[23] *Thornhill v. Alabama*, 310 U.S. 88, 97 (1940). Moreover, the statute may well effect a prior restraint on speech to the extent it suppresses speech before viewers receive it. *See, e.g.*, *Blount*, 400 U.S. 410 (holding unconstitutional as a prior restraint provisions of postal laws that enabled the Postmaster General to halt delivery of mail to individuals). Such a prior restraint "'bear[s] a heavy presumption against its constitutional validity,'" *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 558 (1975) (quoting *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963)), and "'avoids constitutional infirmity only if it takes place under procedural safeguards designed to obviate the dangers of a censorship system,'" *id.* at 559 (quoting *Freedman v. Maryland*, 380 U.S. 51, 58 (1965)).
[24] *Maryland v. Joseph H. Munson*, 467 U.S. 947, 965-66 (1984).
[25] *Ashcroft v. Free Speech Coalition*, 122 S.Ct. 1389, 1404 (2002) (quoting *Broadrick*, 413 U.S. at 612).
[26] *See, e.g.*, *American Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 167 (S.D.N.Y. 1997); *Cyberspace Commun., Inc. v. Engler*, 142 F. Supp. 2d 827 (E.D. Mich. 2001); *PSINet, Inc. v. Chapman*, 108 F. Supp. 2d 611 (W.D. Va. 2000).
[27] *American Libraries*, 969 F. Supp. at 167, 173-74.
[28] *Reno*, 521 U.S. at 851.
[29] 47 U.S.C. § 230(b)(2); *see also id.* at § 230(a)(4) (finding that "[t]he Internet and other interactive computer services have flourished, to the benefit of all Americans, with a minimum of governmental regulation").
[30] *See, e.g.*, *American Libraries*, 969 F. Supp. at 183; *Wabash, St. L. & P. Ry. Co. v. Illinois*, 118 U.S. 557 (1886) (holding railroad rates exempt from state regulation because of the need for uniform national regulation).
[31] *Healy v. Beer Inst.*, 491 U.S. 324, 336 (1989).