UIC John Marshall Journal of Information Technology & Privacy Law

Volume 23
Issue 2 *Journal of Computer & Information Law - Winter 2005*

Article 6

Winter 2005

Pennsylvania and Pornography: CDT v. Pappert Offers a New Approach to Criminal Liability, 23 J. Marshall J. Computer & Info. L. 411 (2005)

John Spence

PENNSYLVANIA AND PORNOGRAPHY: CDT V. PAPPERT OFFERS A NEW APPROACH TO CRIMINAL LIABILITY ONLINE

I. INTRODUCTION

The field of Internet legislation is littered with spectacular failures.[1] Successes have been modest, few and far between. The rapid expansion of information technology in the past few years has left states and the Federal government struggling desperately to keep up. In response there have been a number of laws passed that attempt to regulate the Internet and information technology in general.[2] Many of these laws, however, show a lack of understanding how the affected technology actually works.[3] It has also at times had a retarding effect on the growth and distribution of new ideas and inventions. The courts have generally recognized this problem but various legislative bodies have been slower to follow step.[4] If read literally, the outcome of some laws would incapacitate the Internet and potentially bring it to a screeching halt.[5]

---

1. *See e.g. Communications Decency Act*, 47 U.S.C. § 223 (1995) (struck down in *Reno v. ACLU*, 521 U.S. 844 (1997)) [hereinafter "CDA"]; *Child Pornography Prevention Act* (CPPA), 18 U.S.C. § 2256 (1996) (held unconstitutional in *Ashcroft v. The Free Speech Coalition, et al.*, 535 U.S. 234 (2002)). There has also been a long string of state attempts to regulate the Internet that have been successfully challenged on Constitutional grounds. "In fact, every federal court that examined a state law that directly regulated the Internet determined that the state law failed the Pike balancing Test." *Center for Democracy & Technology et al vs. Pappert,* 337 F. Supp.2d 606, 661 (E.D. Penn. 2004).

2. *See* Child Online Privacy Act, 47 U.S.C. § 231 (1998) [hereinafter "COPA"]; Digital Millennium Copyright Act, 17 U.S.C. § 512 (1998) (dealing in part with restrictions on using technology to circumvent encryption or other security devices) [hereinafter "DMCA"]; The Children's Internet Protection Act, 20 U.S.C. § 7001 (1998) (requiring the installation and use by schools and libraries of Internet filtering technology) [hereinafter "CIPA"].

3. *Infra* n. 5.

4. *Fabulous Associates, Inc., v. Pennsylvania Public Utility Commission*, 896 F.2d 780 (1990); *Sable Communications of California, Inc. v. FCC*, 492 U.S. 115 (1989); *United States v. Playboy Entertainment Group*, 529 U.S. 803 (2000).

5. *See Electronic Communications Privacy Act*, 18 U.S.C. § 2510 (1986) (making it illegal for anyone but the intended e-mail recipient to look at the content of an e-mail data packet). The effect would be to stop all e-mail from being delivered since every computer in the chain must look at the information to determine if it is the recipient or if the data packet should be sent along to the next stop in the route. This law demonstrates the discon-

While it is easy to criticize past legislative efforts, it is obviously impossible for politicians to be experts on all matters. The incredibly wide range of topics covered by pending bills requires reliance on a number of experts to help form opinions. However, many of these experts directly contradict each other on issues ranging from the trivial to ones that strike the very core of public policy.[6] Adding to the confusion are the pressures of special interest lobbying groups and public opinion.[7] Especially when it comes to issues such as child pornography and the accessing of pornography by minors, long range thinking and careful deliberation must seem like a luxury. These traditional "hot button" issues have gotten even hotter with the further expansion of the Internet and the growing percentage of Americans who have access to it.[8] While these problems are inherent in all legislative processes it is especially pronounced in the field of information technology due to its rapidly evolving nature. Simply put, the field is growing so fast and reaching so far

---

nect between the understanding of traditional modes of communications, where a sender and recipient create a closed loop, and electronic communications where there are many participants routing information in a number of ways. *See generally* Marshall Brain, *How E-mail Works*, http://computer.howstuffworks.com/email.htm (accessed Mar. 7, 2005).

6. *See generally* Usenet.com, *Newsgroups and Newsgroup access, The #1 Uncensored Premium Usenet Service on the Planet*, http://www.usenet.com/index.htm (accessed Mar. 7, 2005); Timothy Campbell, *Flame Wars and Other Online Arguments* http://members.aol.com-/intwg/flamewars.htm (accessed Apr. 20, 2003). One of the more interesting facets of Internet and computer culture is that every single detail, from the grandest vision to the smallest technical minutia is argued passionately and at great length. Some of the seemingly epic struggles have included: Mac versus PC, Microsoft versus other software and operating system developers, competing sets of technical standards, and encryption users versus the Federal government. While a few of these issues might provoke strong responses among the public, countless Web site forums and chat rooms are filled with emotional arguments and "flame wars" over topics that ninety-nine percent of the general population knows nothing about, nor cares about in the slightest. Topics that often seem largely academic can quickly devolve into name calling and vicious personal attacks. *Id.*

7. Microsoft, *Microsoft Chairman Bill Gates Calls on Congress to Give President Authority to Negotiate New World Trade Deals*, http://www.microsoft.com/presspass/press/1999/Feb99/WorldTradePr.asp (accessed Feb. 26, 1999). The financial clout of companies interested in issues such as the Internet and information technology cannot be overestimated. Music labels, movie studios, software, and computer companies have all become involved in testifying in front of legislative bodies as well as lobbying for the passage or defeat of specific proposed laws. *Id.* Bill Gates and other members of Microsoft are particularly involved in lobbying and speak on a wide range of issues that touch upon everything from the purely technical to the President's authority to negotiate "fast track" economic pacts. *Id.*

8. Internet World Stats, *Top Ten Countries in Internet Usage and Penetration*, http://www.internetworldstats.com/top10.htm#pop (accessed Mar. 7, 2005). The rapid growth of the Internet has made pornography more readily accessible to technology-sophisticated children than any time before. While there are a number of resources for parents to limit their children's exposure to such material, their knowledge of computers and the Internet has often lagged behind.

that it is difficult, if not impossible, for most people to keep up. The Internet has penetrated the home market at a speed matched by no other means of communication before it.[9] Radio and Television took decades before they gained a foothold into a majority of the homes in this country.[10] The Internet on the other hand can be accessed in more locations then ever before including homes, schools, and libraries. In the world of information technology new innovations and fields of industry seemingly appear overnight and bring with them a whole host of questions and concerns.[11] Governments are still reacting to, and legislating about, technology that has largely come and gone. While the mention of Napster[12] will still evoke strong responses from many in the public policy sphere it has long since been replaced by new models of file sharing technology such as Grouper,[13] Kazaa,[14] and BitTorrent.[15] By the time legislation can address a specific issue or problem it has often already been solved by the market or replaced by a newer version. It would be the same exercise in futility if governments were to pass laws regulating the use of blank audio cassettes or Betamax machines.

The very nature of the legislative process does not lend itself well to regulating technology. While a vast majority of the concerns raised by parents and other groups are already covered by non Internet related laws, the pressure to "do something" about these supposedly new threats

9. *See e.g.* Humphrey Taylor, *The Harris Poll*, http://www.harrisinteractive.com/harris_poll/index.asp?PID=295 (Apr. 17, 2002) While reliable statistics for Internet use are difficult to come by, the majority of studies indicate that the growth in the penetration rate of the Internet into the American home from approximately 1995 to 2002 was incredible. *Id.*; *see also* Miniwatts International Inc., *World Internet Usage Statistics and Population Stats*, http://www.internetworldstats.com/stats.htm. (accessed Mar. 7, 2005) (For a compilation of Internet usage statistics and lists); *see also* Network Overview, *Internet Traffic Report*, http://www.internettrafficreport.com/main.htm (accessed Mar. 7, 2005) (For an up to the minute tracking of Internet usage and the quality of connections broken down by geographic area).

10. Northwestern University Media Management Center, *Media Info Center*, http://www.mediainfocenter.org/compare/penetration/ (last updated Mar. 23, 2004).

11. *See generally A&M Records v. Napster*, 239 F.3d 1004 (9th Cir.2001); *A&M Records v. Napster*, 114 F. Supp.2d 896 (N.D.Cal 2000); *Sony Corp. of America v Universal City Studios, Inc.*, 104 S.Ct. 774 (1984). Major music labels and associated copyright holders were seemingly caught off guard by the explosion in peer to peer file sharing technology. *Id.* File sharing programs such as Napster suddenly made the widespread dissemination of copyrighted material cheap and relatively easy. *Id.* CD burners and machines capable of playing reformatted music have also pushed copyright holders into reevaluating their legal strategies as well as their overall business model. There is a string of cases dealing with the issue of unauthorized copying and fair use. *Id.*

12. Napster, *Napster.com*, http://www.Napster.com (accessed Mar. 7, 2005).

13. Grouper Networks Inc., http://www.Grouper.com (accessed Mar. 7, 2005).

14. Sharman Networks Ltd, http://www.Kazaa.com (accessed Mar. 7, 2005).

15. Bram Cohen, *The Official BitTorrent Home Page*, http://bittorrent.com/ (accessed Mar. 7, 2005).

has been overwhelming.[16]

The problems inherent in regulating technology are only exacerbated when combined with sexually explicit content, another source of constant difficulty and struggle. One area in particular that has been the subject of widespread concern and attention is online pornography.[17] While it is not a surprise that the adult industry is big business, few people realize just how big it truly is. According to one survey,[18] pornography is a fifty-seven billion dollar a year industry with over twelve billion dollars a year generated in the United States alone.[19] Online pornography accounted for approximately two and a half billion dollars in 2003,[20] a number that is probably conservative and was outdated the moment it was printed. Pornography as a driving force behind technological innovation is nothing new. It has been the economic engine behind many types of commercial technology including: home videos, pay-per-view movies, and countless aspects of the Internet as a whole.[21] Problems arise however when governments attempt to restrict online access to pornography and other sexually explicit content. Given the current state of technology it is extremely difficult, if not impossible, to

16. *See generally*, Wired, *Wired News: Movie Studios Sue File Traders*, http://www.wired.com/ news/digiwood/0,1412,65730,00.html (Nov. 16, 2004). Generally speaking, the recent wave of laws related to the Internet and the widespread coverage of the DMCA provide evidence of the pressure being brought upon legislators to address these issues. Also, the recent lawsuits filed by movie studios against file swappers signals the opening of a new front in the war over copyrights and fair use. *Id.*

17. *See* FPC, *Foreign Press Centers*, http://fpc.state.gov/documents/organization/35133.pdf (last updated July 6, 2004). The majority of laws regarding the Internet which have been struck down deal with pornography or sexually explicit material in some sense. *Supra* nn. 1-2. There has been a wave of laws relating to the Internet and user privacy, such as the use of cookies and spyware. *See* Internet Spyware Prevention Act of 2005 H.R. 744 (2005); CAN-SPAM Pub. L. No. 108-187, 117 Stat. 2699 (2003). However, the laws which caused the most concern, those dealing with children and pornography, were the first to be challenged. *Id.*

18. Top Ten Reviews, *Internet Pornography Statistics* http://www.internetfilterreview.toptenreviews.com/internet-pornography-statistics.html (accessed Mar. 7, 2005).

19. *Id.*

20. *Id.*

21. *See* Steve Baldwin, *Ghost Sites: The Museum of E-Failure (Dead Web Site Screenshots)*, http://www.disobey.com/ghostsites/mef.shtml (accessed Mar. 7, 2005); FuckedCompany, *FuckedCompany.com- Official lubricant of the new economy*, http://www.fuckedcompany.com/ (accessed Mar. 7, 2005). (detailing an eye-opening tour through some of the various failed, and failing online businesses) Money follows where demand is greatest. Pornography was the first, and still one of the few, industries to earn a profit from online activities. *see also* Fredrick S. Lane, *Obscene Profits: The Entrepreneurs of Pornography in the Cyber Age*, (Routledge 2001). Pornography has been such a large player in the online world that it has driven technology that originally was designed for specified usage but later found its way into mainstream public use. *Id.* This includes technology such as online video conferencing, voice over Internet, and the push towards higher broadband service to speed the storage and download of images and video files. *Id.*

block content in a way that complies with Constitutional requirements as well as makes any kind of economic sense.

This article will focus on the recent District Court of Pennsylvania decision in *Center for Democracy & Technology et al vs. Pappert*[22] as an example of why current legislation, specifically on a state level, of the Internet simply does not work. This is especially true when dealing with issues such as pornography and obscenity. For reasons discussed below, this law was a legal train wreck of epic proportions. There is virtually no aspect of the Act, or its implementation, that could fairly be considered Constitutional or effective.

The *Pappert* case is the latest in a string of decisions striking down laws aimed at regulating online access to pornography and other sexually explicit material.[23] It also has direct parallels in a number of cases that deal with the "real world" distribution and sale of pornography and the government's attempts to regulate and ban such material.[24] State governments have not been able to devise a plan capable of limiting the spread of contraband material online.[25] Not only do these laws have a number of inherent Constitutional problems, they simply do not work.

The first step in crafting a response to the legitimate interests of stopping child pornography and the access of adult material by minors is to do nothing. While this may seem counterintuitive at first one need only look to the glaring failures of recent Internet related laws, specifically the *Communications Decency Act*[26] and others, to see what previous efforts have wrought. Also needing consideration are traditional criminal and civil statutes that already address many of the issues raised by sexually explicit material on the Internet.

---

22. *Center for Democracy & Technology et al vs. Pappert*, 337 F. Supp.2d 606 (E.D. Pa. 2004).

23. *See American Booksellers Foundation et al v. Dean*, 342 F.3d 96 (2003) (striking down 13 V.S.A. § 2802a which prohibited the dissemination of indecent material to minors); *ACLU v. Johnson*, 194 F.3d 1149 (1999)(striking down N.M. Stat. Ann. § 30-37-3.2(A) prohibiting the dissemination by computer of material that is harmful to minors); *PSInet v. Chapman*, 167 F.Supp.2d 879 (2001)(Striking down Va.Code Ann. § 18.2-391 criminalizing the dissemination by computer of material that is harmful to minors).

24. *See Bantam Books v. Sullivan*, 372 U.S. 58 (1963)(finding the authority wielded by the commission to encourage morality in youth unconstitutional); *New York v. P.J. Video*, 475 U.S. 868 (1986)(concerning the seizure of allegedly obscene materials and the standards applied to the issuance of search warrants); *Vance v. Universal Amusement Co.*, 445 U.S. 308 (1980)(finding unconstitutional a statute which permitted the prior restraint of speech).

25. In the sense of drafting legislation capable of withstanding a constitutional challenge as well as their general ineffectiveness in stopping the dissemination of child pornography and obscenity. As the *Pappert* court makes clear in their decision, state laws meant to stop child pornography have had no appreciable impact in the availability of such material. *CDT v. Pappert*, 337 F. Supp. 2d 606, 654 (E.D. PA. 2004).

26. 47 U.S.C. § 223 (1995).

Ultimately, the best answer to furthering the legitimate interests of controlling access to obscenity and child pornography lies in a combination of federal/international legislation, self regulation by the adult industry, and most importantly common sense by individual users. This approach to regulating the Internet springs from the various violations of the Constitution inherent in current legislation as seen in the present case including but not limited to: the dormant commerce clause, due process protections of the fourteenth Amendments, the prior restraint of speech in violation of the first Amendment, and the over breadth doctrine.

II. BACKGROUND

The rise of the Internet has once again brought old judicial problems to the forefront, this time with additional layers of difficulty.[27] The interrelated issues of pornography, obscenity, and access to this material have been giving the court system headaches for years.[28] An exact difference between obscenity and pornography, and the legal analysis of what to do with both, has proven difficult to come by. At various points in time the Supreme Court has formulated different tests to determine the line between pornography and obscenity, often with little preciseness or understandable articulation.[29] While obscenity may be entirely proscribed by government, pornography enjoys a degree of first amendment protection.[30] This distinction is of vital importance when considering the constitutionality of any law that attempts to block access by an adult to sexually explicit material. As in the Pennsylvania statute, overbreadth and due process are serious problems with most laws trying to limit speech. While the Internet has certainly made pornography and obscen-

27. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse,* 1996 U. Chi. Legal F. 207 (1996) (regarding further information about the possible benefits and concerns of mixing new and traditional approaches to the law and the Internet); and Lawrence B. Solum & Minn Chung, *The Layers Principle: Internet Architecture and the Law* 79 Notre Dame L. Rev. 815 (2004).

28. *Infra* n. 31.

29. *See e.g. Miller v. California,* 413 U.S. 15 (1973); *New York v. Ferber,* 458 U.S. 747 (1982). Anyone who claims to be able to differentiate between obscenity and pornography should be treated with a great deal of skepticism. At some point, the famous answer of "I can't explain it but I know it when I see it" will no longer suffice as grounds for the suppression of speech whether commercial or purely expressive. Calling the distinction between obscenity and pornography a legal fiction would seem to be generous. Anytime something as nebulous as "community standards" acts as a determinative factor, great caution must be exercised.

30. *See generally City of Littleton, Colorado v. Z.J. Gifts,* 124 S.Ct. 2219 (2004). As the cases dealing with the licensing of adult businesses show, pornography is afforded constitutional protection, but may be much more tightly controlled than other kinds of speech. *Id.* Pornography also always runs the risk of crossing the invisible and imperceptible line into obscenity which falls outside of constitutional safeguards. *Id.*

ity more readily accessible, it is hardly a novel problem or concern.[31] Pennsylvania's recent approach to controlling it however, is.

In February of 2002, Pennsylvania passed the Internet Child Pornography Act.[32] In short, the Act requires an Internet Service Provider (ISP) to disable access to child pornography that is "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. . . ."[33] This demand by the Attorney General's office comes with a novel hook, the threat of criminal prosecution.[34]

In much the way the Recording Industry of America Association ("RIAA")[35] went after music traders by suing the means of access such as Napster,[36] Pennsylvania went after ISPs to try and cut off subscribers' ability to reach child pornography. Although the Pennsylvania Attorney General has conceded that the ISPs themselves had no part in creating or distributing the alleged contraband, they still attempted to apply a criminal statute to them that forces compliance.[37] While many tools have been used by law enforcement agencies to try and stem the tide of child pornography, this is the first attempt by a state to enforce criminal

31. *See e.g. Bantam Books vs. Sullivan*, 372 U.S. 58 (1963); *Sable Communications v. FCC*, 492 U.S. 115 (1989); *New York v. P.J. Video*, 475 U.S. 868 (1986); *U.S. v. Playboy Entertainment*, 529 U.S. 803 (2000) (exemplifying some of the more famous cases over the years dealing with the issues of pornography, obscenity, child pornography, and access by minors).

32. 18 Pa.C.S.A. §§ 7621-7630; *see also Pappert*, 337 F. Supp.2d at 609.

33. 18 Pa.C.S.A. §7622.

34. 18 Pa.C.S.A. §7624.

> Notwithstanding any other provisions of law to the contrary, any Internet service provider who violates section 7622 relating to duty of Internet service provider commits:
> (1) A misdemeanor of the third degree for a first offense punishable by a fine of $5,000
> (2) A misdemeanor of the second degree for a second offense punishable by a fine of $20,000
> (3) A felony of the third degree for a third or subsequent offense punishable by a fine of $30,000 and imprisonment for a maximum of seven years (emphasis added).

35. RIAA, *Recording Industry of America*, http://www.riaa.org (accessed Mar. 7, 2005).

36. *A&M Records v. Napster*, 239 F.3d 1004 (9th Cir. 2001) and *A&M Records v. Napster*, 114 F. Supp.2d 896 (N.D.Cal 2000).

37. *Pappert*, 337 F. Supp.2d at 633. This can be seen most clearly in the nature of the Act by which legislators criminalized the ability to access the child pornography. There are already laws which make the distribution or possession of child pornography illegal. *Id.* Yet instead of using existing laws, they sought to force ISPs to act as deputized law enforcement agents. *Id.* In at least one instance, the Attorney General's office contacted the host of an allegedly offending Web site themselves, clearly showing that they did not need an ISP to remove offending content from a Web site. *Id.* at 620. They also suggested that ISPs could do the same in order to block access to the material. *Id.* at 624.

penalties against someone with no direct link to the content.[38]

Although the general population is increasingly familiar with the Internet, a short description of what an ISP is, and just as importantly is not, is necessary.[39] ISPs are the gateway to what is generally referred to as the Internet and allow users to send and access information in an increasingly wide variety of means and formats.[40] People often think of their local ISP as the main and only entity responsible for their ability to access the Internet. The reality of the situation is more complicated. Any number of companies and institutions that an individual user has never heard of, and with whom they have no contractual relationship, handle their information as it winds it way along the path.[41] When a user connects to their ISP through either a dial-up modem or other higher speed connection, the local ISP will then connect to another, larger, ISP into what is called an Internet backbone provider.[42] Backbone providers a re essentially high speed and high volume ISPs that serve as the trunk of the tree that branches off in countless directions to smaller ISPs and finally the end destination sought by the user.[43] Much like using local side-streets to get onto the highway and then exiting and returning to smaller roads to reach your destination, users are likely to take a number of different steps along the route to reach their intended endpoint.[44] Just as with automotive traffic, information congestion on an ISP will cause alternate routes to be taken in order to carry out a user

---

38. *Id.* at 610.

39. *See generally* Jeff Tyson, *How Internet Infrastructure Works* http://computer.howstuffworks .com/internet-infrastructure.htm (accessed Mar. 7, 2005) (detailing background on the structural underpinnings of ISPs and the Internet as a whole).

40. *See* FCC, *The FCC History Project - INTERNET: Making the Connections*, http://www.fcc.gov/omd/history/internet/making-connections.html (last updated June 24, 2004). As the number of computer and Internet users has grown, so has the number of ways in which information can be formatted and sent. Increases in connection speed and the power of personal computers has allowed data transmission on a scale undreamed of even in the recent past. *Id.* Users with broadband or other high speed connections can stream music and download entire movies in a fraction of the time required by dial up; *see also See* FCC, *Voice-Over-Internet* Protocol, http://www.fcc.gov/voip/ (last updated on Nov. 10, 2004). New applications of this capacity can be seen in the expanding fields of Interactive television and Voice over Internet telephone services ("VOIP"). *Id.*

41. Curt Franklin, *How Routers Work*, http://computer.howstuffworks.com/-router10.htm (accessed Mar. 7, 2005); *See* Howstuffworks, *What is a packet?* http://computer.howstuffworks.com/question525.htm (accessed Mar. 7, 2005) (explaining how and why in transit data is broken into smaller "data packets").

42. *Id.*; Jeff Tyson, *How Internet Infrastructure Works* http://computer.howstuffworks -.com/internet-infrastructure1.htm (accessed Mar. 7, 2005).

43. *Id.* at http://computer.howstuffworks.com/internet-infrastructure3.htm (accessed Mar. 7, 2005).

44. Curt Franklin, *How Routers Work*, http://computer.howstuffworks.com-/router10.htm (accessed Mar. 7, 2005).

request.[45] The very structure of the Internet makes centralized control over information impossible because of the global nature of Internet service and access.[46] This is because the Internet is premised upon the idea of a decentralized series of redundant connections that do not follow historic concepts of jurisdiction or location.[47]

Another difficulty with implementing the Pennsylvania act is that ISPs are not all created the same. Some ISPs offer Web hosting services where they will post a subscriber's Web site and make it accessible to other users.[48] Other ISPs are nothing more then a conduit for information to come and go.[49] Even for those ISPs which store user's information on their servers, the ability to restrict access to specific material is limited at best and often heavy handed.[50] The vast majority of Web sites and information which reside on the Internet do not exist under the control of the requesting user's ISP.[51] Any one singular ISP has no ability

45. *Id.* at http://computer.howstuffworks.com/router.htm (accessed Mar. 7, 2005).

46. David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr., *The Accountable Internet: Peer Production of Internet Governance* 9 Va. J.L. & Tech. 9 (2004); James E. Gaylord, *State Regulatory Jurisdiction and the Internet: Letting the Dormant Commerce Clause Lie* 52 Vand. L. Rev. 1095 (1999); Dennis T. Rice, *Problem in Running a Global Internet Business: Complying With Laws of Other Countries* 797 PLI/Pat 11 (2004). The Internet is comprised of a large number of networks connected to each other tending to make any kind of centralized legal authority difficult.

47. *See* Michael Hauben, *Behind the Net - The untold history of the ARPANET* http://www.dei.isep.ipp.pt/docs/arpa.html (accessed Mar. 7, 2005) (detailing the very beginnings of what would develop into the Internet); *see also* FCC, *The Internet: A Short History of Getting Connected* http://www.fcc.gov/omd/history/internet/ (last updated June 02, 2004).

48. *See generally* Isp Guide, *Web Hosting Directory* http://www.isp-guide.com (accessed Mar. 7, 2005) (overview of the number of ISPs currently available). A large number of companies such as America On Line (AOL) provide users with the ability to post their own homepages.

49. Part of the problem with many laws regarding the Internet is that terminology is often difficult to define in a precise manner. Before, there was never a need for highly technical definitions for every piece of hardware or computing process. As seen in the *Pappert* case, the decision as to what constitutes an "ISP" is contentious with companies such as MSN arguing that they should not be subject to the informal notices because they did not own or operate its own network. *Pappert* at 626.

50. Yahoo, *Ecommerce Hosting Solutions from Yahoo! Small Business*, http://smallbusiness.yahoo.com/merchant/ (accessed Mar. 7, 2005). The sheer number of users on the Internet who have the ability to post a Web site renders strict oversight by a company difficult. Geocities.com is a division of Yahoo and is one of the largest Web hosting services. While actual numbers are hard to determine, a search of the Geocities.com site for user pages dealing with "music" netted sixteen distinct categories of individual Web sites. Each of these categories then lists thousands, if not tens of thousands, of Web pages. Geocities also offers hosting services for small businesses. *Id.*

51. *Pappert*, 337 F. Supp.2d at 626. This is also clear from the difficulty ISPs had in implementing the Pennsylvania Act. They quickly realized that they had no authority to force a third party to remove the offending material so in order to avoid criminal charges they resorted to blocking the site entirely regardless of the imprecise nature of their actions. *Pappert* at 619-620.

or authority to demand that another ISP remove prohibited content from its servers or another server further down the line.[52] Companies such as Microsoft protested vigorously that they did not own the actual means through which their client's gained access to the Internet and therefore had no ability to force a third-party to comply with a court order.[53] Therefore, removing the offending content is often impossible without the permission and cooperation of the actual host or owner.[54] This leaves ISPs with the unenviable, and largely technologically impossible, task of blocking individual Web sites which exhibit or traffic in prohibited material.

The process by which the Pennsylvania Attorney General's office initiated the process of blocking access to specific Web sites highlights the difficulties and weaknesses of the law.[55] Statutory language states that a District Attorney has the authority to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" that ISP's service upon a showing of probable cause that the item qualifies as child pornography as defined by the statute.[56] Interestingly, the hearing to issue the court order was conducted on a purely ex-parte basis without the knowledge of either the ISP or the individual Web site owner that was the cause of the objection.[57] Nor was there any notice given after the hearing to the Web site owner, only the ISP which was then ordered to comply by shutting off access. In other words the owner of a specific Web site, and those blocked by accident, had no way of knowing that their site had been banned and no way to challenge that decision.[58]

---

52. *Id.*

53. *Id.* at 627; *supra* n. 49.

54. This is where many of the "wild west" aspects of the Internet become apparent. Because of the multitude of jurisdictions involved with the Internet there is no one central authority that an ISP can go to for help in shutting down a Web site. While federal law enforcement agencies, such as the Secret Service, may investigate allegations of child pornography, ISPs themselves have no special legal authority to require the removal of content. For one ISP to tell another ISP what they must do would be analogous to Ford telling Chevrolet what safety standards must be included in their new vehicles. While it is certainly in everyone's best interest to work together in combating the spread of child pornography, this basic lack of authority is a fundamental flaw in the Pennsylvania act which makes ISPs responsible for enforcing criminal statutes.

55. Specifically the Due Process issues involved in the effective seizure of a Web site address. As mentioned, there was no opportunity for the ISP or Web site owners to object to or participate in the issuance of a court order. In effect, the court was asked to issue an order to a party not involved in the hearing, forcing them to either block access to a Web site or to somehow force another third party to remove material from a Web site. This again points out the slippery slope aspect of this statute since the owner of the Web site might have no connection to the state of Pennsylvania other then having a Web site that is accessible from the state. *Pappert* at 662.

56. 18 Pa.C.S.A. §§7626-7628; *Pappert*, 337 F. Supp. 2d. at 618.

57. *Id. at 619.*

58. *Id.*

Once the court order had been issued, the Attorney General's office notified the ISP by providing them with a copy of the court order.[59] The ISP then, by statute, had five business days to block access to the named content or face criminal liability.[60]

Shortly after the Pennsylvania Act went into effect, various ISPs reported to the Attorney General's office that they were worried about their inability to comply with the court order, especially within the five day window provided for in the statutory language.[61] Specifically, the ISPs stated they were unable to limit blocking of certain Web sites to Pennsylvania citizens alone, due to the borderless nature of the Internet and the infrastructure of the various ISPs themselves.[62] In response to the concerns raised by the ISPs, the Attorney General's office decided to utilize a more informal and flexible process by which they could notify an ISP that child pornography had been found to be accessible through its service and give them the chance to remove the items or block access.[63]

The Attorney General's office set up a special unit to coordinate efforts to implement the new law and established a citizen complaint forum where individuals could report Web sites containing content that they believed to be child pornography.[64] Upon receiving notice of alleged chilled pornography, a supervising agent reviewed the Web site and upon a positive finding sent out a notice to the ISPs.[65] The actual language of the informal notice changed several times, with words such as "must" being replaced by "should," and language referring to the criminal sanctions of refusing to comply being added.[66]

In total, approximately 470 informal notices were sent to various ISPs that the Attorney General's office had subscribed to, dealing with about 376 different URLs.[67] The ISPs that received these notices were generally able to prove to the satisfaction of the Attorney General that they had removed the contested item or blocked access to the material.[68] Largely they did this by either Internet Protocol (IP) filtering or Domain Name Servers (DNS) filtering which lead to a large amount of over blocking of innocent and unrelated Web sites.[69]

In July, an ISP named WorldCom wrote the Attorney General's of-

59. *Id.*
60. *Pappert*, 337 F. Supp.2d at 619.
61. *Id. at 619-620.*
62. *Id at 619.*
63. *Id.* at 620.
64. *Id.* at 619.
65. *Id.* at 620.
66. *Pappert*, 337 F. Supp.2d at 620-623.
67. *Id.* at 623.
68. *Id.*
69. *Id.* at 627-630 and 656-659.

fice a letter.[70] It stated that while WorldCom was "absolutely opposed" to child pornography and actively worked with law enforcement to aid in the prosecution of child pornographers, that it was not possible to block access to a Web site based on the information provided by the Attorney General's office.[71] WorldCom was also concerned with the informal nature of the notices as opposed to a formal court order.[72] Specifically, they were concerned with being held legally liability to their customers if they were to block access to their Web site or remove content absent proper authority.[73] In response, the Attorney General's office obtained a court order requiring WorldCom to remove or disable access to the child pornography.[74] The Attorney General then issued a press release stating that:

> In the vast majority of cases, the ISPs have agreed to disable access to the child pornography site to all of their Pennsylvania customers [in response to an 'informal notification' from the OAG]. . . [The OAG] notified WorldCom that an agent had discovered child pornography at several Internet sites accessible through WorldCom. Fisher's agents requested that access to the sites be disabled. However, *WorldCom informed the Attorney General's Office that it would not deny access to the child pornography sites.*" (Emphasis added).[75]

So not only did WorldCom and other ISPs face criminal sanctions for non compliance, they also were being publicly identified as unwilling or uninterested in stopping the dissemination of child pornography.[76]

This case started when individual members of the ACLU, and other advocacy groups, were unable to access specific Web sites that had been blocked by their ISP in response to either a court order or informal notice. The Attorney General's office conceded that the sites noted by Plaintiff did not contain child pornography.[77] The case was argued primarily on two issues. First, that it was an unlawful restriction of free speech.[78] Secondly, that the Act violated the Dormant Commerce Clause by seeking to regulate economic activity taking place outside of Pennsylvania.[79] The court held that the law was unconstitutional on both grounds. While the goal of the Act was to suppress only material which has no legal protection, the implementation proved to be far more complicated. The Pennsylvania Attorney General's Office, without hinting

70. *Id.* at 623.
71. *Id.*
72. *Pappert,* 337 F. Supp.2d at 623-624.
73. *Id.*
74. *Id.* at 624.
75. *Id.*
76. *Id.*
77. *Id.* at 626.
78. *Pappert,* 337 F. Supp.2d at 611.
79. *Id.*

which of the steps they would prefer, offered three techniques for ISPs to comply with an order to block access to a Web site.[80] Specifically, they suggested DNS filtering, IP filtering or null routing, and URL filtering as possible solutions.

DNS[81] filtering is a technique that works at the level of the DNS server in order to block access to a Web site.[82] The domain name of a specific Web site means nothing to a computer unless it is first converted into a format which it can understand.[83] When a user enters a Web site address, the request is sent to a DNS server which then translates the request into the Web site's IP address.[84] IP addresses are assigned to each machine connected to the Internet and consist of four sets of numbers ranging from 0 to 255 with each set separated by a period.[85] Once the user's computer has the IP address of the requested page it can receive the data from the Web site and display the content. Without this critical and very complicated intermediary step users would have to memorize long lists of IP octets to reach their favorite Web sites.[86]

A DNS filter works by an ISP maintaining a list of blocked domain names and checking any user requests against it.[87] If the request matches one of the blocked Web sites, the filter will bounce the request back and display a message that the information is not available.[88] The main problem with DNS filtering is that users are not required to use an ISP's DNS and therefore are able to bypass any restrictions placed on individual Web sites done at this level. There are a number of legitimate reasons why a user might choose not to utilize an ISP's DNS server, including that they have their own.[89] DNS filtering also leads to substan-

80. *Id.* at 620.

81. DNS are what allow Web sites to have human friendly names, such as http://www.howstuffworks.com instead of its IP address http://216.183.103.150

82. *Pappert*, 337 F.Supp.2d at 627.

83. *See* Marshall Brain, *How Domain Name Servers Work* http://computer.howstuffworks.com/dns.htm (accessed Mar. 7, 2005) (explaining DNS functions).

84. *Pappert*, 337 F. Supp. 2d at 616.

85. Marshall Brain, *How Domain Name Servers Work* http://computer.howstuffworks.com/dns.htm (accessed Mar. 7, 2005).

86. *Supra* n. 83, Without DNS servers, users would have to enter the IP address for each Web site that they wished to visit instead of being able to use the domain name. Considering the explosion in popularity of the Internet and the number of Web sites, DNS has been and continues to be absolutely essential to the function of the Internet.

87. *Pappert*, 337 F.Supp.2d at 627.

88. *Id.* at 627. The browser may show a 404 page not found error, or it may have a customized screen stating that the requested Web site has been blocked by the ISP, depending on the service. The service may also simply return a wrong web page.

89. A number of companies with internal networks of computers choose to run their own DNS service. Most often this is done to better tailor the service to a particular need or scale of use. Other users simply prefer other services than the one provided by their ISP. Howstuffworks.com runs its own DNS system as explained at: Marshall Brain, *How Do-*

tial over blocking as well since Web sites can change domain names.[90] Furthermore, DNS filtering will block sites with new content that take over a blocked site's address since there is no formal notice to the new owner and no clear way to get the block removed.[91] Finally, it also allows sites containing contraband to reopen in a matter of hours if not minutes, by changing their domain name.[92]

The second technique proposed by the Attorney General's Office is commonly known as IP filtering or null routing. IP filtering is similar to DNS filtering but performs its functions at a different step in the transmission of data.[93] IP filtering works by keeping a list of blocked IP addresses and stopping all requests to access that page at the server level.[94]

A number of ISP providers such as Worldcom and AOL use IP filtering techniques in order to prevent various computer problems such as spam, denial of service attacks and viruses.[95] However, IP filtering also leads to massive over blocking of innocent Web sites.[96] The problem with blocking individual IP addresses is that a number of different Web sites can share the same IP address. This is most often the case where there is a company performing "virtual hosting" by allowing individual

---

main Name Servers Work http://computer.howstuffworks.com/dns6.htm (accessed Mar. 7, 2005). Individual users are able to change the DNS settings which are provided by their ISP in order to use DNS that provide better services. Because users can choose their own DNS, the result is that requests for blocked Web sites are completed because the chosen DNS would not necessarily have the same list of banned addresses as the DNS run by the ISP.

90. *Id.*; http://computer.howstuffworks.com/dns1.htm (accessed Mar. 7, 2005).

91. *Pappert,* 337 F. Supp.2d at 657 (E.D. PA. 2004). There was no clear procedure for later owners of a Web site to find out that their Web site had been blocked. Nor was there any official procedure to get the block removed.

92. *See generally* Yahoo, *Geocities* http://geocities.yahoo.com/ (accessed Mar. 7, 2005);Terra, *informacion, noticias, servicios interactivos y eventos multimedia* http://www.terra.es/ (accessed Mar. 7, 2005) (hosting an extremely large number of individual user pages. Geocities provides basic hosting of sites for no charge and users could simultaneously hold a number of different sites with the same, or completely different, hosting services.). Once an owner or operator learns that users are unable to reach their Web site they can simply move the content of the page, or the whole page itself, to a new domain name that remains unblocked. Considering the ready availability of free or very low cost Web sites, the time between a site being shut down and subsequently reopened can be minimal. Especially for Web sites which are little more then picture or video collection points.

93. Carnegie Mellon Software Engineering Institute, *Configure firewall packet filtering* http://www.cert.org/security-improvement/practices/p058.html (last updated July 1, 1999). Instead of stopping the request at the DNS stage, null routing works by blocking the actual IP address of the targeted Web site as opposed to the domain name. *Id.* It is basically the same idea as DNS filtering, just performed after the DNS has performed its function. For a brief explanation of IP filtering and how it can be designed. *Id.*

94. *Pappert,* 337 F. Supp.2d at 627 (E.D. PA. 2004).

95. *Id.*

96. *Id.* at 632-633.

users to place their content on a sub page of the company's site.[97] Therefore, if the IP address that is blocked is that of a hosting service, all the sub-domain pages will be blocked as well regardless of content. In the case of a large hosting service, the number of blocked sites could run into the thousands.[98] Furthermore, IP addresses can change on a regular basis without changing the URL.[99] While specialized software can track these changes and alert the operators, it is unclear if this would be practicable on a significantly larger scale then it is currently used.[100]

The third and final technique involves "URL filtering." This requires: placing an additional router or reconfiguring an existing router to reassemble the data packets for specific Internet traffic, discern each Web site request, and match it against the list of blocked URLs.[101] Some services such as AOL use URL filtering as part of its "parental controls" package but could not perform URL filtering on the scale necessary to comply with the Pennsylvania statute.[102] In fact, an AOL engineer testified that implementing URL filtering would take years to implement network wide and be extremely expensive.[103] ISPs would not be able to implement URL filtering without sacrificing a sizeable amount of its performance, the key factor customers use to decide their service pro-

97. Yahoo, *Geocities* http://geocities.yahoo.com/ (accessed Mar. 7, 2005); Terra, *informacion, noticias, servicios interactivos y eventos multimedia* http://www.terra.es/ (accessed Mar. 7, 2005). These are two examples of large Web hosting communities specifically cited in the decision.

98. *Pappert*, 337 F.Supp.2d at 632-633. The record indicates that at the time of data collection that at least fifty percent of domains shared an IP address with at least fifty other domains. *See* Benjamin Edelman, *Web Sites Sharing IP addresses: Prevalence and Significance*, http://cyber.law.harvard .edu/people/edelman/ip-sharing/ (last updated September 12, 2003) (describing the problem of multiple sites sharing a single IP address).

99. Techtarget Network, *static IP address/dynamic IP address*, http://searchwebservices.techtarget .com-/sDefinition/0%2C%2Csid26_gci520967%2C00.html. (last updated July 19, 2004). There can be a number of reasons why an IP address changes. *Id.* Depending on the computer in question it might have a different IP address every time it accesses the Internet. *Id.* This is referred to as a "dynamic IP address." *Id.* Generally speaking, servers will keep the same IP address (i.e. they have a static IP address) but there are times when a Web site's IP address will change. *Id.* This can be done in order to evade blocking measures or simply be necessary because of technology reasons. *Id.* Neither of these situations requires that the Web site actually change its domain name. *Id.* So users looking for a blocked Web site could still find it if the IP address changes, thereby avoiding IP filtering.

100. *Pappert*, 337 F. Supp.2d at 632. There is software available that can track changes to a particular Web site's IP address and then implement a ban on the second IP address as well. *Id.* However, there was no evidence given to suggest that this would be efficient or usable on the scale needed for the Pennsylvania statute. *Id.*

101. *Id.* at 627.

102. *Id. at 629.*

103. *Id.*

vider.[104] To maintain their current service quality would require the purchase of a large number of switches and routers to greatly expand their network, because of the strain put on their system by URL filtering.[105] A Verizon employee testified that the cost to implement URL filtering would be "well into seven figures," and WorldCom would be unable to use it altogether due to speed issues and hardware incompatibility.[106]

III. ANALYSIS

A. TECHNOLOGY ISSUES

It is tempting to think that the answer to problems involving technology is more technology. This often seems faster and easier then dealing with the underlying issues that caused the offending behavior in the first place.[107] While technology can make certain tasks easier,[108] it is not a replacement for careful planning and human oversight. In the quest for a magic solution to the spread of child pornography, Pennsylvania tried to use ISPs' resources to impact the greatest number of people with the least expenditure of capital.[109] The rationale likely went that if the Internet is allowing citizens to access child pornography then you simply cut off access and the problem is solved. Instead of investi-

104. As is shown by the commercials for competing ISPs which all tout their connection speed as a main reason to sign up. America Online, *AOL.com: AOL for Broadband- Make the Most of Your Online Experience* http://www.aol.com/price_plans/bfsbroadband.adp (accessed Apr. 23, 2005). Netzero, *NetZero Free Dial Up Internet Service - High Speed ISP - Net Zero Internet Provider - Netzero* http://www.signup.netzero.net/s/signup?r=learnmore_n (accessed Apr. 23, 2005). Earthlink, *Earthlink High Speed* http://www.earthlink.net/highspeed/ (accessed Apr. 23, 2005).

105. *Pappert*, 337 F.Supp.2d at 629.

106. *Id.* at 630. Apparently, the hardware needed to run URL filtering does not connect to the type of wiring that WorldCom uses.

107. This brings up yet another basic problem with the Act. There are clear difficulties with assigning criminal liability to one actor for the actions of another. Here, there is no allegation that employees of the ISP or the ISP itself is distributing or viewing child pornography. However, they were still liable to suffer the penalties for actions of a customer that it cannot control with any great success.

108. Specifically, the collection and categorization of large amounts of information. The problem is that solutions driven by technology are only as useful and accurate as their construction and programming. In this instance, the Pennsylvania Attorney General's office collected massive amounts of data in terms of the number of individual Web sites blocked. One of the problems with a system that collects so much information is that there is no readily apparent way to sift through the results for errors. The basic design of the measures used by the Attorney General was not only unconstitutional but also operated on a scale which ensured its failure.

109. *Infra* n. 110. The Pennsylvania criminal approach is unique in the online world. At its heart, it is an attempt to conserve resources and expend them in a way that has the widest possible impact. Going after individual users is a much more time and money consuming proposition. This plan is new on the Internet but not in the "real world."

gating individuals and asking their ISP to shut down the account, Pennsylvania tried to be proactive in stopping the crime before it occurred. In other words, law enforcement officials went one step up the supply chain and focused on the groups providing access instead of individual users or suppliers. Considering the financial and human resource constraints that law enforcement groups are in, this plan is appealing for a number of reasons.

Unfortunately, this approach has drastic shortcomings in the online world. A brick and mortar store selling obscenity or child pornography can be raided and the contraband removed thereby cutting off one means of access to the material.[110] Disruption caused to innocent businesses and individuals that surround the store is kept to a minimum and a clear warning is sent to potential future offenders. The operators of an offending Web site, just as if they owned the store above, might well be liable to criminal prosecution.[111] The majority of their customers however will forever remain anonymous or outside of competent jurisdiction.[112] A further complication for law enforcement is the reality that child pornography cannot be completely physically seized since other copies are almost assuredly floating through cyberspace somewhere.[113] Therefore,

110. *See e.g. New York v. Ferber*, 458 U.S. 747 (1982); *Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46 (1989).

111. In theory, the registered owners of a specific Web site could be charged with the distribution of child pornography if they had knowledge of the material on their site. This kind of criminal prosecution would be much more likely on smaller individual Web sites rather then a large Web hosting community with hundreds of thousands of pages such as Geocities or Terra. This is due to the overall size and scope of the larger Web hosting companies which make oversight much more complicated.

112. *See e.g.* Verifia, *NetGeo-Internet Geography Intelligence*, http://www.netgeo.com (accessed Mar. 7, 2005) (this company markets a product claiming that it allows Web site owners to detect where there visitors are located). There is definitely a market for such a service on a widespread level since it would help alleviate some problems of Internet jurisdiction. Substantial questions remain however including: cost of implementation, accuracy, privacy concerns, scalability, and interoperability. Finally, it is also a reality of the Internet and the limitations of human resources that the sheer number of Internet users makes tracking difficult. However, the use of Internet anonymizers and other similar techniques will often allow users to effectively shield their location and identity. While these techniques may not always be 100 percent effective, at a minimum they complicate investigations tracing individual users. A number of companies offer such products, including Steganosis and Stompsoft. Steganosis, *Steganosis, Freedom Online*, http://www.steganosis.com/?layout†efault&content=productssiapro&language=en (accessed Apr. 23 2005); Stompsoft, *StealthSurf X-treme, IP Blocker by StompSoft* http://www.stompsoft.com/stealthsurfextreme.html (accessed Apr. 23, 2005).

113. *See generally* National Center for Missing and Exploited Children, *National Center for Missing & Exploited Children*, http://www.ncmec.org (accessed Mar. 7, 2005). The unfortunate reality of child exploitation is that the mementos of abuse (i.e. photographs and video) tend to be traded over and over again among individuals all over the world. Normally, evidence of a crime is disposed of as quickly as possible. In this kind of crime however it is often copied for exchange with others thereby victimizing the child over again.

all law enforcement can realistically do, with the resources they have available, is minimize the number of locations where child pornography is available.[114] Problems begin however when legislative bodies try to help law enforcement by passing laws mandating the use of technology which is not viable either from an economic or technical standpoint.[115]

A state attempting to control erotic materials through blocking technology is nothing new. The medium has simply switched from cable and the telephone to the Internet. The two most famous examples of this are *Sable Communications of California v. FCC*[116] and *United States v. Playboy Entertainment.*[117] In the *Playboy* case, section 505 of the Telecommunications Act of 1996[118] was challenged on constitutional grounds.[119] This section of the Act required cable television operators to completely scramble or otherwise block channels dedicated primarily to sexually explicit material.[120] Otherwise the programming had to be restricted to hours when minors were unlikely to be watching television.[121] The impetus behind the legislation was that available scrambling technology was not perfect and occasionally "signal bleed" would occur,[122] enabling non subscribers to see pictures or hear audio from an adult

114. While it may be frustrating, the most realistic approach to combating online child pornography seems to be working with ISPs and Web hosting companies to limit the number of Web sites where child pornography is available. Unfortunately, those who strongly desire such material will go to great lengths to get it. However, law enforcement can make it a dangerous search as seen by the FBI's Operation Candyman. FBI, *FBI -Operation Candyman* – http://www.fbi.gov/pressrel/candyman/candyman home.htm (accessed Apr. 23 2005).

115. Courts have generally been unwilling to impose solutions, technological or otherwise, which would impose a huge burden on an industry. This is especially true when there are other less intrusive ways of achieving the same goal. As discussed below, some of the suggested techniques for blocking Web sites are not practicable since they would be extremely expensive to implement and would degrade the quality of service. Furthermore the current state of technology limits the available modes of compliance. As the field advances new techniques may be developed that are better suited to block individual Web sites without blocking others in the process.

116. 492 U.S. 115 (1989).

117. 529 U.S. 803 (2000).

118. 47 U.S.C. § 561.

119. Specifically, Playboy successfully argued that that the statute was an unconstitutional content based restriction on the freedom of speech because other less restrictive measures were available. *U.S. v. Playboy*, 529 U.S. 803, 815 (2000).

120. *U.S. v. Playboy*, 529 U.S. 803, 804-806 (2000).

121. *Id.* at 806. This time frame was from 10 P.M. to 6 A.M. according to administrative regulations. This technique is commonly referred to as "time channeling."

122. Signal bleed occurs when one channel runs into another. Much like being able to hear parts of two different radio stations at once, signal bleed on television means that part of one channel can be seen on an adjoining channel. In this particular case, the allegation was that some of the content from the Playboy Channel could be seen on channels that had not been blocked. Therefore, even if an objectionable channel was blocked, it still might be visible on other channels. FTC, *How to Prevent Viewing of Objectionable Television Pro-*

channel for a few moments.[123] Due to technological and economical restrictions, cable operators chose to "time channel" adult programming rather then rely on imperfect technology which could leave them legally liable.[124] The decision goes into a thorough analysis of the current state of scrambling technology and how it impacts the First Amendment due to the Act's content based focus.[125] The court explicitly stated that adults have the right to receive erotic material and that it is up to parents, not just the distributor of the material, to take steps to restrict their children's exposure.[126]

In other words, technology is not a panacea for all ills resulting from adult content. Instead it is a tool, albeit an imperfect one at times, for individual users to determine what is and is not appropriate for them and their family. Just as in the case at hand, the court in *Playboy* recognized that legislature bodies can not wish technology into existence and then demand that providers use it.[127] They also may not require an expenditure of money so large that it would destroy the health and growth of an entire industry.[128]

Under similar reasoning, the courts in *Sable Communications vs. FCC*[129] and *Fabulous Associates, Inc. v. Pennsylvania Public Utility Commission, et al.,*[130] refused to require adult service providers to spend enormous amounts of money to comply with a law that strictly limited the dissemination of constitutionally protected material. This is especially true when other less intrusive methods of control were available to the State and individual citizens. The courts also rejected other mandatory measures such as requiring consenting adults to obtain spe-

---

grams http://www.fcc.gov/cgb/consumerfacts/objectionabletv.html (last updated Mar. 3, 2002).

123. *Playboy*, 529 U.S. at 808.

124. *Id.* at 809.

125. *Id.* at 811-816.

126. *Id.* at 826.

> It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act.

Id.

127. *Id.* at 806.

128. As explicitly discussed in the *Sable* and *Fabulous* decisions, the court in *Playboy* appeared at least cognizant of the financial strain put on producers of adult materials by the regulation in question. Time channeling, special access codes, or special authorizations all inflicted, or would have, serious economic harm to a legal and constitutionally protected industry. *Playboy* at 808.

129. 492 U.S. 115 (1989).

130. 896 F.2d 780 (1990).

cial access codes for adult material.[131] The overall message of *Sable, Playboy,* and *Fabulous Associates* is that the courts will not allow a total ban on erotic content, nor will it allow the heavy handed use of technology where less restrictive means exist, especially when available at the user level.[132]

B. Free Speech and Due Process Problems

The Pennsylvania statute and others like it raise a number of problems relating to the First Amendment and due process. Any governmental restriction on expression, especially by a criminal statute, will be closely scrutinized for constitutional flaws.[133] These problems are only exacerbated by the current state of technology and the inability to block individual Web sites with precision.[134] Due to the nature of the Pennsylvania statute[135] and methods of compliance, these conflicts were virtually assured from the outset. Specifically, the problems relate to: the over blocking of innocent Web sites resulting in the suppression of protected speech, the permanent blocking of Web sites, and the seizure of property all without due process.

1. *Freedom of Speech*

Pennsylvania's Attorney General's Office admits that it is very easy to block a large number of innocent Web sites using techniques such as IP filtering.[136] Due to the current state of technology as discussed above, ISPs ordered to block access to specific Web sites will also by necessity block a large number of other unrelated sites.[137] This means that a

131. *Fabulous Associates v. Pennsylvania Public Utility Commission,* 896 F.2d 780, 789 (1990).

132. *See Playboy,* 529 U.S. at 822-826; *Sable,* 492 U.S at 124-125, and *Fabulous,* 896 F.2d at 788-789 (In these cases, the court clearly recognized the fact that individuals bear the ultimate responsibility to take action on their own and make decisions on what is and is not morally acceptable. Rather than simply banning the production or distribution of the material, the courts have sought to utilize a combination of industry self regulation and user action.).

133. *See R.A.V. v. City of St. Paul, Minnesota,* 505 U.S. 377 (1992) (showing the difficulty of using criminal laws to limit even speech which is generally not constitutionally protected).

134. This is because there can be no clear explanation or justification for why Web sites were blocked if it was unintentional. Any restriction of speech, even if not legally considered speech for reasons of constitutional analysis, must be done with great care and supporting evidence. The problem in this situation is that such evidence does not exist for the large number of Web sites which were blocked despite not having any connection to child pornography. *Pappert* at 650.

135. Specifically, the potential criminal penalties for non compliance acting as an additional pressure on ISPs. *Pappert* at 619.

136. *Pappert,* 337 F. Supp.2d at 632-633.

137. *See supra* III(A) (discussing technology issues).

large number of Web sites will be shut down for containing child pornography despite being completely innocent. There has been no assertion that the sites blocked by accident also contained child pornography or were otherwise involved in illegal activity.[138] They simply happened to share a second level domain name[139] or IP address with a targeted site. This is an unconstitutional restriction of free speech on an enormous scale.[140]

As a general rule, any content specific suppression of speech by the Government is presumptively invalid.[141] Child pornography however is not afforded Constitutional protection due to its contraband nature.[142] If the only Web sites blocked by the Pennsylvania Attorney General's office were those that contained child pornography there would be no problem. Complications arise however when Web sites which contain protected speech are also blocked.[143] Some of the over blocked sites may have had erotic, but constitutionally protected, content while others were completely unrelated to adult material.[144] These two kinds of Web sites

138. *Pappert,* 337 F. Supp.2d at 632-633.

139. A "second level" domain name is that part of an URL which is most recognizable to Internet users. For example, in http://www.yahoo.com, "yahoo" is the second level domain name. This is especially important in this context because some kinds of filtering focus only on this more general part of the address instead of the complete URL. This in turn leads to over blocking. For example, if there is an individual page at http://www.geocities.com/anonymous_user/index.html that needs to be blocked, IP filtering and DNS filtering would block all requests for http://www.geocities.com regardless of the sub domain. Therefore, every individual Web site at geocities would be blocked instead of just the targeted Web site.

140. Any governmental action based on the content of its message is highly suspect to begin with. In most cases the Government can at least argue that there is a specific reason why they seek to restrain the message. In this instance however a large number of innocent Web sites have been condemned without any determination of their content, cursory or otherwise. Not only has the Pennsylvania Attorney General's office unconstitutionally banned certain Web sites, but also a number of other sites that they have never seen. *Pappert* at 650.

141. *Simon & Schuster, Inc. v. Members of N.Y. State Crime Victims Bd.*, 502 U.S. 105 (1991); *Consolidated Edison Co. of N.Y. v. Public Serve. Comm'n of N.Y.*, 447 U.S. 530 (1980); *R.A.V. v. City of St. Paul, Minnesota*, 505 U.S. 377 (1992).

142. As held in *New York v. Ferber,* 458 U.S. 747 (1982) there is no need to go through the balancing act of *Miller v. California*, 413 U.S. 15 (1973). Instead, child pornography is a separate category apart from obscenity and may be proscribed entirely regardless of where it is found. This is because the freedom of speech is not unlimited and there are certain categories of expression which are not legally considered "speech" because the content has exceedingly slight, if any, social value. A Classic example of this is the "fighting word" doctrine from *Chaplinsky v. New Hampshire*, 315 U.S. 568 (1942).

143. The problem of over blocking is not only one of inconvenience. It places an unconstitutional burden on protected speech because unrelated Web sites are blocked along with those targeted by the Attorney General. *Pappert* at 650.

144. Again, there is no way to know exactly which Web sites were banned and therefore it is impossible to say what content they contained. Just as is true with the Internet as a

are subject to different levels of control by the Government but neither may be entirely proscribed especially without a judicial determination of some kind.[145] In effect, Pennsylvania has silenced the speech of a large number of individuals without legal authority or justification.[146]

Enforcement of the statute also poses a problem regarding the prior restraint of speech. Over the years, the courts have taken a very dim view on the constitutionality of any governmental attempt to restrain speech before it even happens.[147] This is especially true if there are no procedural safeguards built into the censorship scheme. "The teaching of our cases is that, because only a judicial determination in an adversary proceeding ensures the necessary sensitivity to freedom of expression, only a procedure requiring a judicial determination suffices to impose a valid final restraint. . .."[148] As *Freedman v. Maryland* and its progeny make clear, before there is any hope of a constitutional prior restraint of speech the government must go through the minimum steps required by due process. Specifically, there must be notice given to the affected party and a chance to be heard by an impartial third party.[149] Here, neither of the basic requirements was met. The process followed by the Pennsylvania Attorney General's office in seeking to block Web sites changed

---

whole, some of the Web sites may have had sexually explicit themes while others did not. It would be impossible to say that each of the accidentally blocked Web sites also contained child pornography and therefore their blocking was inconsequential. *Pappert* at 650.

145. *See generally Miller v. California*, 413 U.S. 15 (1973); *New York v. Ferber*, 458 U.S. 747 (1982); *Roth v. U.S.*, 354 U.S. 476 (1957). It is black letter law that purely expressive speech receives the greatest amount of First Amendment protection. *Id.* While not without some limitations, citizens' right to free expression has consistently been upheld and protected against Government suppression and regulation. Pornography is also protected speech, but is subject to more control then other kinds of speech. *Id.* What is addressed in almost every case dealing with Government controls on pornography is the question of how you are allowed to do it, not if. *Id.*

146. The actions of the Pennsylvania Attorney General's office affect two distinct groups of Web sites. First are those specifically targeted for blocking because they allegedly contained child pornography. As discussed in this article, there are a number of Constitutional flaws in the process used. But at least there was an established process. The second group of Web sites were those blocked by accident because of the defects in available technology. For these Web sites there was no process of any kind. They simply fell into a black hole for Pennsylvania users and disappeared from the Internet. If this kind of collateral damage to innocent third parties happened in the real world, massive civil lawsuits would quickly follow. If hundreds and thousands of neighboring shops were also randomly shut down because of one individual store violating the law, the public outcry would be overwhelming. In the online world it is a bit more difficult however because there was no immediate notice of the Attorney General's actions. *Pappert* at 641.

147. *Cantwell v. Connecticut*, 310 U.S. 296, 306 (1940); *Texas v. Johnson*, 491 U.S. 397, 408 (1989).

148. *Freedman v. Maryland*, 380 U.S. 51, 56 (1965) (laying out the required steps in due process for the review and possible censoring of films).

149. *Logan v. Zimmerman Brush Co. Et Al.*, 455 U.S. 422, 426 (1982) (citing *Mullane v. Central Hanover Bank & Trust Co.*, 339 U.S. 306 (1950)).

during their enforcement of the statute.[150] At first a court order was obtained requesting affected ISPs to block a Web site. Then a more informal process was used, bypassing the court entirely and going straight to the ISPs.[151] Neither of these approaches can be considered sufficient as safeguards of constitutional rights. Even when the Attorney General's office obtained a court order requiring an ISP to block a Web site the owner of the Web site was not notified of the hearing or given the opportunity to present an argument. They could not tell the Judge why their Web site should not be blocked nor was there any clear process to appeal such a decision.[152] In the second and more informal process even the minimal protections afforded were taken away.[153]

As noted in Plaintiff's brief,[154] there are direct parallels between the case at hand and earlier state attempts at controlling unpopular speech. In *Near v. State of Minnesota*[155] the state government was attempting to suppress the publication and dissemination of a "malicious, scandalous and defamatory newspaper, magazine or other periodical."[156] According to statutory language the crime was in continuing the production of a suppressed publication after the Court had determined it to be a public nuisance. In other words, the offending act was a violation of a court order, not the actual publication itself.[157] Conviction of this offense was punishable by a fine of not more then $1,000 or by imprisonment in the county jail up to twelve months.[158] Not only did the statute punish individuals for the expression of their ideas but also permanently barred them from publishing other "scandalous" materials as well as conducting

150. *Pappert,* 337 F. Supp.2d at 619-620. As discussed both above and below, the Attorney General's office changed their approach to enforcing the statute after receiving complaints from the affected ISPs. *Id.* At first they obtained a court order directing the ISPs to block specific Web sites. *Id.* Later they simply gave the list of targeted Web sites to the ISPs and bypassed a formal hearing altogether. *Id.*

151. *Pappert,* 337 F. Supp.2d at 620.

152. *Id.* at 619, *supra* n. 58.

153. However, the reason the Attorney General went to a more informal approach was at the request of various ISPs. The ISPs felt they would be unable to comply with the court order in the amount of time permitted by statute. Worldcom on the other hand was worried about their legal liability for blocking a Web site without the authority of a court order. This again points out the weaknesses inherent in the statute. The deficient process used to obtain a court order, as weak as it was, remained the only protection provided at all. In response, the Attorney General did at times give ISP additional time to comply with the court order although the legal effect of these actions on the validity of the court order is unclear. *Pappert* at 623.

154. Center for Democracy and Technology, *Free Speech Online*, http://www.cdt.org/speech/pennwebblock/040105PAPlaintiffs.pdf (accessed Mar. 7, 2005).

155. 283 U.S. 697 (1931).

156. *Id.* at 700.

157. *Id.* at 703.

158. *Id.* at 700.

business of any kind under the name of the banned publication.[159] This meant that if a publication was deemed to have run afoul of the law the name of that publication, in this case "The Saturday Press," was forever barred.[160] Even if the newspaper or magazine changed its focus and began publishing weather forecasts or baking recipes, it could not keep the name.[161]

The *Near* court's statutory interpretation strikes similar notes to issues raised by the Pennsylvania law.[162] Instead of seeking to punish the actual lawbreakers, the goal was the suppression of ideas because the state viewed that as the more efficient and meaningful remedy.[163] The nature of the Internet combined with its exponential growth has left authorities in the difficult position of trying to enforce laws against people with unclear identities or locations.[164] So instead of going after individuals, Minnesota and Pennsylvania attempted to cut off the means of access to the offending material.[165] In both cases however, that approach led to the unconstitutional suppression of protected speech through prior restraint.[166] One of the flaws of the Pennsylvania scheme was that there was no effective way to monitor the subsequent changes to any of the blocked sites.[167] Just like the newspaper name "Saturday Press," once a Web site has been banned, it will theoretically remain so forever regardless of current content.[168] This means that any subsequent operator of the site will have fallen into a black hole of suppression from which there is no apparent escape.

The issue of prior restraint raised by the Pennsylvania statute also has striking similarities to a line of cases involving the sale of allegedly obscene books. In *Bantam Books, Inc. v. Sullivan et al.*,[169] the state of

159. *Id.* at 700-701.

160. *Id.* at 703.

161. *Near v. State of Minnesota*, 283 U.S. 697, 702 (1931).

162. Specifically, the legislation sought to permanently ban the use of certain names and addresses or other means of locating and accessing the information associated with it.

163. *Near*, 283 U.S. at 704.

164. *Supra* n. 112. As discussed earlier, the geographical location and identity of individual users can be exceedingly difficult to determine due to the decentralized nature of the Internet. *Id.*

165. Minnesota tried to ban an entire newspaper and Pennsylvania tried to restrict access to targeted Web sites. Neither state sought out individual users of the available information. Instead they attempted to shut off the method of distribution.

166. As the *Near* court makes clear, the instances when prior restraint is constitutional is very narrow and not subject to widespread use. *Near* at 716.

167. *Pappert*, 337 F. Supp.2d at 656-657.

168. *Id.* at 643. Plaintiffs bought and re-registered one of the blocked domain names and turned it into a site explaining the current case and issues at hand. CDT, *Little-Angel.tv BANNED IN PENNSYLVANIA!*, http://www.little-angels.tv (accessed Nov. 28, 2004).

169. 372 U.S. 58 (1963).

Rhode Island had established a "Commission to Encourage Morality in Youth."[170] The Commission had nine members appointed by the Governor and had the authority to: investigate questionable situations which might lead to misbehavior, educate the public of these situations, and recommend legislation and prosecution to eliminate the problems.[171] Appellants in this case were publishers who had received at least thirty-five notices from the Commission that certain titles of theirs had been deemed "obscene" and therefore could not be sold in Rhode Island.[172] The notices thanked appellants for their cooperation and usually reminded them of the Commission's duty to recommend the prosecution of purveyors of obscenity.[173] The Commission used the power of its official sanction to suppress the sale and distribution of a wide range of material without any prior judicial determination of it being obscene.[174] Just as in Pennsylvania, someone other then a Court with competent jurisdiction was in charge of deciding what was and was not obscene or contraband.[175] There was no due process in the sense of an adversarial procedure where affected parties could challenge the designation. Instead, in both cases decisions were made ex-parte with no input from the purported lawbreakers.[176]

---

170. *Id.* at 61.

171. *Id.*

172. *Id.* at 61-62. In response, the publisher sent associates to try and gather any remaining copies of the banned work that were still for sale rather then risk criminal prosecution. *Id.* at 63.

173. *Id.* at 62.

174. While the "Commission" was enacted by state legislation it was not a judicial body and possessed no authority to ultimately determine where the line stood between obscenity and pornography. *Id.* at 71.This task has proven exceedingly difficult even for the Supreme Court. The balancing tests involved are nearly impossible to articulate and are not well suited for use by lay persons.

175. In this case it was a panel of citizens appointed by the Governor. *Id.* at 61. In Pennsylvania it was members of the Attorney General's office. *Pappert* at 632. Neither had the authority to make final determinations of what is and is not obscenity or child pornography.

176. *Id.* at 65-66. Specifically the Court held that:

> In thus obviating the need to employ criminal sanctions, the State has at the same time eliminated the safeguards of the criminal process. Criminal sanctions may be applied only after a determination of obscenity has been made in a criminal trial with the procedural safeguards of the criminal process. . .There is no provision whatsoever for judicial superintendence before notices issue or even for judicial review of the Commission's determinations of objectionableness. The publisher or distributor is not even entitled to notice and hearing before his publications are listed by the Commission as objectionable.

Id. Just as in the case of *Pappert*, there was no adversarial process where affected individuals could make a case for themselves. Nor was there a process to reverse the Web site's designation as containing child pornography.

2. *Property and Due Process*

The first question asked in any due process analysis is if the interest involved is one that is recognized under the Fourteenth Amendment.[177] The language of the Amendment states that a person may not "be deprived of life, liberty, or property, without due process of law;"[178] so the first step is to determine if in fact there was a person being deprived of one of the protected interests. As discussed earlier, a large number of innocent Web sites were blocked by the actions of the Pennsylvania Attorney General's office. Some of these domain names were owned by individuals and others by companies.[179] The question then is whether or not an owner of a Web site holds a property interest in the affected domain name. The most clearly reasoned analysis of the question comes from the case of *Kremen v. Cohen*.[180] In *Kremen*, the registrant and owner of http://www.sex.com was deprived of his interest in the domain name by a con man[181] named Stephen Cohen. Having just recently gotten out of prison, he sent Network Solutions[182] a letter he had supposedly received

177. *See generally Logan v. Zimmerman Brush Co. et al.*, 455 U.S. 422 (1982); *Board of Regents of State Colleges et al. v. Roth*, 408 U.S. 564 (1972); *Bolling v. Sharpe*, 347 U.S. 497 (1954); *Graham v. Richardson*, 403 U.S. 365 (1971). If not, then the analysis is over. There have been a number of cases regarding exactly what qualifies under each of the three main categories of life, liberty, and property.

178. U.S. Const. amend. XIV.

179. *U.S. v. Amedy*, 24 U.S. 392 (1826); *U.S. v. Brownfield*, 130 F.Supp.2d 1177 (C.D.Cal.S.Div., 2001); *Charlotte, C. & A.R. Co. v. Gibbes*, 12 S.Ct. 255 (1892) (both holding that a corporation may be treated as a person for the purpose of legal action including jurisdiction and constitutional protections).

180. 337 F.3d 1024 (9th Cir. 2003). However the Supreme Court of Virginia, in a case of first impression, held that an interest in a domain name is not liable to garnishment because it is a contractual right that is bound to the services provided by the domain name registrar. *See Network Solutions, Inc. v. Umbro Int'l Inc.*, 259 Va. 759 (2000). The court in *Kremen* obviously contradicts the holding of the Virginia court but cites to Network Solution's oral argument before the Virginia court stating that a domain name constitutes property. *Infra.* n. 190.

181. *Kremen et al. v. Cohen et al.*, 337 F.3d at 1026 (9th Cir. 2003). Just before sending the letter in question, Mr. Cohen was serving time for impersonating a bankruptcy attorney. *Id.*

182. Network Solutions, *Your homepage for domain name registration, web site design, web hosting, web site promotion* http://www.networksolutions.com (accessed Mar. 23, 2005). Network Solutions was one of the first and largest registrars of domain names. There is some debate over how and why they were selected as the first registrar. Ross Wm. Rader, *One History of DNS* http://www.byte.org/one-history-of-dns.pdf (accessed Apr. 23, 2005). While domain names are no longer free, they are still relatively inexpensive to register through an accredited registrar such as Network Solutions or GoDaddy. Go Daddy Software, *Domain Name Registration, Domain Transfers. Your domain name search setarts here* http://www.godaddy.com (accessed Apr. 25, 2001). Along with a number of other services, Network Solutions can: register domain names, transfer registrations of existing domain names (as is the matter of controversy here), broker the sale of domain names and otherwise manage accounts of domain name registrants. Network Solutions, *Your*

from Mr. Kremen's company as the owner of the URL.[183] The letter stated that the company had been forced to fire Mr. Kremen but had not gotten around to changing the administrative contact information for the domain name from Mr. Kremen to another employee.[184] The letter further stated they were abandoning the domain name and had no objections to Mr. Cohen registering and using it.[185] Apparently, Network Solutions did not find it odd that the owners of the Web site, a company named Online Classifieds, did not have an Internet connection available to send the letter themselves. Instead, they supposedly sent this letter to a third party with no apparent relationship to the company who just happened to be interested in the domain name as well.[186] Despite the obviously fraudulent nature of the letter, Network Solutions deleted the registration of Mr. Kremen and transferred it to Mr. Cohen. It came as no surprise that Mr. Cohen was difficult to find when the lawsuit was filed and it is believed that he eventually escaped to Mexico.[187] So Mr. Kremen pursued his claim by suing Network Solutions, among others, for conversion of property by giving the rights to the domain name to Mr. Cohen.[188]

The *Cohen* court goes into an in depth examination of the nature of a property right and concludes that an interest in a domain name does in fact qualify as a property right.[189] Interestingly, Network Solutions has basically said, in other lawsuits, that they believe such a right to exist.[190] A three part test was applied by the court to determine the existence of a property interest in a domain name. "First, there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have es-

---

homepage for domain name registration, web site design, web hosting, web site promotion http://www.networksolutions.com (accessed Mar. 23, 2005). There are a number of registrars accredited through the Internet Corporation for Assigned Names and Numbers (ICANN). ICANN, *ICANN,* http://www.icann.org (last updated Sept. 24, 2004). ICANN is a joint public/private global organization that is responsible for maintaining the Domain Name System as well as some other issues that relate directly to the allocation and management of domain names.

183. *Kremen*, 337 F.3d at 1026.

184. *Id.*

185. *Id.*

186. *Id.*

187. *Id.*

188. *Id.* at 1028.

189. *Kremen*, 337 F.3d at 1028-1033.

190. *See Network Solutions, Inc. v. Umbro Intl. Inc.*, 259 Va. 759, 769-770 (2000) (stating that Network Solutions admitted at oral argument that an interest in a domain name qualifies as a type of intangible personal property); *Network Solutions, Inc. v. Clue Computing, Inc.*, 946 F. Supp. 858 (D. Colo. 1996).

tablished a legitimate claim to exclusivity."[191] As the court correctly reasons, a domain name satisfies each of these elements, all of which are closely intertwined. A domain name is a well defined interest since the owner makes virtually all decisions regarding the content, shape, and nature of the Web site.[192] Also, when someone owns a domain name no one else may use it and all visitors are on clear notice that the specific address is being used by an identifiable party. Finally, domain names are no longer free to register[193] and have been traded, bought, and sold for large sums of money the same as any other kind of property.[194]

So if individual citizens and companies do have a property interest in their domain names, the Pennsylvania government took the property without any due process or payment in return.[195] When the Pennsylvania Attorney General's office forced an ISP to block a Web site, it effectively destroyed the property interest of the owner. This is especially troubling when considering the issues of over blocking discussed earlier. Even for those Web sites which were singled out there was no Due process protection. The clearest analogy is, again, that of a real world brick and mortar store or residence. If the state of Pennsylvania padlocked a building with no judicial process it would be a matter of minutes before protests were made, lawyers hired, and lawsuits filed. Just because an action occurs online does not convert if from illegal to legal. There still must be a balancing of interests done to determine what kind of process is owed to the property owner.[196] As the court held in *Fuentes v. Shevin*:[197]

> The constitutional right to be heard is a basic aspect of the duty of government to follow a fair process of decision making when it acts to deprive a person of his possessions. The purpose of this requirement is not only to ensure abstract fair play to the individual. Its purpose, more

191. *Kremen*, 337 F.3d at 1028 (quoting *G.S. Rasmussen & Assoc., Inc. v. Kalitta Flying Service, Inc.*, 958 F.2d 896 at 903 (9th Cir. 1992)).

192. *Kremen*, 337 F.3d at 1028.

193. *See generally* Network Solutions, *Your homepage for domain name registration, web site design, web hosting, web site promotion*, http://www.networksolutions.com (accessed Mar. 7, 2005); GoDaddy, *Domain Name Registration, Domain Transfer. Your domain name search starts here*, http://www.godaddy.com (accessed Mar. 7, 2005).

194. *Kremen*,. 337 F.3d at 1028.

195. *U.S. v. Miller*, 317 U.S. 369, 373-374 (1943); *Lucas v. South Carolina Coastal Council*, 505 U.S. 1003, 1014 (1992) (stating that governments may not take property without fair compensation). It could be argued that the property rights of the owner were not completely destroyed by the state. Pennsylvania would argue that it was a partial taking at most since some parts of the country would still have been able to reach the Web site. The question then is if the restrictions on the interests of the property owner are severe enough to be considered a governmental taking. This determination is made on a case by case basis. *Penn Cent. Transp. Co. v. City of New York*, 438 U.S. 104, 123-125 (1978).

196. *Carey v. Piphus*, 98 S.Ct. 1042 (1978).

197. 407 U.S. 67 (1972).

> particularly, is to protect his use and possession of property from arbitrary encroachment. . .So viewed, the prohibition against the deprivation of property without due process of law reflects the high value, embedded in our constitutional and political history, that was place on a person's right to enjoy what is his, free of governmental interference.[198]

Here, there was no notification of a hearing given to the owner of the domain names because either the hearing was purely ex-parte,[199] or there was no hearing at all.

The final issue involving a lack of due process involves the virtual "seizure" of the material on blocked sites.[200] Once a determination was made by the Attorney General's office that a site contained child pornography, notice was given to certain ISPs who then instituted a blocking procedure.[201] This in effect shut down that site, and possibly several hundred others that shared its IP address, rendering it inaccessible to citizens in Pennsylvania as well as other states that the ISPs serviced.[202] While it may be impossible to physically seize computer images and other information from a Web site, the effect is the same when a Web site is blocked and the content suppressed. Instead of law enforcement carting off books and magazines from an adult bookstore, the Attorney General's Office simply had the entire store permanently shut down.

The wholesale seizure of allegedly obscene materials before judicial determination of their nature has been held unconstitutional.[203] In *Fort Wayne v. Indiana,* the state of Indiana seized a large quantity of materials from an adult bookstore under a RICO[204] statute charging the store

198. *Id.* at 75.

199. *Supra* n. 57.

200. No physical items were seized during the enforcement of the Pennsylvania statute. However, for Web sites that sell virtual goods or run membership only areas, the actual content of the Web site itself are the confiscated goods. There are a number of different business models in the world of online commerce. Many commercial Web sites, dealing with both adult and mainstream content, maintain separate "members only" sections that can be accessed only after paying a fee. Other Web sites allow paying users to download content to their computer. In either case, the actual goods of the Web site exist in digital form and would be effectively seized by the blocking of the hosting Web site.

201. *Supra* nn. 60, 152. As noted earlier, this consisted either of an official court order or an informal notice. Both procedures were instigated by the Pennsylvania Attorney General's Office and listed Web sites that were to be blocked. *Id.*

202. Again, because of the nature of ISPs, the effect of this Act spilled over the Pennsylvania border and affected citizens of other states. As discussed above, ISPs are not able to differentiate users based on their physical location. *Id.* at 662-663.

203. *Fort Wayne Books, Inc. v. Indiana,* 489 U.S. 46, 66-67 (1989); *Marcus v. Search Warrant,* 367 U.S. 717, 731-732 (1961); *A Quantity of Copies of Books v. Kansas,* 378 U.S. 205, 210-211 (1964); *Lee Art Theatre, Inc. v. Virginia,* 392 U.S.636, 637 (1968).

204. 18 U.S.C.A. §§ 1961-1968. (1970). R.I.C.O. stands for Racketeer Influenced and Corrupt Organizations Act. *Id.* The RICO Act was passed in 1970 and was intended as a tool to use against the mafia's involvement in some otherwise legitimate businesses as well

with a pattern of selling obscene materials.[205] A trial court held an ex-parte hearing and entered an order allowing the seizure of all publications and personal property of those charged along with the padlocking of the store itself.[206] The court upheld the application of RICO charges to the Defendants but overturned the seizure of materials without due process.[207] Specifically, the Court points out that the wholesale pre-trial seizure of materials is prohibited. The court does allow the taking of some material but only for the narrow purpose of determining obscenity.[208] Put simply, the Supreme Court has held that a single copy of specific material may be seized, but the wholesale confiscation or destruction of the material without judicial process is unconstitutional.[209] The court makes it clear that while contraband can generally be seized even without a warrant, this does not necessarily authorize law enforcement to make determinations of what is and is not obscene or contraband.[210] As specifically stated by the court "mere probable cause to believe a legal violation has transpired is not adequate to remove books or films from circulation."[211] While contraband is legally distinguishable from both pornography and obscenity, it is not always possible to categorize each at first glance.[212] Therefore, the established procedure, or com-

---

as their method of banding together to act as an enterprise in the commission of illegal acts. *See generally* Jeff Grell, RICO ACT, Jeff Grell, Racketeer Influenced and Corrupt Organizations, RICO, Attorney at Law http://www.ricoact.com (accessed Apr. 23, 2005). One of the strongest parts of the RICO act is that it also allows the seizure of "any property constituting, or derived from, any proceeds which the person obtained, directly or indirectly, from racketeering activity or unlawful debt collection in violation of section 1962. The court, in imposing sentence on such person shall order, in addition to any other sentence imposed pursuant to this section, that the person forfeit to the United States all property described in this subsection." 18 U.S.C.A. § 1963(a)(3). In other words, any personal property that can be tied back to money earned through a RICO violation can be seized.

205. *Fort Wayne Books, Inc.*, 489 U.S. at 55.

206. *Id.*

207. *Id.*

208. *Id.* at 62. "In a line of cases dating back to *Marcus v. Search Warrant*, 367 U.S. 717 . . . (1961) this Court has repeatedly held that rigorous procedural safeguards must be employed before expressive materials can be seized as 'obscene.'. . .pretrial seizures of expressive materials could only be undertaken pursuant to a 'procedure designed to focus searchingly on the question of obscenity"

209. *Id.* at 57. *See also New York v. P.J. Video, Inc.*, 475 U.S. 868, 873 (1986) and *Lo-Ji Sales, Inc. v. New York*, 442 U.S. 319, 327-328 (1979).

210. *Fort Wayne Books, Inc.*, 489 U.S. at 57 (1989).

211. *Id.* at 58.

212. *See generally Roth,* 354 U.S. 476; *Miller*, 413 U.S. 15; *Ferber*, 458 U.S. 747. As is seen in the difficulties the Supreme Court has had in distinguishing obscenity from pornography and what guidelines should be used. *Id.* The amount of confusion generated by this issue makes it clear that such determinations, as much as possible, should be left to the court system and not individual non judicial actors. Some materials will very clearly fall into one category or another but oftentimes the lines are unclear at best.

plete lack thereof, clearly violates the due process requirements of the Constitution as well as aspects of the First Amendment right to free speech.

C. Commerce Clause Issues

There can be no question that Pennsylvania's desire to limit the sexual exploitation of children by blocking the viewing of child pornography is an entirely legitimate and compelling state interest.[213] The terrible effects that the production of such materials has on the children involved has been well documented and widely reported.[214] However, even taking this interest into consideration is not enough to save the statute from being unconstitutional.

The Internet poses unique problems for those states that attempt to regulate criminal behavior occurring online.[215] When faced with such a horrible crime, the legislature tried to graft old legal theory onto new methods of communication.[216] While Pennsylvania may have intended to regulate the behavior of only its citizens, the effects of the bill had much further reach and violated the Dormant Commerce Clause.

It has been long settled by the Supreme Court that the Federal Government's sole authority to control commerce between the states[217] also involves a "Negative" or "Dormant" Commerce Clause that inhibits individual state's ability to do the same.[218] If the statute in question discriminates against out of state commerce on its face, it is invalid.[219] When discrimination occurs through the operation of the statute then strict scrutiny applies.[220] If the statute in question only "incidentally" burdens interstate commerce then the statute will be upheld unless the burden is clearly excessive in relation to the benefit enjoyed by the

213. See *Ginsberg v. New York*, 390 U.S. 629 (1968); *ACLU v. Johnson*, 194 F.3d 1149 (10th Cir. 1999); *Reno v. ACLU*, 521 U.S. 844 (1997). The devastating impact that sexual exploitation has on children is widely reported. *Id.* In virtually every case dealing with the interaction of minors and pornography or obscenity the court has clearly stated that the protection of children from sexual abuse and exploitation is a compelling state interest. *Id.*

214. *See generally* The National Center for Missing and Exploited Children, *National Center for Missing Exploited Children*, http://www.ncmec.org (accessed Nov. 28, 2004).

215. Tyson, *supra* n. 42.

216. *Supra* n. 1. Pennsylvania tried to approach the problem of online child pornography in much the same way as they would deal with distribution of contraband in the physical world. *Id.* As noted above, the track record of state regulation of sexually explicit material online is very poor. *Id.*

217. U.S. Const., Art. I, § 8, cl. 3.

218. *Cloverland-Green Spring Dairies, Inc. v. Pa. Milk Mktg. Bd.*, 298 F.3d 201(2000); *Pike v Bruce Church, Inc.* 397 U.S. 137 (1970); *Healey et al. v. The Beer Institute Et al.*, 491 U.S. 324 (1989); *Hughes v. Oklahoma*, 441 U.S. 322 (1979).

219. *Shafer v. Farmers Grain Co.*, 268 U.S. 189, 199 (1925); *Pike v. Bruce Church, Inc.*, 397 U.S. 137, 142 (1970).

220. *Pappert*, 337 F. Supp.2d at 660.

state.[221] The *Pappert* court analyzed the Pennsylvania statute under the balancing test of *Pike Church* and determined that it impermissibly regulated interstate commerce.[222]

In *Pappert*, the court came to the realization that the methods chosen by the Pennsylvania legislature and Attorney General's Office not only are overbroad, but unfortunately also grossly ineffective:

> This Court also concludes that the burdens imposed by the Act are clearly excessive in relation to the local benefits. Defendant claims the Act is justified by reducing the sexual abuse of children. However, as discussed, defendant did not produce any evidence that the Act effectuates this goal. . . .To the contrary, there have been no prosecutions of child pornographers and the evidence shows that individuals interested in obtaining or providing child pornography can evade blocking efforts using a number of different methods.[223]

Therefore, the benefit realized by the State is very small if it exists at all.[224] When weighed against the cost imposed on interstate commerce, this statute had no chance of surviving even the most generous of readings under *Pike*.[225]

While child pornography itself is obviously not "commerce," Pennsylvania's method of combating it focused on the very heart of online commerce itself the ISPs and Web site owners.[226] Some courts have begun to truly grasp the problem of state regulation of the Internet and its impermissible national, and international, impact on commerce.[227] ISPs are not like utility companies in their ability to partition their customers based on location because ISPs often have customers in more then one state.[228] A local electric or energy company can easily comply with the

---

221. *Id.* at 661 (quoting *Pike v. Bruce Church*, 397 U.S. at 142).

222. *Pappert*, 337 F. Supp. 2d at 660-662.

223. *Id.* at 660.

224. The only argument that Pennsylvania could make is that there was some small benefit realized when users were unable to access blocked Web sites which formerly contained child pornography. This would be impossible to quantitatively measure in any accurate way and as the court notes, individuals were easily able to circumvent the restrictions. *Pappert* at 654.

225. The *Pike* balancing act requires that there be a benefit to government action before it can be measured against its burden. The court here clearly held that there was little to no benefit. Therefore, the statute could not possible offset the burden placed on interstate commerce. *Pappert* at 654.

226. Pennsylvania's approach focused on the ISPs who make a large part of the commercial aspect of the Internet, both in the buying and selling of goods as well as the commerce aspect of the Internet itself, possible. *Pappert* at 612.

227. *American Libraries Assn. v. Pataki*, 969 F.Supp. 160 (S.D.N.Y. 1997), *American Booksellers Foundation v. Dean*, 342 F.3d 1149 (10th Cir. 1999).

228. *See* America On Line, *AOL's Worldwide Services* http://www.aol.com/info/international.adp (accessed Mar. 7, 2005). ISPs such as MSN and AOL serve customers worldwide. *Id.* An ISP may have a subscriber's billing address on file and therefore have an idea in which state they are likely based. *Id.* However, there are still multiple problems with

laws of their state and there is no reason to be concerned about differing regulations in neighboring states. But because of the nature of the Internet, ISPs for the most part are unable to tell where a particular user is accessing its services from. This is due to the fact that users are not assigned IP numbers based on their geography but instead by the order upon which they logged on to the Internet.[229] Therefore, An ISP has no idea whether a user is signing in from Pennsylvania, Ohio, New Mexico, or even from across the globe.[230] This means that subscribers in other states are unable to access certain Web sites due to determinations made by the Pennsylvania Attorney General.[231] This is a very clear example of one state trying to export its domestic policies into other states. Citizens of other sovereign states and nations, with no relation to Pennsylvania, suddenly found themselves limited in what they can see and read regardless of their own local standards.[232]

The Attorney General's actions also directly affected domain name owners.[233] As discussed above, the technological steps ISPs were forced to take resulted in massive over blocking.[234] That means that an astronomical number of innocent Web sites suddenly disappeared from the Internet because of a Pennsylvania statute.[235] These actions interfered

---

assuming that an ISP can sort customers by location. Apart from the technical and resource limitations, customers are able to sign in from anywhere in the world regardless of where their credit card bills are sent. Also, an ISP can not realistically be asked to interpret laws and implement a plan for each state and country that their users might access the Internet from. Furthermore, each state has multiple District Attorneys who would likely have the authority to exercise their personal discretion in bringing a criminal action. This would result in uncertainty and chaos on an enormous scale and shows why state based legislation of the Internet does not make sense from a legal or public policy viewpoint.

229. Marshall Brain, *How Web Servers Work*, http://computer.howstuffworks.com/-webserver5.htm (accessed Mar. 7, 2005).

230. *See* Martin Dodge, *The Geography of Cyberspace Directory – Mapping the Internet*, http://www.cybergeography.org/mapping.html (accessed Mar. 7, 2005). This may change in the future as technology increases and Internet geographical services grow in sophistication and utility; *see also* Verifia *supra* n. 112. At the present time, however, ISPs are not set up to track and record the physical location of each user that signs on.

231. As seen in this case, when faced with possible criminal sanctions ISPs will implement the blocking procedure as widely as possible. While it is grossly ineffective and unconstitutional, it protects them from prosecution. *Pappert* at 636-637.

232. This is the very essence of the problem regarding state based Internet legislation. ISPs are forced to over block in order to satisfy statutory requirements. This in turn puts an individual state in charge of what foreign citizens may access. Customers of these ISPs who live in Ohio or Minnesota are restricted to the local standards of obscenity in Pennsylvania, not in their home state. *Id.* at 662-663.

233. This is discussed in detail in the Due Process section of this article. *Supra* (B)(2).

234. *Pappert*, 337 F. Supp.2d at 639-641.

235. *Id.* The court goes through a detailed listing of the over blocking caused by specific actions taken by the Pennsylvania Attorney General's Office. *Id.* One expert testified that the number of innocent Web sites blocked was upwards of 1,200,000. *Id.* at 641.

with innumerable commercial enterprises from online store fronts suddenly gone dark to personal Web sites posted by paying customers.[236] Also, the over blocking led to advertisers paying for ads that cannot be seen by potential customers in a number of markets.[237]

If stretched slightly further, this statute could mean that all ISP in the country are susceptible to Pennsylvania law even if they have no customers in the state at all. As discussed above, ISP do not exclusively handle the data of their users but instead pass it off to a number of other carriers and servers in order to efficiently complete the request.[238] Packets of information which make up the user's transmission might travel anywhere in the country or world on any number of different ISPs before arriving at its final destination.[239] It is unclear how broad of a statutory reading the Attorney General was contemplating, but his office's approach to the limited examples contained in this lawsuit suggest it is quite expansive.[240] Theoretically, every single ISP involved in transmitting data packets, for their subscribers or others, is criminally liable for "allowing access" to child pornography.[241] Especially in light of possible

236. While some companies provide free Web site hosting to users many others charge a fee for their services. Yahoo, *Web Hosting Services from Yahoo! Small Business* http://www.smallbusiness.yahoo.com/webhosting/ (accessed Apr. 23 2005). Even those that do not directly charge users raise revenue through placing ads on the users' pages. When innocent Web sites are blocked it means that customers are not getting the services they paid for since their Web sites are not available to a certain percentage of the public. Finally, the most clear cut example is that of online businesses which sell products and services. Without warning or explanation their store was suddenly shut down to a part of the population with no legal process or means for appeal.

237. *See* Interactive Advertising Bureau, *IAB Press Release 2/03/05* http://www.iab.net/news/pr_2005_2_22.asp (Feb. 22, 2005). Because of the nature of Internet advertising, individual Web sites being shut down affects the number of viewers a particular ad will have. Web hosting companies such as Geocities make money by selling ad space on members' pages. When Web sites suddenly disappear advertisers are not getting the amount of exposure for their products that they would have otherwise. While this may not seem to be a heavy burden in the case of a few individual pages, when hundreds of thousands go dark the cumulative effect quickly adds up. Also, since Web sites can be viewed from virtually any part of the world, the impact a well placed ad can have is invaluable in terms of national or global exposure.

238. Tyson, *supra* n. 39.

239. Franklin, *supra* n. 41. As discussed earlier, information packets travel the fastest route which is often not the shortest. Information packets might travel any number of different routes to its intended destination. *Id.*

240. For example, the Attorney General's office itself decided to call a Web site owner in Ohio and request that he remove specific pictures from his Web site which they believed to be child pornography. The site was devoted to nudism and included adolescents along with separate photographs of adults, all apparently in non-sexual contexts. The Web site owner complied with the request of the Attorney General's Office instead of facing possible criminal sanctions. *CDT v. Pappert*, 337 F.Supp. 2d 606, 620 (E.D.PA. 2004).

241. This is the point at which the slippery slope problem of the Pennsylvania statute turns into a free fall. Since a number of ISPs will handle the requests of a Pennsylvania

criminal penalties, including jail, ISPs are going to err on the side of extreme caution and block anything requested of them and sort out the results later, if at all.

D. Federal and State Laws

So if Internet regulation at the state level is unconstitutional and ineffective, and federal attempts have proven similarly fruitless then what is left? The answer is to find a balance between recognizing the challenges and features of the Internet and utilizing existing legislation in a more efficient and practical manner. Finally, the methods of law enforcement agencies have to evolve in order to save time and money as well as prosecute criminals.

One central issue with the Internet is that the choices made about its original structure have been responsible for many headaches in the legal community.[242] Some of the original reasons behind the construction of the Internet have made it maddeningly difficult to govern.[243] However, the reasons that make regulation complicated are the same reasons why the Internet is so important and will only continue to grow. While the Internet has been compared to many things, one of its main features is that it gives millions of individuals the modern day equivalent of a personal printing press.[244] Just as Johannes Gutenberg's innovations with the movable type printing press lowered the cost of printing and made it affordable to the masses,[245] so has the

---

user, each of those ISPs could be described as allowing access to child pornography. *Id.* at 613-614.There is nothing readily apparent in the statute that would shield them from legal liability despite being even further removed from the distribution or consumption of proscribed material.

242. *See* Lawrence Lessig, *Code and other laws of cyberspace* (Basic Books 2003). Professor Lawrence Lessig has written extensively about the construction of reality in the online world and how early choices shape subsequent options. Also, as is described earlier, the Internet developed in leaps and bounds with very little regulation after the initial push to create Arpanet. *Supra* n. 47.

243. Tyson, *supra* n. 39. The original underpinnings of the Internet were designed without geography and boundaries in mind. Instead they were built to move information in an efficient way that was secure from the threat of nuclear attacks in a way that phone lines and other modes of communication were not. This also means that tracking users on the Internet can be difficult. While certainly not impossible, determining normally simple issues such as who has jurisdiction can become extremely complicated.

244. *See* Perseus Development Group, *Online Surveys from Persues – The BLogging Geyser* http://www.perseus.com/blogsurvey/geyser.html (accessed Apr. 23, 2005). Instead of personal paper journals, individuals now can put their most private thoughts and experiences on the Internet to share with the world. The low price of maintaining a Web page means that any person with even slight computer knowledge can have their own virtual corner of the world replete with pictures and text for the cost of a monthly access fee.

245. Mary Bellis, *Johannes Gutenberg- Printing Press*, http://inventors.about.com/library/inventors/blJohannesGutenberg.htm (accessed Mar. 7, 2005); The Great Idea Finder,

Internet. Hosting companies such as Geocities have provided a way to distribute information on an unrivaled scale and made it available to anyone with access to the Internet.[246] It has attracted users from every corner of society and the world at large. While this global exchange of ideas has brought many benefits it is also precisely what has made controlling the Internet extremely troublesome.

In the end, no one law alone will be able to address all the issues regarding the Internet and the legal problems it presents. Pennsylvania tried to deal with the problem of child pornography by choking off access to the material instead of going after either the suppliers or consumers. While this is a novel idea, it is unworkable at this time for many of the reasons addressed above. However, this statute being struck down does not make child pornography any more legal to produce, distribute, or consume.[247] Just because the original child pornography statute does not specifically mention the Internet does not mean it cannot apply to those using the Internet to break the law. The Internet does pose unique legal challenges, but it does not require us to shred the entire Criminal Code in attempts to bring justice.[248]

There seems to be a real dichotomy between the approaches to handling Internet related criminal cases. Generally speaking, no law enforcement group wants to handle these issues because of the expense and difficulties involved. However, once a successful prosecution has occurred or the media focuses on the issue everyone wants to get involved. The trick would seem to be in developing a network of resources that is capable and responsible for handling these issues in order to spread out the burden. Part of the answer lays in the various law enforcement agencies working together more efficiently. Any time an issue falls under

---

Printing Press History – Invention of the Pringing (sic) Press, http://www.ideafinder.com/history/inventions/story039.htm (last updated July, 2004).

246. Of course, just because a Web site is available to the entire world does not mean that anyone will actually read it. However, the Internet has changed the concept of economy of scale just as Gutenberg did. To mail a thousand fliers promoting a business or point of view involves spending money to make the fliers and the pay for the postage. Online however, a Web site can be created for very little if any cost and it works around the clock. While this is of great benefit to many, it also is the reason why fraudulent e-mails and unsolicited bulk e-mail is so popular. *See* Richard Warner, *SPAM and Beyond: Freedom, Efficiency, and the Regulation of E-mail Advertising*, 22 John Marshall J. Computer & Info. L. 141 (2003).

247. 18 Pa.C.S.A. § 6312.

248. *See* FTC, *E-Commerce & the Internet* http://www.ftc.gov/bcp/menu-internet.htm (last updated Nov. 8, 2004). There is a necessary balance in applying law to the Internet between recognizing the unique nature of the Internet but at the same time determining what laws still easily apply to behavior online. Many of the frauds being perpetrated on the Internet are nothing more then old scams in new dressing. *Id.* Simply because the criminals are using the Internet as the means of communication does not mean that traditional rules of criminal law do not apply.

the control of more then once agency they become even more difficult because different people are doing the same work over and over. Also, inter-agency rivalries can prevent the efficient sharing of resources and knowledge.[249] Law enforcement then must learn to utilize the strengths of the Internet to use resources more efficiently.[250] Asking one or two federal agencies alone to police the Internet for child pornography clearly is impossible. The amount of available resources to any one group is simply not adequate. If there were more cooperation between local, state, and federal law enforcement groups however the problem would be less pronounced. The uniquely borderless nature of the Internet demands that petty fights over jurisdiction not be allowed to stall progress.

E. INDUSTRY SELF POLICING[251]

The adult industry is still treated as a dirty secret better not spoken of in public.[252] This leads to a lot of unnecessary misunderstanding and

249. Dan Verton, *Inadequate IT contributed to 9/11 intelligence failure* http://cio.co.nz; *search* Dan Verton (July 25, 2003). These kinds of turf wars are a large part of the recent push behind creating a national intelligence chief to oversee the various governmental agencies involved in intelligence activities. The September 11th attacks highlighted the need for improved interagency cooperation and the cessation of budget fights and jealousy between groups that should be working together.

250. *See e.g.* IFCC, *Internet Fraud Complaint Center*, http://www.ifccfbi.gov/index.asp (accessed Mar. 7, 2005). The IFCC is a joint effort between law enforcement and the private sector. Specifically, it is a joint creation between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C). *Id.* It also maintains close working ties with the U.S. Postal Inspection Service and the Internal Revenue Service. *Id.* The IFCC acts as a central data collection point where individuals can report instances of online fraud and criminal activity. *Id.* The group then parcels out the complaints to the appropriate law enforcement agencies as well as identifies and tracks overall trends of Internet fraud. *Id.* During the calendar year of 2003, the Web site received 124,509 complaint submissions and referred 95,064 of them to various agencies across the country. *Id.* Having one central contact point for citizens to report online crime can save countless hours of wasted effort on behalf of citizens as well as law enforcement. When online crime occurs, victims can find it difficult to figure out where they should complain. By using the IFCC Web site, citizens know that their cases are being referred to the correct groups. This also can reduce the strain on local police departments who do not have the resources or training needed to handle such complaints.

251. *See* Jose Ma. Emanuel, *Lessons From ICANN: Is Self-Regulation of the Internet Fundamentally Flawed?* 12 Intl. J.L.& Info. Tech. 1; David Johnson & David Post, *Law and Borders—The rise of law in cyberspace* 48 Stan. L. Rev. 1367; Jay P. Kesan & Andres A. Gallo, *Optimizing Regulation of Electronic Commerce* 72 U. Cin. L. Rev. 1497. Regulation of the Internet is a topic that has been covered fairly widely in both the mainstream media and academic journals. *Id.* Scrutiny has not been focused only on the adult industry but the idea of Internet self regulation as well as government regulation of the Internet in general.

252. This is the clear undercurrent of a number of the cases discussed in this article including: *Bantam Books at 65-66, Fort Wayne Books at 63-64, Playboy at 817-818, Fabulous at 783, Sable at 124,* Etc. The issue of adult material makes many otherwise

confusion. The reality is that no responsible producer of adult material wants minors to have access to its products.[253] For any producer to knowingly allow minors to purchase pornography would be financial and professional suicide. Simply put it is not worth the potential economic harm as well as the criminal investigation and prosecution that are sure to follow.[254] This is why reputable adult companies have taken steps to limit the access of minors to its Web sites while still being able to market their products to willing adults. For example, a number of companies use age verification services that charge users a fee in order to access individual Web sites which have contracted with the service.[255]

Playboy, as one of the largest publishers and distributors of adult material, maintains an extensive Web site that has an entire page specif-

---

rational people crazed. While there is a need to shield minors from pornography, the reality is that adults have the right to purchase and enjoy it. The courts in these cases all recognized that the world of erotic material does not fall completely outside the realm of legal protections. Sooner or later, the American public will have to accept that sexually explicit material is a fact of life instead of a source of constant embarrassment enjoyed only by deviants.

253. This is part of the reason for the proliferation of companies providing adult verification services as well as Web sites adding disclaimer pages requiring the user to acknowledge their consent to receive the adult content. *Infra* n. 255.

254. *See generally* Musicland, *Suncoast.com*, http://www.suncoast.com (accessed Nov. 28, 2004); Best Buy, *Best Buy*, http://www.bestbuy.com (accessed Nov. 28, 2004). Successful companies which produce or distribute pornography make incredible profits on each sale. *Id.* Taking the example of DVDs, the average price of recently released single disc DVDs is approximately $15.00 to $25.00. *Id.* Even if the price of pornographic DVDs is similar to main stream releases, the costs of production and publicity for pornography are a fraction of that spent on mainstream releases. Martin Grove, *Lower marketing costs not necessarily good news* http://www.hollywoodreporter.com/thr/columns/grove display.jsp?vnu_content_id=1000847860 (Mar. 22, 2005). (stating that the average marketing budget for Motion Picture Association of America members was $34.4 million in 2004) The enormous profits available in the sale of pornography are far too appealing to endanger by selling to minors. Also, law enforcement and the public at large have no tolerance for companies who knowingly sell pornography to minors. Criminal prosecutions, possibly including RICO charges, would be sure to follow.

255. Adult Check, *Adult Check: The World's Largest Adult Entertainment Network*, http://www.adultcheck.com (accessed Mar. 7, 2005) is one of the largest examples of an adult verification service. A basic ninety day membership costs $19.95, and a "Gold" membership is $24.95. *Id.* According to the Web site, a membership enables the user to access over 200,000 galleries of high quality adult material covering a broad spectrum of interests. *Id.* After signing up for a membership a user is assigned an ID and password which is then entered at individual sites to gain access. *Id.* Memberships are obtained primarily by credit or debit card through a Verisign secured transaction but can also be purchased by electronic check transfer or mail order. *Id.* Other similar services include: Tri-Tech Internet Service Inc., *CyberAge.com*, http://www.cyberage.com (accessed Mar. 7, 2005), NetVerifier, *Welcome to Netverifier we have thousands of hardcore xxx galleries*, http://www.netverifier.com (accessed Mar. 7, 2005), and Sexkey, *SexKey*, http://www.sexkey.com (accessed Mar. 7, 2005).

ically addressing the issue.[256] On the page, Playboy lists the IP addresses of its two Web sites as well as the machine names. Also, Playboy.com is rated with the Internet Content Rating Association ("ICRA").[257] The ICRA is an international organization that acts in a similar fashion to the Television rating system.[258] Unlike the Motion Picture Association of America,[259] the ICRA does not rate the content of Web sites.[260] Instead, individual users may voluntarily rate their site and submit it to the ICRA. The Web site will then carry the ICRA logo as a way for parents to judge how appropriate the site is for their children.[261] Furthermore, the ICRA both offers its own Internet filter and works with other filters to block access to registered sites that parents object to.[262] As with any kind of rating system, it only works when parents invest the time to utilize the software and monitor usage by their children.[263]

F. User self regulation

Ultimately, the individual users of the Internet have a responsibility to take steps to protect their own interests and safety. While law enforcement and the traditional governmental bodies will continue to have a role to play, individual citizens and families must play their part as well. Restricting access to pornography and other objectionable material is obviously a legitimate concern for parents and other individuals.[264]

256. Playboy Enterprises, *playboy.com / help / info for parents*, http://www.Playboy.com/help/parents.html (accessed Mar. 7, 2005).

257. ICRA, *ICRA: Internet Content Rating Association: Choice not censorship*, http://www.icra.org/ (accessed Mar. 7, 2005).

258. TV Parental Guidelines, *The TV Parental Guidelines*, http://www.tvguidelines.org/default.asp (accessed Mar. 7, 2005).

259. MPAA, *Motion Picture Association*, http://www.mpaa.org (accessed Mar. 7, 2005).

260. ICRA, *ICRA: Internet Content Rating Association: Choice not censorship*, http://www.icra.org/faq/abouticra/ (accessed Mar. 7, 2005).

261. *Id.* at http://www.icra.org/faq/abouticra/ (accessed Mar. 7, 2005).

262. The filter allows a parent to set different levels of access for different users in a household. Sites are grouped by their ratings and then may be allowed or disallowed on a categorical basis. http://www.icra.org/icraplus/help/differentrule.htm.

263. MPAA, *MPA Movie Ratings History*, http://www.mpaa.org/movieratings/about/content.htm (last updated Dec. 2000).

> The basic mission of the rating system is a simple one: to offer to parents some advance information about movies so that parents can decide what movies they want their children to see or not to see. The entire rostrum of the rating program rests on the assumption of responsibility by parents. If parents don't care, or if they are languid in guiding their children's movie going, the rating system becomes useless. Indeed, if you are 18 or over, or if you have no children, the rating system has no meaning for you. Ratings are meant for parents, no one else.

Id. (quoting Jack Valenti, President of the MPAA).

264. The inherent problem with asking the Government to decide what is and is not appropriate for your family is that every person has different standards and therefore what

However, when it comes to problems on the Internet, the Government cannot, and should not try to, solve every problem. It is every person's responsibility to decide whether or not to have Internet access in their home and what amount and kind of usage is acceptable by those in their household. While it often seems that the Internet is an unavoidable part of life, it is nothing more than a means of communicating information that you can choose to utilize, or not. The notion of the Internet as a world wide town square is cliché but accurate in many ways. People go online to communicate, exchange ideas, conduct business and countless other reasons that reflect the disparate interests and desires of human beings. As such, some of the ideas expressed are going to be crass, shabby, and objectionable to many people. However, as the Supreme Court has ruled in a long string of cases,[265] erotic material is protected under the First Amendment and can not be completely proscribed. As with any other means of communication, simply having access does not mean that all usage is suddenly acceptable or inevitable. There are a large number of options for those who wish to allow their kids on the Internet but worry about them being exposed to adult materials. Unlike the Government, parents do not have to worry about Constitutional challenges to their blocking methods due to over breadth or prior restraint. Techniques for restricting usage range from stand alone software programs, to built in parental controls, to restricting computer usage in general.[266]

IV. CONCLUSION

As can be seen by the string of failed Internet regulations on both the state and federal level, the time has come for a new approach. Individual state governments attempting to pass laws regulating the Internet have had virtually no success in surviving Constitutional challenges on grounds including: the First Amendment and Prior re-

---

is allowed in each individual home will, and should, vary. This strongly supports the fact that parents need to make their own decisions regarding what their children should be exposed to.

265. *Miller v. California*, 413 U.S. 15 (1973) and *New York v. Ferber*, 458 U.S. 747 (1982).

266. *See* TopTenREVIEWS Inc., *TopTenREVIEWS*, http://www.toptenreviews.com (accessed Mar. 7, 2005). Independent software programs include products such as: Content-Protect, CYBERsitter, and Net Nanny. For a review and comparison of these products, Services such as America On-Line (AOL) and other comparable ISPs provide "Parental controls" which help to limit the access minors have to adult material. Among other things, they will prevent minors from going into chat rooms that are designated as having adult content. It also has a filtering program which blocks access to specific Web sites that are believed to be adult in nature. Their, and a number of other companies, filtering software is handled by RuleSpace, Inc. at RuleSpace Inc., *The World's Leading Provider of Parental Controls* http://www.rulespace.com (accessed Mar. 7, 2005).

straint, due process in the seizure of property, and perhaps most technically difficult the Dormant Commerce Clause.[267] The states share many problems with the Federal government in trying to police a world that does not conform to traditional notions of jurisdiction and scope.[268] As discussed above, the courts have begun to realize the futile nature of regulating the Internet on a state by state basis. The first step towards an effective and rational Internet policy is to stop passing new laws. Especially on a state level, it is impossible to pass Internet related laws that do not violate any number of different Constitutional requirements.

Now that it has become clear that the Internet is not going to subside or disappear it is time to seriously consider the long term implications. While it might be wishful thinking, a new and clearly delineated national policy regarding the Internet and regulation is clearly needed. The current patchwork of federal and state groups, laws, and regulations has never been more confusing or difficult to navigate.[269] The strain on law enforcement and the legislature has come from the numerous lengthy court battles which have largely gone against attempts at regulation. Given the incredibly rapid expansion of the Internet, the haphazard series of erected dams is crumbling faster then can be replaced or repaired. Instead, it is time to undertake the daunting task of eliminating a large percentage of the laws which currently exist, and combine those that remain with a coherent national and international policy.[270]

There has been an enormous amount of hyperbole written about the

267. While First Amendment issues can be complicated, all speech is not afforded the same level of protection and certain types of speech may be banned entirely. *Pappert* at 649-650. If a statute could be very narrowly drawn it is possible that it could survive a challenge on Constitutional grounds. The Dormant Commerce Clause, however, is different. Until Web sites and ISPs are able to identify the geographic location of a user efficiently and with great assurance there is no way to limit statutory impact inside state lines. The Internet is as much an instrument of interstate commerce as the highways and waterways. Just as the courts have not allowed states to place an undue burden on this kind of commerce, they have not and will not allow them to do so to the Internet. *Pappert* at 661-662. *AmericanLibraries Assn. v. Pataki*, 969 F.Supp. 160, 183 (S.D.N.Y. 1997); *PSINet, Inc. v. Chapman* 362 F.3d 227, 239-240 (4th Cir. 2004).

268. Dan L. Burk, *Federalism in Cyberspace*, 28 Conn. L. Rev. 1095 (1996).

269. The explosion of online commerce has proven to be both a benefit and a burden to merchants. While it has allowed them to expand their market worldwide almost instantly, it has also raised concern of complying with numerous state laws as well as establishing jurisdiction in foreign locales. *See generally* Karen Sanzaro and David Keating, *Online Privacy Policies and Practices Under Fire* http://www.gigalaw.com/articles/2000-all/sanzaro-2000-03-all.html (Mar. 2000).

270. Specifically, many state laws simply need to be repealed. The Internet is clearly not amenable to horizontal regulation. Not only because of issues relating to the Commerce Clause, but also due to logistical and human resource limitations. *Supra* n. 267.

Internet in both the academic journals and the mainstream press.[271] While it is certainly true that the Internet has forever changed the way many people live, work, and shop it is not the first time that technological advancements have forced a fundamental shift in the way we approach writing laws. Eventually, just like every other innovation, the Internet will be regulated to some extant. The question then becomes how much and by whom. Ultimately the answer lies in a combination of: existing Federal legislation, increased cooperation between law enforcement agencies, Industry self policing, and user participation.

John Spence, Esq.†

271. In the past ten years or so it seems that the Internet has been a regular topic of discussion in every magazine, newspaper, and journal. A quick search in the archive of almost any news publication will yield multiple stories, surveys, and charts.

† John Spence is a solo practitioner in the state of Minnesota. B.A. May 1999, Hampshire College; J.D., May 2002, University of Cincinnati College of Law; L.L.M. expected in May 2005 from The John Marshall Law School. I would like to thank the editorial staff at the journal for their invaluable assistance as well as my family for all of their continued support.