

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA**

<b>AMERICAN CIVIL LIBERTIES UNION,</b>	)	
<i>et al.,</i>	)	
	)	
<b>Plaintiffs,</b>	)	Civil Action No. 98-CV-5591
	)	
v.	)	
	)	
<b>ALBERTO R. GONZALES,</b> in his official	)	
capacity as Attorney General of the United	)	
States,	)	
	)	
<b>Defendant.</b>	)	

**DEFENDANT’S POST-TRIAL  
PROPOSED FINDINGS OF FACT AND CONCLUSIONS OF LAW**

PETER D. KEISLER  
Assistant Attorney General

PATRICK L. MEEHAN  
United States Attorney  
RICHARD BERNSTEIN  
Assistant U.S. Attorney

THEODORE C. HIRT  
Assistant Branch Director  
RAPHAEL GOMEZ  
Senior Trial Attorney

ERIC J. BEANE  
ISAAC CAMPBELL  
JOEL McELVAIN  
KENNETH SEALLS  
JAMES TODD  
TAMARA ULRICH  
Trial Attorneys  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
20 Massachusetts Ave., N.W.  
Washington, DC 20530  
(202) 616-2035

Date: December 8, 2006

**TABLE OF CONTENTS**

	<b>PAGE</b>
<b>PROPOSED FINDINGS OF FACT</b> .....	1
<b>I. BACKGROUND</b> .....	1
A. Findings Concerning Scope of Litigation .....	1
B. Defining the Scope of COPA .....	2
C. The Plaintiffs in This Litigation Are Not Within the Scope of COPA .....	3
<b>II. STATUS QUO: CHILDREN’S EXPOSURE TO PORNOGRAPHY ON THE WEB</b> .....	6
A. The World Wide Web .....	6
B. The Use of Search Engines on the Web .....	9
C. The Use of HTTP Protocol on the Web .....	11
D. The Prevalence of Sexually Explicit Content on the Web .....	13
E. Children’s Exposure to Sexually Explicit Content on the Web .....	16
<b>III. FILTERING SOFTWARE OFFERS AN INADEQUATE SOLUTION TO THE PROBLEM</b> .....	18
A. The Architecture of Filtering Software .....	18
B. The Limited Effectiveness of Filtering Software .....	21
C. Other Problems with the Use (or Non-Use) of Filtering Software .....	32
D. The Inherent Limitations of Filtering Software Technology .....	34
E. Market Failure in the Filtering Software Industry .....	36
F. Professor Cranor’s Shallow Analysis is Entitled to No Weight .....	38
G. Testimony Regarding Enterprise Filtering Is Not Relevant .....	42

H.	Filtering Products Fail to Address Access to the Web from Mobile Devices .....	44
<b>IV.</b>	<b>COPA PROVIDES THE MOST EFFECTIVE SOLUTION TO THE PROBLEM .....</b>	<b>46</b>
A.	Credit Card Verification on the Web .....	46
1.	Minors Do Not Have Traditional Payment Cards Under Their Own Control .....	48
2.	The Existence of Non-Reloadable Gift Cards Does Not Undermine COPA’s Credit Card Affirmative Defense .....	51
3.	The Conclusions of Plaintiffs’ Payment Card Experts Are Not Supported by Their Reliance Material .....	52
B.	Micro-Payment Technology Facilitates the Purchase of Content .....	54
C.	Online Age Verification Services Are Highly Effective .....	56
D.	Implementation of COPA Will Not Materially Affect the Web .....	59
1.	Businesses Can Adapt to a Minor Regulatory Change in the Adult Entertainment Industry .....	59
2.	Consumers Are Adaptable and Increasingly Willing to Provide Personal Information on the Internet .....	61
3.	Commercial Web Sites Easily Can Comply with COPA .....	64
E.	COPA Provides a Worldwide Solution .....	65
1.	COPA Applies to Domestic and Foreign Websites .....	66
2.	Commercial Web Sites Can Tailor Their Sites to Different Geographic Regions .....	68
3.	The Majority of Commercial Pornography Comes from the United States, or Has Ties to the United States .....	69

<b>PROPOSED CONCLUSIONS OF LAW</b> .....	73
<b>I. STATUTORY INTERPRETATION</b> .....	73
A. COPA Contains Statutory Limits to Ensure That It Is Narrowly Tailored to Commercial Pornography on the World Wide Web .....	73
B. COPA’s Harmful-to-Minors Definition Narrowly Tailors COPA’s Restrictions to Material That Is Obscene for Minors .....	75
C. COPA’s Affirmative Defenses .....	82
<b>II. PLAINTIFFS LACK STANDING</b> .....	83
A. Web Site Plaintiffs Lack Standing .....	83
B. Non-Testifying Plaintiffs Lack Standing .....	85
<b>III. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON PLAINTIFFS’ FIRST AMENDMENT OVERBREADTH CLAIM</b> .....	87
A. Because COPA Regulates Only Commercial Entities, Intermediate Scrutiny Should Be Applied .....	88
B. COPA Satisfies Even Strict Scrutiny .....	90
1. Legal Standards .....	90
2. The Government Has a Compelling Interest in Protecting Minors .....	91
3. COPA Is Narrowly Tailored .....	92
4. Plaintiffs’ Arguments that COPA’s Narrow Tailoring Renders COPA Ineffective Are Without Merit .....	94

5. Plaintiffs' Argument that COPA Is Ineffective Because It Does Not Apply to Overseas Web Sites Is Incorrect as a Matter of Law . . . . . 98

6. COPA Is the Most Effective Way to Prevent Minors from Accessing Harmful Material . . . . . 99

7. There Are No Less Restrictive Alternatives to COPA . . . . . 101

a. The Private Use of Filtering Software Is Not a Less Restrictive Alternative . . . . . 102

b. Plaintiffs' Further Proposals Regarding the Use of Filters Are Not Less Restrictive Alternatives . . . . . 104

c. Prosecutions Under the Obscenity Laws, or Under Other Existing Laws, Are Not a Less Restrictive Alternative . . . . . 107

d. Plaintiffs' Suggestions for Narrowing the Application of COPA Would Undermine Its Effectiveness . . . . . 110

e. Educational Efforts Will Not Be as Effective as COPA in Protecting Children from the Exposure to Harmful Material . . . . . 111

**IV. JUDGMENT SHOULD BE GRANTED TO DEFENDANT ON COUNT TWO OF THE AMENDED COMPLAINT (ALLEGED VIOLATION OF OLDER MINORS' RIGHTS) . . . . . 113**

**V. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON  
COUNT THREE OF THE AMENDED COMPLAINT (VIOLATION  
OF THE RIGHT TO COMMUNICATE AND ACCESS INFORMATION  
ANONYMOUSLY) ..... 115**

**VI. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON  
PLAINTIFFS' FIRST AMENDMENT VAGUENESS CLAIM ..... 119**



F. Supp. 2d 473 (E.D. Pa. 1999). For ease of reference, citations to COPA herein will refer to its codification at 47 U.S.C. § 231.

3. Plaintiffs are either web site operators, none of whom have anything to do with the commercial display and distribution of pornography on the Web, or associations suing on behalf of members who operate or access web sites. Joint Ex. 1 at ¶¶ 2-29.

**B. Defining the Scope of COPA**

4. COPA defines “material that is harmful to minors” as “any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind” that is “obscene” or that:

(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

47 U.S.C. § 231(e)(6). COPA defines a minor as “any person under 17 years of age.” *Id.* at § 231(e)(7).

5. COPA’s commercial purposes definition limits COPA’s obligations to persons “engaged in the business” of distributing harmful-to-minors material. 47 U.S.C. § 231(e)(2)(A). Persons are “engaged in the business” only if they seek to profit from such material, and even businesses that seek to profit from harmful-to-minors material are not covered unless they do so

as a “regular course” of their business. *Id.* at § 231(e)(2)(B). COPA thus narrowly limits its obligations to businesses that regularly seek to profit from harmful material as a regular course of their business. By implication, an entity could not be prosecuted under COPA for the inadvertent, intermittent communication of material that the statute defines as harmful to minors.

6. These important qualifications reflect Congress’s intent to target commercial pornography. Congress stated:

Given that the scope of the bill is limited to commercial activity, and that the age verification system procedures prescribed under the bill represent standard procedures for conducting *commercial activity on pornographic Web sites*, the effect of the bill is simply to reorder the process in such a way as to require age verification before pornography is made available, essentially requiring the *commercial pornographer* to put sexually explicit images ‘behind the counter.’ The *commercial pornographer* is not otherwise restricted in his trade.

H.R. Rep. No. 105-775, at 15 (1998) (emphasis added). *See also id.* at 7 (“While legitimate U.S. businesses should remain free from unnecessary government regulation, the adult entertainment industry has traditionally been subject to restrictions because of the danger posed by pornographic material to children.”). Not surprisingly, the House Report repeatedly refers to those covered by COPA variously as “publishers of pornography,” “commercial purveyors of pornography,” and “commercial sellers of material harmful to minors.” *Id.* at 7, 14, 18.

**C. The Plaintiffs in This Litigation Are Not Within the Scope of COPA**

7. Plaintiffs represent a range of individuals and entities including speakers, content providers, and ordinary users on the World Wide Web (the “Web”), as that term is defined in the Act. Plaintiffs post content including, *inter alia*, resources on sexual health, safe sex, and sexual education; visual art and poetry; resources for gays and lesbians; online magazines and articles;

music; and books and information about books that are being offered for sale. Joint Ex. 1 at ¶ 2.

8. Six Plaintiffs had representatives testify at trial: Salon.com, Nerve.com, Condomania, Sexual Health Network, Heather Corinna, and Urban Dictionary. None of the other Plaintiffs testified at trial.

9. The following individuals also testified at trial: Alicia Smith, Barbara DeGenevieve, Marilyn Jaye Lewis, and Wayne Snellen. None of these individuals are Plaintiffs in the case, and none have claims before the Court.

10. Some of the Plaintiffs provide interactive fora on their Web sites, such as online discussion groups, bulletin boards and chat rooms, which enable users to create their own material on Plaintiffs' Web sites. Some of the verbal and visual exchanges that could potentially occur in these chatrooms or in the postings on their bulletin boards may include language or images that contain sexual content. Joint Ex. 1 at ¶ 3.

11. None of the Plaintiffs is a commercial purveyor of what is commonly termed "pornography." For example, Salon does not consider any material on its Web site to be pornographic. Salon does not fear prosecution under state harmful-to-minors laws and has not been threatened with prosecution under state harmful-to-minors laws or under federal obscenity laws. Testimony of Joan Walsh, at 175:6 – 176:21 (Oct. 23, 2006) ("Walsh Testimony"). When it established its web site in 1996, Condomania tried to make sure that it would not be associated with the pornography industry; it had no X-rated or pornographic images on its site. Testimony of Adam Glickman, at 164:4-12 (Oct. 30, 2006) ("Glickman Testimony").

12. No Plaintiff has demonstrated that his or her business, or any part thereof, is devoted to making harmful-to-minors communications for profit. Nor has any Plaintiff

demonstrated that it intends to make harmful-to-minors communications for profit as a regular course of its business. For example, Sexual Health Network's web site does not look like an adult entertainment site. Testimony of Dr. Mitchell Tepper, at 12:7-9 (Oct. 31, 2006) ("Tepper Testimony"). In fact, Dr. Tepper testified that the Sexual Health Network's mission is not to transmit pornographic material over its web site. *Id.* at 12:21-23.

13. All of the Plaintiffs express a subjective fear of prosecution under the statute. Joint Ex. 1 at ¶ 30.

14. Although some or all of the Plaintiffs purport to fear prosecution under the statute, these fears are without a substantial basis in fact. No Plaintiff has ever been contacted by state or local authorities, nor prosecuted nor arrested regarding any investigation into criminal violations. Joint Ex. 1 at ¶ 31.

15. The "speech" that Plaintiffs allege gives rise to their fear of prosecution does not contain any material that is designed to appeal or pander to a prurient (*i.e.*, shameful, morbid, or obsessive) interest in sex. For example, Sexual Health Network's mission statement reads: "The Sexual Health Network is dedicated to providing easy access to sexuality information, education, mutual support, counseling, therapy, healthcare, products and other resources for people with disabilities, illness or natural changes throughout the life cycle and those who love them or care for them." Tepper Testimony, 10/31/06 at 6:8-20; Def.'s Ex. 282 at 8-9. Similarly, Condomania's mission is to provide information, education and guidance for people to purchase condoms, and to learn about safer sex practices. Glickman Testimony, 10/30/06 at 95:2-10, 95:22-25, 138:7 – 141:20; Def.'s Ex. 169. The mission of Scarleteen, a web site operated by Plaintiff Heather Corinna, is "to provide sexuality information and education for young adults

and teenagers that is comprehensive, accurate and age appropriate.” Testimony of Heather Corinna, at 73:6-9 (Nov. 2, 2006) (“Corinna Testimony”).

## **II. STATUS QUO: CHILDREN’S EXPOSURE TO PORNOGRAPHY ON THE WEB**

### **A. The World Wide Web**

16. The Internet is an interactive medium based on a decentralized network of computers. Joint Ex. 1 at ¶ 78.

17. The primary method of remote information retrieval over the Internet today is the World Wide Web (“WWW” or simply “the Web”). The Web is a global information space operating over the Internet, which people can read from and write to via a variety of different Internet-connected devices, including for example, computers, Personal Digital Assistants (“PDAs”), and cellular phones. Testimony of Paul Mewett, at 94:9-20 (Nov. 7, 2006) (“Mewett Testimony”); Def.’s Ex. 82 at ¶ 8.

18. The Web is a service that operates over the Internet. The Web is the complete set of documents residing on all Internet servers that use the Hypertext Transfer Protocol (“HTTP”), which is the protocol specifying how hypertext will be moved around the Web. Mewett Testimony, 11/7/06 at 94:9 – 95:5; Def.’s Ex. 82 at ¶ 9.

19. The World Wide Web combines four basic components:

- a. Hypertext, that is the ability, in a computer environment, to move from one part of a document to another, or from one document to another, through internal connections among these documents (called “hyperlinks” or “links”);
- b. Resource Identifiers, that is the ability, on a computer network, to locate a particular resource (computer, document or other resource) on the network through a unique identifier;
- c. The Client-server model of computing, in which client software or a client computer makes requests of server software or a server computer that provides the client with resources or services, such as data or files; and

- d. Markup language, in which characters or codes embedded in text indicate to a computer how to print or display the text, *e.g.* as in italics or bold type or font.

Def.'s Ex. 82 at ¶ 10.

20. On the World Wide Web, a client program called a Web browser retrieves information resources, such as Web pages and other computer files, from Web servers using their network addresses and displays them, typically on a computer monitor, using a markup language that determines the details of the display. One can then follow hyperlinks in each page to other resources on the World Wide Web of information whose location is provided by these hyperlinks. The act of following hyperlinks is frequently called “browsing” or “surfing” the Web. Joint Ex. 1 at ¶ 79.

21. Web pages are often arranged in collections of related material called “Web sites,” which consist of one or more “Web pages.” Joint Ex. 1 at ¶ 80. Particular items of content on a Web site may be placed on a single Web page, or they may be placed on multiple Web pages. For example, an article on a news Web site can be broken up into two or more Web pages. Testimony of Dr. Edward Felten, at 58:14 – 59:1 (Oct. 25, 2006) (“Felten Testimony”).

22. To navigate to different pages on the Web, an HTTP request is sent to the Web server working at that IP address for the page required. In the case of a typical Web page, the HTML text, graphics and any other files that form a part of the page will be requested and returned to the client (the Web browser) in quick succession. The Web browser's job is then to render the page as described by the HTML and other files received, incorporating the images, links and other resources as necessary. This produces the on-screen “page” that the viewer sees.

Most Web pages contain hyperlinks to other relevant and informative pages and perhaps to downloads, source documents, definitions and other web resources. Joint Ex. 1 at ¶ 81.

23. A viewer typically will reach a Web page on the World Wide Web either by typing the address, or Uniform Resource Locator (“URL”), of the page into a Web browser, or by following a hypertext link to that page or resource. When the viewer does so, the server-name part of the URL is translated into an Internet Protocol (“IP”) address by the global Internet database known as the Domain Name System (“DNS”). This database stores all the registered domain names and associated IP addresses. When a user types in a domain name, the system looks it up and then uses the IP address that was found in the database. A domain name is the name that identifies one or more IP addresses on the Internet. The system allows people to refer to locations on the Internet by names, while the computers on the Internet can communicate by referring to each other as numbers. The IP address is the numerical identifier for a computer or device on the Transmission Control Protocol/Internet Protocol (“TCP/IP”) network. Mewett Testimony, 11/7/06 at 95:6-18; Def.’s Ex. 82 at ¶ 12.

24. The U.S. Census Bureau’s Current Population Survey’s results show that in September 2001, approximately 54 percent of the U.S. population was using the Internet from any location. That figure rose to 59 percent in 2003. Joint Ex. 1 at ¶ 97.

25. Some Web sites serve as a proxy or intermediary between a user and another Web page. When using a proxy server, a user does not access the page from its original URL, but rather from a URL on the proxy server. Joint Ex. 1 at ¶ 82.

26. Some Web sites will automatically open new windows that a user did not affirmatively take steps to access, or will re-direct the user to a different site altogether. Mewett Testimony, 11/7/06 at 141:7-21.

27. Some content from the Internet is now capable of being viewed on devices other than traditional personal computers. Examples include mobile devices such as mobile phones, personal digital assistants (“PDAs”) such as the Blackberry, portable audio/video players such as the iPod, and game consoles such as the XBox or PlayStation. Joint Ex. 1 at ¶ 96.

**B. The Use of Search Engines on the Web**

28. Modern search engines search for and index web pages individually. Search engines are Web sites that provide links to relevant Web pages, in response to search terms (words or phrases) entered by a user. They are a popular way of finding information online. Joint Ex. 1 at ¶ 83.

29. Most users interact with the Web by using a search engine. A search engine is a computer program designed to help find information stored on a computer system such as the World Wide Web. The search engine allows the user to request content that meets specific criteria (typically those containing a given word or phrase) and to retrieve a list of references that match those criteria. Joint Ex. 1 at ¶ 84.

30. The result of a Web search is usually a list of URLs with short explanatory summaries. Search engines do not search the Web; instead, they search regularly updated indexes to operate quickly and efficiently. Mewett Testimony, 11/7/06 at 96:8-15; Def.’s Ex. 82 at ¶ 14.

31. Search engines obtain their Web page listings in two ways. Web site operators may submit their own Web pages to the search engines, or the search engines may “crawl” or “spider” documents by following one hypertext link to another. The latter process returns the bulk of the Web pages and associated URL listings contained in search engine databases. Crawlers work by tracking and recording hypertext links in the Web pages that they index while crawling. A copy of each Web page visited is then stored on the search engine servers. These servers are generally located in server farms, and the major search engines may operate many thousands of these servers. When a user enters a query on a search engine via their browser, that query is sent to the databases on these servers. Mewett Testimony, 11/7/06 at 96:16 – 99:2; Def.’s Ex. 82 at ¶¶ 19-20.

32. The operators of Web sites can designate which pages on their sites they would like search engines to include in their indices. They do so by designating a particular file, known as a “robot.txt” file, which can be read by the search engine’s spiders. Web site operators can designate pages behind age verification screens to be indexed by the search engines. If such a page is returned in response to a query on a search engine, the viewer would be directed to an age verification page, or to the web site’s home page. Mewett Testimony, 11/7/06 at 98:25 – 100:6.

33. Search engines such as Google, MSN or Yahoo! Search, and directories such as Yahoo! Directory, give access to only a small part of the Web. This portion of the Web is often referred to as the Surface Web or the “Accessible” Web. The technology used by these conventional search engines does not provide access into a vast area of the Web called the Deep

Web, which is much larger than the Surface Web. Mewett Testimony, 11/7/06 at 100:7 – 101:1; Def.'s Ex. 82 at ¶ 16.

34. The Deep Web is composed of Web documents that are poorly indexed or not indexed at all by the broad-based conventional search engines. Pages on the Deep Web comprise a variety of materials, including dynamic content, databases, documents omitted because they are too large, pages protected by the author, and pages with restricted access. Mewett Testimony, 11/7/06 at 100:7-101:1; Def.'s Ex. 82 at ¶¶ 21, 23.

35. Most users of the Internet who start their typical surfing journey using a search engine will initially view the Surface Web. However, once links start to be clicked and the journey progresses, the likelihood of staying in the Surface Web diminishes. Def.'s Ex. 82 at ¶ 24. It is becoming more likely that users of the Internet will be steered to content in the Deep Web, for several reasons. Web content providers increasingly use dynamic content in their Web sites. In addition, some Web content providers use URL redirection to steer viewers from the URL that they intended to access to a different URL. Redirected content frequently is found in the much larger, less structured Deep Web. Def.'s Ex. 82 at ¶ 25.

**C. The Use of HTTP Protocol on the Web**

36. HTTP stands for hypertext transfer protocol; it is widely used on the Internet. Joint Ex. 1 at ¶ 110. Among the web sites that use primarily HTTP are *The New York Times*, *Washington Post*, and even Plaintiffs ACLU, Electronic Frontier Foundation, Electronic Privacy Information Center, and Salon Media Group. Joint Ex. 1 at ¶ 112.

37. FTP stands for file transfer protocol. It is used primarily to transfer files across the Internet. Joint Ex. 1 at ¶ 110. It serves a different purpose than does HTTP, and has been structured accordingly. Mewett Testimony, 11/7/06 at 174:22 – 175:6.

38. Most URLs use HTTP. Joint Ex. 1 at ¶ 113.

39. Numerous practical and technical obstacles will prevent a wholesale shift of Web sites from HTTP to FTP. Search engines are structured around HTTP, consumer search habits are deeply ingrained, and firewalls retard movement from HTTP pages to FTP pages because the protocols operate from different ports. For these reasons, it is unlikely that commercial Web sites would convert to the use of FTP. Mewett Testimony, 11/7/06 at 176:8 – 179: 24.

40. It is technically possible to convert a Web site delivered over the HTTP protocol to the FTP protocol. However, it is unlikely that all of the existing code on the site would work without modification. This is particularly true if the Web page has embedded CGI scripts, which are the most common way for Web servers and Web browsers to handle information from HTML forms on Web pages. Mewett Testimony, 11/7/06 at 178:4-25; Def.'s Ex. 83 at ¶ 25.

41. A Web site operator who wishes to convert his site from HTTP to FTP would likely need to maintain at least some of the pages on the Web site in HTTP, with traffic moving between the HTTP pages and the FTP pages. Mewett Testimony, 11/7/06 at 179:20-24; Def.'s Ex. 83 at ¶ 25.

42. There may be complications for the viewer if a Web site is converted to FTP. FTP requires specific ports, ports 20 and 21, to be left open to facilitate the connection. Some work environments, and even firewalls in domestic environments, may have these ports closed, rendering the Web site inaccessible. In addition, firewalls may time out during large data

transfers from FTP sites, causing an error to be generated. Mewett Testimony, 11/7/06 at 177:16 – 178:3; Def.’s Ex. 83 at ¶ 25.

43. Search engines index only HTTP sites, and so simply entering a search term in the search engine will not return an FTP site. A viewer would either need to know the exact address of an FTP site to access it, or the Web site operator would be required to maintain an HTTP site to direct viewers to the new site. Mewett Testimony, 11/7/06 at 176:2-15; Def.’s Ex. 83 at ¶ 27.

44. Security concerns would likely deter Web site operators from converting to FTP. That protocol is not designed for sharing sensitive information, such as payment transactions or other financial information. It is therefore likely that a commercial Web site operator who operates an FTP site would revert to the HTTP protocol for the purpose of processing sensitive information, rather than converting the web site entirely to FTP. Mewett Testimony, 11/7/06 at 179:10-24; Def.’s Ex. 83 at ¶ 28.

45. There are forms of content on the World Wide Web, such as streaming video, that are contained on files that do not use the HTTP protocol. However, this content can be found within larger Web pages that use the HTTP protocol. Further, a viewer could publicly access these forms of content over the Internet through the use of HTTP. Felten Testimony, 10/25/06 at 47:22 – 49:20. For example, streaming video files containing adult entertainment content are linked to adult entertainment sites on the World Wide Web. Testimony of Michael A. Russo, at 36:4-14 (Oct. 26, 2006) (“Russo Testimony”).

**D. The Prevalence of Sexually Explicit Content on the Web**

46. Adult material is widespread on the World Wide Web. The surface portion of the Web – that is, the portion of the Web that is capable of being indexed by search engines –

includes at least 25 billion web pages, and it is reasonable to estimate the Surface Web to contain 64 billion web pages. Mewett Testimony, 11/7/06 at 100:23 – 101:1. Approximately 1.1% of those pages are sexually explicit. Def.’s Ex. 65.

47. Thus, a very conservative estimate would find that there are at least 275 million, and as many as 700 million, sexually explicit web pages on the Surface Web alone. Mewett Testimony, 11/8/06 at 48:19 – 49:9.

48. Moreover, those Web pages are returned in response to queries on search engines more frequently than other pages are, and they are returned much more frequently in response to the most popular search engine queries. Def.’s Ex. 65.

49. The Deep Web – the portion of the Web that is not indexable by the search engines – is much larger than the Surface Web, and so the actual number of sexually explicit Web pages may be much higher. Mewett Testimony, 11/7/06 at 101:20 – 102:2.

50. The Web is also constantly growing. The Surface Web alone is growing by about 50 million Web pages per day. Mewett Testimony, 11/7/06 at 102:3-11.

51. Even seemingly innocent popular queries will return sexually explicit material. Testimony of Clover Taylor, at 183:14-24 (Nov. 1, 2006) (“Taylor Testimony”). For example, in the testing performed by Mr. Mewett (described in greater detail below), even innocuous queries such as “Online Games” and “Oops” returned sexually explicit material. Def.’s Ex. 82 at ¶ 57.

52. These are not the only examples of innocuous searches returning sexually explicit material. Envisional, a company that operates a search facility for companies that can detect online misrepresentations of their brands, performed a study on children’s toy brands. Its

search of the 26 most popular children's characters, including Pokemon, My Little Pony, Toy Story and Furby, revealed several thousand links to pornographic sites. Thirty percent of these sites featured hard core sexually explicit material. The remainder of those linked sites contained nudity, obscene language, or extreme violence. Def.'s Ex. 82 at ¶ 57.

53. Given the vast range of adult material available on the Web, it should not be surprising that fully one-quarter of children have been inadvertently exposed to sexually explicit material online. Pls.' Ex. 54 at 0169.

54. The majority of sexually explicit web sites are commercially driven. This is because those web sites have significantly higher bandwidth costs than do other web sites. The sexually explicit web sites can be categorized into two groups – “feeder” web sites, and membership web sites or “pay sites.” Both categories of adult web sites are likely to be commercially driven. Testimony of Dr. Matthew Zook, at 114:16 – 115:10 (Oct. 26, 2006) (“Zook Testimony”); Pls.' Ex. 29 at 4-5.

55. Sexually explicit web sites that offer subscription memberships often use feeder web sites as “bait” for the pay sites, and the feeder web sites profit from successfully guiding viewers to premium services on other web sites. Russo Testimony, 10/26/06 at 35:6-15. Affiliate fees from the membership web sites are the primary source of revenue for feeder sexually explicit web sites. Zook Testimony, 10/26/06 at 115:4-21; Pls.' Ex. 29 at 5.

56. Because of large bandwidth requirements, companies specializing in the adult industry, rather than traditional hosting services, generally host adult web sites. Because traffic to adult web sites can build quickly, hosting is generally the most significant cost to web sites. Zook Testimony, 10/26/06 at 117:11 – 118:3; Pls.' Ex. 29 at 6.

57. These hosting costs make the paid membership web sites essential to the functioning of a commercial Internet adult industry. The more content that is downloaded from a web site, the higher consumption of bandwidth. Without paid memberships, the Internet adult industry could not pay for the bandwidth that it consumes. Zook Testimony, 10/26/06 at 117:11 – 118:3; Pls.’ Ex. 29 at 6.

**E. Children’s Exposure to Sexually Explicit Content on the Web**

58. The World Wide Web is widely accessible by minors. According to a recent study conducted on behalf of the U.S. Department of Education, approximately 59 percent of all students (from nursery school through the 12th grade) use the Internet. Twenty-three percent of students in nursery school use the Internet, as do 32 percent of students in kindergarten, 50 percent of students in the 1st through 5th grades, 70 percent of students in the 6th through 8th grades, and 79 percent of students in the 9th through 12th grades. Def.’s Ex. 81 at 35.

59. In light of the widespread availability of the Internet, a parent cannot guarantee that his or her child will not have access to sexually explicit material, even if he or she were to take the drastic step of removing computers from the home. In addition to using the Internet in their own homes, 43 percent of all students use the Internet at school, 10 percent use the Internet at libraries, and nine percent use the Internet at other person’s homes. Def.’s Ex. 81 at 35.

60. Minors commonly are exposed to pornography on the Internet. One report has found that 25% of minors surveyed between the ages of 10 and 17 who regularly use the Internet inadvertently viewed pornography in the prior year. Another study noted that 70% of minors between the ages of 15 and 17 have accidentally come across pornography on the Web. Pls.’ Ex. 54 at 0161-62.

61. Minors who can read and type are capable of conducting Web searches as easily as operating a television remote. While a four-year-old may not be as capable as a thirteen-year-old, given the right tools (e.g., a mouse and browser software) each has the ability to “surf” the Web and will likely be exposed to harmful material. H.R. Rep. No. 105-775, at 9-10 (1998).

62. Even a child supervised by the best-informed and perceptive adult may be exposed to pornography by accidentally mistyping a web site’s address or by searching for common terms. Many web sites do not warn viewers of their harmful material prior to displaying it, setting a trap for even experienced Web surfers. H.R. Rep. No. 105-775, at 10 (1998); Mewett Testimony, 11/7/06 at 141:7-21.

63. In the “bricks and mortar” world, stores and enterprises that offer adult entertainment (e.g., video stores) often segregate the “adult” material for sale in their establishments by creating a separate room or section of their establishment with signs designating “Adult area,” with no one under a certain specified age permitted to enter. Establishments that sell adult magazines make special efforts to display adult magazines in a separate rack or area of the store, behind the counter, or behind special blinder racks for the purpose of compliance with various state “harmful to minors” statutes, including “display” laws. H.R. Rep. No. 105-775, at 10-11.

64. By contrast, purveyors of sexually explicit material on the World Wide Web often display many unrestricted and sexually explicit images to advertise and entice the consumer into engaging in a commercial transaction. H.R. Rep. No. 105-775, at 10.

65. Pornography sites are sometimes “mousetrapped” or programmed to make them difficult to exit. This practice involves the access by a viewer to a web page that is seemingly

harmless, but in fact contains adult material. The viewer is then precluded from clicking the exit button to leave the site; the viewer will then be automatically be directed to more adult sites rather than being allowed to leave. Mewett Testimony, 11/7/06 at 143:3-21.

66. Even if the drastic step of ridding the household of computers were taken, minors still would have access to harmful material from computers with Internet connections located in schools, libraries, retail outlets, and other people's homes, as well as Internet access over cell phones, personal digital assistants, and other electronic media. Def.'s Exs. 4 at ¶¶ 44, 81 at 25; Joint Ex. 1 at ¶ 96.

67. According to the National Research Council's [NRC] report, "it is probably not feasible [for parents] to provide constant supervision of [a] child's Internet access, especially as [the] child gets older." Pls.' Ex. 54 at 0251.

68. The NRC report concludes that, while parental supervision and education may be useful in part to counter the problem of minors' exposure to sexual materials on the Internet, "the expectations for such education and socialization should not be unrealistic." Pls.' Ex. 54 at 0398.

### **III. FILTERING SOFTWARE OFFERS AN INADEQUATE SOLUTION TO THE PROBLEM**

#### **A. The Architecture of Filtering Software**

69. Internet content filtering software programs attempt to categorize the vast array of all of the web pages available on the World Wide Web, and to block certain categories of those pages, including adult material. Joint Ex. 1 at ¶ 85.

70. Filters use two main approaches to attempt to do this, normally in tandem. The first approach uses a "black list" of known Web sites, areas within Web sites, or specific Web

pages. Outbound requests are checked against this list, and the software attempts to block the requested material if it matches the list. Mewett Testimony, 11/7/06 at 102:12 – 103:5; Joint Ex. 1 at ¶¶ 87-88. Some filters also use “white lists” of web pages that have been reviewed and determined not to contain objectionable content. Joint Ex. 1 at ¶ 89.

71. It is not possible for a black list to correctly categorize all of the content on the Web. The Web is growing too quickly, and is changing too quickly, for any person or entity to be able to compile a black list that will remain current. A black list cannot both accurately and thoroughly categorize the content of the entire Web. Mewett Testimony, 11/7/06 at 103:6-14.

72. Filters therefore use a second approach, called “dynamic filtering.” This process involves the automated checking of inbound data against keywords and/or phrases in an attempt to establish if that data contains content that contravenes the filtering rules. If it does, then the software attempts to block the data. Mewett Testimony, 11/7/06 at 103:18 – 104:4.

73. Dynamic filtering is an imperfect method for classifying the content of web sites, in part, because there is no residential filtering software that is currently available that is able to analyze and classify the images on a web page. Mewett Testimony, 11/7/06 at 144:6-19; Testimony of Dr. Lorrie Cranor, at 142:11-14 (Oct. 24, 2006) (“Cranor Testimony”); Def.’s Ex. 82 at ¶ 74(j).

74. Some filtering programs attempt to compensate for their inability to classify images by instead analyzing the file names that web site operators have assigned to the images in the computer code underlying their web sites. Operators of adult web sites, however, can easily prevent filtering programs from recognizing the images simply by assigning non-descriptive file

names, rather than names that identify the images as containing adult material. Mewett Testimony, 11/7/06 at 145:16 – 146:1.

75. Some filtering programs also attempt to compensate for their inability to classify images by analyzing the metadata, or underlying computer code associated with a web site, to determine the content of that web site. However, the operators of adult web sites frequently do not use metadata that would identify the site as adult. A large majority of the adult web pages that were identified in Mr. Mewett's and Dr. Stark's study did not have metadata. Mewett Testimony, 11/7/06 at 146:12-18, 147:8 – 148:1.

76. Filtering programs also attempt to compensate for their inability to classify images by analyzing the text of the web sites. A computer program, however, can only analyze the formal features of text. No purely formal method, like a computer program, can ever fully distinguish adult content from other content. A dynamic filtering program will result in significant underblocking, significant overblocking, or both. Testimony of Dr. Stephen Neale, at 28:1-13, 81:3-16 (Nov. 9, 2006) ("Neale Testimony").

77. The operators of adult web sites also use several methods that further complicate the operations of filtering software programs. In particular, they use a process called "URL redirection." In this process, the adult web site operator will use one web page which lacks any adult content, and thus would not be blocked by filtering software. A viewer who arrives at this web site will be automatically redirected to another web site, where the adult content resides. The web site operators can cycle the viewer through many of these adult web sites. The blacklist of the filtering software is incapable of identifying these adult web sites to which the viewer has been redirected. Mewett Testimony, 11/7/06 at 141:7-21, 142:8 – 143:2.

**B. The Limited Effectiveness of Filtering Software**

78. Internet content filtering software may be ineffective in two ways: underblocking and overblocking. Underblocking occurs when the filter fails to block content that would meet the filtering criteria (such as sexually explicit content). Overblocking occurs when the filter prevents access to material that does not meet the filtering criteria, resulting in the inaccurate blocking of, for example, political, social, and health-related Web sites. Testimony of Dr. Philip Stark, at 95:16 – 96:13 (Nov. 8, 2006) (“Stark Testimony”).

79. Paul Mewett and Philip Stark tested the rates at which various filter products underblock sexually explicit material, and at which they overblock non-explicit, or “clean,” material. In order to do so, Dr. Stark used scientifically sound methods to gather random samples of web pages found on the search engine indices of the Google and Microsoft corporations. He also used scientifically sound methods to gather random samples of queries that had been entered during particular one-week periods on three major search engines. The web pages that were returned to those samples of queries were also used in the testing. Def.’s Ex. 62 at 0002-03.

80. This use of random sampling methods allows the result of the testing on the web pages to be extrapolated to the full contents of the search engine indices, and to the full range of web pages that would be returned to queries entered on the various search engines. In contrast, the results of tests on filtering software by other entities cannot be extrapolated in this manner. Stark Testimony, 11/8/06 at 87:14-17, 126:7 – 127:10, 137:25 – 139:8, 141:20 – 143:5.

81. Mr. Mewett’s and Dr. Stark’s study also used the most recent data available. The results of their study are thus more reliable than the results of other, older studies; the Web is

changing rapidly and thus older data is of limited relevance today. Stark Testimony, 11/8/06 at 125:3 – 126:6.

82. Nine filtering products were tested in the study. Filters offered by ContentProtect, CyberPatrol, CyberSitter, and McAfee were tested because they had been rated by the online magazine TopTenReviews as the most effective filters on the market. Mewett Testimony, 11/7/06 at 106:23 – 108:1. The NetNanny and Norton filtering products were also tested, because they were also highly rated by the same magazine and because they are widely available in the marketplace. Mewett Testimony, 11/7/06 at 108:2-10. Filtering products offered by three Internet service providers – AOL, MSN, and Verizon – were also tested. Mewett Testimony, 11/7/06 108:11-16. (Two additional products were later tested in response to certain claims made by a rebuttal witness whom Plaintiffs had proffered, but chose not to call at trial. The results of the testing of those products were similar to the results of the tests of all the products. Pls.’ Ex. 260 at 3.)

83. Several of the filtering products offer different settings to specify the type of material that the user hopes to block and not to block. In his tests, Mr. Mewett used the settings that were designed to block sexually explicit material, without blocking non-sexually explicit material. He also tested the filters at their default settings, if the product offered a default setting; those default settings could include other categories to be blocked. Mewett Testimony, 11/7/06 at 121:12 – 122:9. The results of the testing for the various filters at both their default and their customized settings are comparable. Def.’s Exs. 68, 74, 78.

84. Mr. Mewett tested each of the filtering products against three types of data sets of web pages. First, as described above, he used sets of web pages drawn from the Google and

Microsoft search engine indices. The results of the testing against these web pages measure the effectiveness of filters against the full range of web pages that are available to be viewed. Stark Testimony, 11/8/06 at 86:25 – 87:17. Second, he used a set of web pages that were returned in response to random samples of queries that had been entered on to major search engines. The results of the testing against these web pages measure the effectiveness of filters against the type of content that web users typically see. Stark Testimony, 11/8/06 at 88:25 – 89:9. Third, he used a set of web pages that were returned in response to the most popular searches. The results of the testing against these web pages measures the effectiveness of filters against the type of content that web users would see most often. Stark Testimony, 11/8/06 at 92:21 – 93:4.

85. Each of these sets of data is relevant in assessing whether filters are effective. No one of the data sets, however, provides the full view; instead, the different sets provide complementary views. Stark Testimony, 11/8/06 at 93:5-10. In particular, the set of data regarding the most popular searches is relevant along with the other data sets, but does not provide the full picture. Children frequently use the Web for a variety of purposes, including research for school work, learning about news, and following sports. Def.'s Ex. 81 at 0040, 0042. Moreover, teenagers spend, on average, one to five hours per week surfing the Web. Pls.' Ex. 54 at 0192. It would therefore not be plausible to claim that minors use only the most popular search terms, and review no other web sites, when they surf the Web.

86. In order to test the various filters against each of the data sets, Mr. Mewett classified the web pages in all of the data sets into several categories, and used two of the categories for purposes of his testing. The first category included web pages that contained absolutely no sexual content or nudity. The web pages that fell into this category were tested to

determine whether filters overblock non-sexually explicit web pages. Mewett Testimony, 11/7/06 at 114:17-25.

87. The remaining web pages contained some reference, however remote, to sexual content or nudity. Plaintiffs' counsel has frequently referred to this category of web pages as "sex sites." *E.g.*, Closing Argument, 11/20/06 at 29:6-16, 48:5-6. This is a highly misleading description of this categorization. Mr. Mewett did not treat the pages in this category as "sex sites" or as adult sites for the purposes of his testing for underblocking. Instead, he created a subset within this category of only the web pages whose apparent primary purpose was only adult entertainment. These web pages were selected as representative of the types of web pages that a filtering product would attempt to block, if it were set to block sexually explicit content. The web pages that fell into this category were tested to determine whether filters underblock sexually explicit web pages. Mewett Testimony, 11/7/06 at 115:1-24. The selection of some of the 1,382 web pages that were included in this category, of course, required the exercise of some judgment; however, the vast majority of the web pages included in this category are unambiguous as to their primary purpose. Mewett Testimony, 11/7/06 at 118:9 – 119:2; 11/8/06 at 14:17- 15:17.

88. Not all of the web pages fell into these two categories. Web pages that contained some reference to nudity or some form of sexual content, but whose apparent primary purpose was something other than adult entertainment, were not included in either of these two testing categories. Mewett Testimony, 11/7/06 at 115:25 – 117:9. Mr. Mewett used several other categories, none of which formed the basis of the filter testing. One of those categories was denominated as "other"; contrary to Plaintiffs' suggestion, *see* Closing Argument, 11/20/06 at

32:5-11, this category did not represent only adult material or borderline adult material, but instead was a miscellaneous category that captured all of the material that did not fall into other categories. Mewett Testimony, 11/7/06 at 225:1-9; 11/8/06 at 53:4-15, 54:19 – 55:6, 61:24 – 65:2.

89. Mr. Mewett did not make determinations as to whether particular web pages in his adult entertainment category would qualify as harmful to minors under COPA. Mewett Testimony, 11/7/06 at 200:19-23. He could not have done so, because he is neither a prosecutor, a judge, nor a jury, and the process of coding web pages for his study is not the same as the process that the legal system would use in determining whether a web site operator has violated COPA. In particular, for the purposes of his coding, he reviewed only particular web pages, and not any broader context, as COPA would require. For example, a web page with a drawing of an erect penis and a reference to drawing “hot horny naked men all day long” was coded as adult entertainment, that is, the type of web page that a filtering program would be likely to attempt to block. Mewett Testimony, 11/8/06 at 25:1-9. This was done even if a broader context would make it unlikely that this particular web site would be deemed to be harmful to minors under COPA. Nonetheless, the vast majority of web pages classified as adult entertainment were unambiguous, and it is unlikely that any broader context would be relevant in determining whether those pages would be subject to COPA.

90. Dr. Stark performed a statistical analysis of the results of the testing of the filters against the “clean” and the “adult” web pages in each of the data sets. Def.’s Exs. 68, 74, 78. As explained below, those results reveal that, with respect to each of the sets of data, the filtering

products underblocked, or missed large portions of adult material, and that there was a direct correlation between the blocking of adult material and the overblocking of clean material.

91. With regard to the web pages drawn randomly from the search engine indexes, all of the filters missed large portions of the adult material. The Norton filter, in particular, missed no less than 54.2% of all of these adult web pages. The filter with the lowest underblocking rate, the AOL filter, still missed at least 8.6% of all of the adult web pages, and it achieved that result only by also blocking over 22% of the clean content. All of the rest of the filters missed at least ten percent of the adult pages, and some of them missed substantially more. There was a direct correlation between underblocking and overblocking; the less that a filter underblocked, the more it overblocked, and vice versa. Def.'s Ex. 68.

92. With regard to the web pages that were returned from a random sample of search engine queries, again, all of the filters missed large portions of adult material. The Norton filter, again, performed particularly poorly. All of the filters except one missed at least ten percent of the adult web pages; some, again, missed substantially more than that. The AOL filter still missed 6.2% of the adult content, and was only able to achieve that result by also blocking 12.5% of the clean content. Def.'s Ex. 74. In this data set, too, there is a correlation between lower underblocking rates and higher overblocking rates. Stark Testimony, 11/8/06 at 109:14-18.

93. All of the filters performed poorly with regard to "underblocking for queries," that is, the number of searches that retrieved at least one unblocked adult web page. This finding is particularly important, as it represents the frequency with which a minor entering typical

search engine queries will be presented with the risk of exposure to sexually explicit material. Stark Testimony, 11/8/06 at 110:24 – 111:14.

94. With regard to the web pages that were returned from the most popular queries, each of the filters continued to miss large portions of adult material. The *percentages* of adult material that were blocked were lower in this particular data set; most of the filters missed less than ten percent of the adult material. Def.'s Ex. 78. However, adult material was returned much more frequently in response to the most popular queries – adult web pages constituted 14.1% of this data set, as compared to 1.7% of the pages returned to typical searches and 1.1% of the pages drawn from the search engine indexes. Def.'s Ex. 65. Thus, in terms of *net amounts*, unblocked adult material was retrieved more frequently in this data set than in the others. Stark Testimony, 11/8/06 at 115:11 – 116:1. With respect to each of the filters, a significant number of queries returned at least one unblocked adult web page. Again, there was a correlation between underblocking and overblocking; the AOL filter, for example, blocked almost 20% of the clean pages in this data set. Def.'s Ex. 78.

95. Defendant's Exhibit 88 includes examples of adult web pages that were missed by at least three of the filters, and thus that would be available to be viewed by a minor even with the filters turned on. Mewett Testimony, 11/7/06 at 126:15 – 127:19.

96. Filters do not necessarily block a certain URL every time that that URL is entered into a browser. In other words, a claimed success rate of 80 percent in blocking sexually explicit content does not entail that 80 percent of all content is always blocked; instead, the same content may be blocked 80 percent of the time and allowed 20 percent of the time. Def.'s Ex. 82 at ¶ 74(e).

97. Plaintiffs presented a demonstrative exhibit at closing argument that they contended showed that adult content is unlikely to be viewed if the AOL filter is activated. No record evidence supports this contention. To the contrary, Dr. Stark directly explained that the type of calculation that plaintiffs attempted to perform was not a meaningful calculation. Stark Testimony, 11/8/06 at 177:13 – 178:17. In any event, even if that calculation was meaningful, it demonstrates, rather than refutes, the scope of the problem. Thirty-five million children use the Internet, and the majority of teenagers go online daily and spend 1-5 hours per week surfing the Web. Pls.’ Ex. 17 at 0002; Pls.’ Ex. 54 at 0192; Def.’s Ex. 81 at 0003. Thus, even if Plaintiffs had succeeded in calculating the likelihood that any one particular web page viewed on any one particular occasion with the AOL filter on would be an unblocked, domestically-hosted, adult web page (and they did not), their calculations would reveal that, at minimum, many thousands of adult web pages are viewed by children every day.

98. Overblocking is a significant concern. Non-sexually explicit web pages appear with much greater frequency than do sexually explicit web pages. Thus, even a relatively small increase in the percentage of “clean” web pages that are blocked can result in a very large number of blocked pages for a typical user. The net effect is that the vast majority of sites that are blocked will be blocked in error. Stark Testimony, 11/8/06 at 106:13 – 107:2.

99. Examples of non-sexually explicit web pages that were blocked by the filters tested by Mr. Mewett include: [www.nakedjuice.com](http://www.nakedjuice.com) (a fruit juice company); [www.topless-sandal.com](http://www.topless-sandal.com) (a footwear company); [www.boobiethon.com](http://www.boobiethon.com) (a breast cancer awareness web site); [www.acluf1.org/news\\_events/calendar/index.cfm?viewDate=6%2F1%2F2005](http://www.acluf1.org/news_events/calendar/index.cfm?viewDate=6%2F1%2F2005) (the calendar of a state ACLU chapter); [www.cia.gov/cia/publications/factbook/geos/mx.html](http://www.cia.gov/cia/publications/factbook/geos/mx.html) (the CIA World Fact

Book); [www.i-love-cats.com](http://www.i-love-cats.com); and [www.weightlossguide.com](http://www.weightlossguide.com). Def.'s Ex. 82 at ¶ 80; Def.'s Ex. 83 at ¶ 12.

100. Even web sites maintained by the Plaintiffs are subject to overblocking. For example, [www.powells.com](http://www.powells.com), an online bookstore, was blocked at the domain level in its entirety by four of the filters, and certain pages were blocked by an additional four filters. All but two of the filters blocked, either entirely or partially, [www.scarleteen.com](http://www.scarleteen.com), a web site operated by Heather Corinna designed specifically for teenagers and young adults. In addition, the Sexual Health Network's web site was blocked either entirely or partially by every filter setting tested. Mewett Testimony, 11/7/06 at 133:11-19; Def.'s Ex. 83 at ¶ 17; Def.'s Ex. 85.

101. Every Plaintiff has Web pages that are blocked by at least two filtering companies in categories designed to assist parents in protecting their children from inappropriate speech about sex. Joint Ex. 1 at ¶ 32. Plaintiff Rufus Griscom testified that Nerve.com has substantially lower traffic as a result of being blocked by filtering companies. Testimony of Rufus Griscom, at 104:5-11 (Oct. 23, 2006) ("Griscom Testimony"). Ms. Corinna testified that it bothers her that her Scarleteen web site is blocked by filters. Corinna Testimony, 11/2/06 at 111:16-18.

102. As further examples, in the Mewett-Stark study, multiple filters blocked: a web page with a cartoon that is clearly not sexually explicit; an article from Parenting Teens magazine; and the web sites of Planned Parenthood, the National Center for Lesbian Rights, and the Gay and Lesbian Medical Association. Mewett Testimony, 11/8/06 at 56:5-20, 58:5-11, 59:7-9, 59:24-60:1, 67:6-11; Pls.' Ex. 177 at 2, 8, 10, 12; Pls.' Ex. 180 at 8. These are examples of web pages that were specifically selected by plaintiffs for purpose of cross-examination; the fact that Mr. Mewett played no role in selecting these particular examples, and that they were

nonetheless widely overblocked by the filters, provides confirmation that the problem of overblocking is widespread.

103. These examples, along with the full range of statistics regarding overblocking, demonstrate that the private use of filtering software – or proposed government efforts to expand the use of filtering software – cannot be a lesser restrictive alternative to COPA. None of the examples cited above could plausibly be said to be likely to be prosecuted under COPA. Yet each of those sites is routinely blocked by filtering software.

104. The overblocking percentages reported in Mr. Mewett's and Dr. Stark's study reflect only the pages in the "clean" category used for testing, that is, web pages with absolutely no reference to any nudity or any form of sexual content. Mewett Testimony, 11/8/06 at 52:9 – 53:3. Plaintiffs' argument that overblocking is not a concern, because some parents may also wish to block their children's access to non-adult material with mature subject matter, fails to address the fact that the filters in fact are blocking web pages with no sexual content or nudity at all. Closing Argument, 11/20/06 at 52:14 – 53:5.

105. Mr. Mewett selected the filter settings designed to block only sexually explicit material, and, where applicable, the settings recommended by the filter companies for older minors. Def.'s Ex. 82 at ¶¶ 39-48. These settings nonetheless overblocked large amounts of "clean" material. Def.'s Exs. 68, 74, 78. Thus, overblocking is the inevitable result of any attempt to use computer programming to identify and block adult material, and not the result of the selection of filtering options designed to block more of both adult and "clean" material.

106. In addition to the personal computer-based and ISP-based filtering products described above, certain search engines also offer filtering services with respect to searches

performed on those search engines. Any user, however, can disable a search engine filter with the click of a button; there is no password protection that would enable parents to ensure the filter is set at all times for every search engine that a child might use. Search engine filters, therefore, do not present a viable means of limiting the access of minors to sexually explicit material. Def.'s Ex. 82 at ¶ 65.

107. Mr. Mewett tested filtering products offered by three search engines – Google, Yahoo!, and Verizon – by running the one hundred most popular search terms through those search engines. Even with the search engine filter setting activated, 3 percent of the top 100 queries returned sexually explicit web pages for Google; 8 percent returned sexually explicit web pages for Yahoo!; and 10 percent returned sexually explicit web pages for Verizon. This is a conservative test, because it is likely that search engine filters would focus their efforts on the most popular queries. Def.'s Ex. 82 at ¶ 69.

108. Significantly fewer than all 100 of the queries would have returned sexually explicit web pages if the search engine filters were turned off. Thus, those filters were not 90%, 92%, or 97% effective; instead, their true effectiveness rate at blocking adult material that would otherwise be available is much lower. Mewett Testimony, 11/7/06 at 139:13- 24.

109. Search engine filters face significant overblocking difficulties. For example, Google SafeSearch consistently blocks web sites operated by the U.S. government, by American newspapers, and by Fortune 1000 companies. Furthermore, Google SafeSearch frequently blocks even web sites that are specifically targeted at, or are helpful to, children. Mewett Testimony, 11/7/06 at 139:25 – 140:9; Def.'s Ex. 82 at ¶ 79.

**C. Other Problems with the Use (or Non-Use) of Filtering Software**

110. The figures that are reported as the results of Mr. Mewett's and Dr. Stark's study reflect the likelihood that a filter, if installed and in proper working order, would block sexually explicit material (albeit with significant over or under-blocking issues). However, not all families employ filters. Different studies report different estimates, but, even under the highest estimate, only 54% of parents with minor children and with Internet connections use filtering software. Cranor Testimony, 10/24/06 at 88:2-5; Def.'s Ex. 4 at 44.

111. Plaintiffs' witness, Professor Lorrie Cranor, offered her opinion that the large numbers of parents who decide not to use filters do so because they do not see any particular need to try to block adult content. Cranor Testimony, 10/24/06 at 90:14 – 91:2. The only study that she relied on in support of her conclusion, however, actually contradicted her. AOL found that the single most-highly rated concern listed by parents was the possibility of their children seeing inappropriate material on the Web. Pls.' Ex. 85 at 0009-10. Despite this, fully 72% of the parents who removed AOL's filtering software did so because they thought the product was too restrictive. Pls.' Ex. 85 at 0005. This is not surprising, given the high rates of overblocking caused by the filtering products, and in particular by the AOL filter, discussed above. As mentioned above, the large majority of sites blocked by that filter are blocked in error.

112. In addition, a computer user must have a significant degree of computer knowledge, and be willing to undertake a certain degree of effort, in order to install, configure, and update filters. An inexperienced parent is likely to face difficulties in installing the software or in attempting to remove it at a later date. Many computers are unable to effectively utilize

filters due to technical constraints and compatibility problems, such as firewalls or anti-virus software. Def.'s Ex. 82 at ¶ 74(b).

113. Further, the conversion of residential households in the United States to broadband Internet connections will exacerbate the limitations of Internet content filtering software. Some personal computers will not be upgraded, but will be expected to cope with the increased volume of data made available at higher speeds through broadband connections. Def.'s Ex. 82 at ¶ 74(f).

114. Even if filters are used, they also can be circumvented. The simplest way for a child to circumvent a filter, of course, is simply to go to another location where the filter does not operate. The testimony of Terri Kirk, a school librarian, is illustrative. She described a particular incident at her school in which an adult web site was widely discussed, and noted that the filters at her school blocked that site. She added, however, that she was "sure that teachers and students [saw that web site] at home." Testimony of Terri Kirk, at 91:4-9 (Nov. 1, 2006) ("Kirk Testimony").

115. In addition, there are many web sites available that describe how to disable or to circumvent specific filters, as well as filters in general. Mewett Testimony, 11/7/06 at 152:19 – 153:18, 157:10-20. It is possible to find these instructions even while the respective filter is turned on. Mewett Testimony, 11/7/06 at 152:24 – 153:5. For at least four of the filters that Mr. Mewett tested, he was able to obtain instructions from the Web on how to disable or bypass that filter, even with the filter turned on. Def.'s Ex. 82 at ¶ 74(c), (d). For example, he was able to find a document at [www.cexx.org/censware.htm](http://www.cexx.org/censware.htm) outlining two methods for bypassing the Net Nanny filter by typing "disable net nanny parental controls" into the Google search engine with

the Net Nanny filter on. Def.'s Ex. 82 at ¶ 74(c); Def.'s Ex. 89. Filtering products attempt to block these instruction pages, but they do not succeed at doing so. Mewett Testimony, 11/7/06 at 157:3-9.

116. Web proxy sites also can be used to gain access to Web sites that have been blocked. A proxy site allows clients to make indirect network connections to other network services. The black list of a filter therefore will not recognize the adult site that is reached as one that should be blocked. Mewett Testimony, 11/7/06 at 157:24 – 158:20. An example of a readily-available web site that instructs viewers on how to use proxy sites to circumvent filters is found at [www.zensur.freerk.com](http://www.zensur.freerk.com). Def.'s Ex. 82 at ¶ 74; Def.'s Ex. 90.

117. Translation tools may also be used to access sexually explicit Web sites in foreign languages. Sexually explicit search words may be typed in English into tools such as Google translation, and the translated into a different language, resulting in a list of foreign URLs that likely can be accessed without being blocked by a filter. This is because most filtering is done through the use of English phrases. Mewett Testimony, 11/7/06 at 162:17 -165:3; Def.'s Ex. 87.

118. Some search engines use a technique called “cache,” which permits a user to view a previous version of a web page if that page has changed after it is first found by the search engine's web crawler. Some filters may block a link to a particular web site with sexually explicit content, but would not block a cached image of that site. Mewett Testimony, 11/7/06 at 158:21 – 162:16; Def.'s Ex. 86.

**D. The Inherent Limitations of Filtering Software Technology**

119. As described above, filtering software relies on analysis of the form of words in the text of a web page to determine whether that page is sexually explicit without reference to

the meaning of the words. Neale Testimony, 11/9/06 a 36:23 – 37:4. Thus, computer software cannot understand text in the same way that a human can; the software can only review the formal features of that text. Neale Testimony, 11/9/06 at 43:19 – 44:5; Def.'s Ex. 59 at ¶ 5.3.2.

120. No automated system, however, is capable of analyzing the formal features of text with the accuracy needed to ensure that filtering software will be effective. Neale Testimony, 11/9/06 at 28:1 – 29:4.

121. These limitations of automated systems are inherent in any attempt to classify text on a purely formal basis. Thus, no text-based filtering system will ever be able to minimize both the underblocking of sexually explicit material and the overblocking of non-sexually explicit material. Neale Testimony, 11/9/06 at 37:9-18, 81:3-16.

122. As a result of these limitations, filtering software that blocks more sexually explicit material will always overblock more non-sexually explicit material as well. Neale Testimony, 11/9/06 at 28:24 – 29:4.

123. There is no reason to think the performance of filters or the basic principles of filtering will change in the foreseeable future. The problems are inherent in any attempt to use computer methodology, rather than human review, to study the formal features of language. Neale Testimony, 11/9/06 at 37:9-18, 81:3-16.

124. Unlike computer software, a human being is able to recognize both the content and the form of text, and is able to recognize the full context of language. Neale Testimony, 11/9/06 at 24:13 – 25:5; Cranor Testimony, 10/24/06 at 154:11-18.

**E. Market Failure in the Filtering Software Industry**

125. Only a portion of households with minor children use filtering software. Market survey evidence suggests that, most likely, approximately four out of ten of these Internet-connected households with children use filtering software. At most, 54 percent of these households do. Cranor Testimony, 10/24/06 at 88:2-7; Testimony of Dr. Jeffrey A. Eisenach Testimony, at 80:15-18 (Nov. 13, 2006) (“Eisenach Testimony”); Def.’s Ex. 4 at ¶ 8.

126. This low level of penetration of filtering software into its potential market indicates a failure of the market to provide products that can be effectively used by consumers. Eisenach Testimony, 11/13/06 at 79:18 – 80:14.

127. Parents are deterred from using filtering software because it causes overblocking and underblocking, and can be circumvented by children. Pls.’ Ex. 85 at 0005; Def.’s Ex. 4 at ¶¶ 119-125.

128. The nature of the filtering software market is conducive to market failure because of the asymmetry of information between consumers and producers of the filtering software. Eisenach Testimony, 11/13/06 at 125:21 – 126:3.

129. Forty-one percent of Internet-connected households have children; these households constitute the potential market for residential filtering software. Because the market for filtering software is smaller than the market for other kinds of security software, filtering software producers have weaker incentives to improve the quality of their product, thus contributing to market failure. Eisenach Testimony, 11/13/06 at 78:10-24, 125:21 – 126:15.

130. Filtering software producers lack an incentive to create a quality product because consumers make purchases without assessing the quality of the product. When consumers use

the product, they are unable to determine whether the product is good or bad. Therefore, the filtering software market lacks the incentive to develop a better product. This is known as the “Lemons problem.” Eisenach Testimony, 11/13/06 at 124:16 – 126:15.

131. In such markets, producers of high quality products are unable to obtain full value for the products they produce, since consumers are unable to distinguish high quality products from low quality products, and therefore are unwilling to pay the full cost of producing a higher quality product. Eisenach Testimony, 11/13/06 at 125:21 – 126:15. In such markets, producers devote their resources primarily to other products. Eisenach Testimony, 11/13/06 at 139:22 – 140:5.

132. The market for filtering software products is such a market, and therefore the quality of filtering software is unlikely to improve significantly in the future. Eisenach Testimony, 11/13/06 at 126:1-15 and 128:7-23.

133. The high fixed costs required to produce filtering software further limit the incentive for producers to offer effective products. Eisenach Testimony, 11/13/06 at 142:10-19.

134. Several factors, in combination, render it unlikely that software producers will devote efforts to producing better filtering products: (1) the fact that there are high fixed costs for the production of filtering software; (2) the smaller market for filtering software as compared to other types of software; (3) the industry practice of bundling filtering software with those other types of software; and (4) the inability of consumers to evaluate the quality of the products. Eisenach Testimony, 11/13/06 at 143:22 – 145:4.

135. These are inherent defects in the market for filtering software. They could not be resolved by offering governmental reviews of filtering products; there are already a number of

product reviews available, and the defects in the market continue to persist. Eisenach Testimony, 11/13/06 at 193:11-16.

**F. Professor Cranor's Shallow Analysis is Entitled to No Weight**

136. Plaintiff presented the testimony of Professor Lorrie Cranor, who offered her opinion that filtering software, in conjunction with parental education efforts, can be effective in protecting minors from access to sexually explicit material. Her opinion, however, is of little relevance to this case, for several reasons.

137. First, Professor Cranor's definition of an "effective" filter is of little use to the Court. She considers a filter to be effective for her purposes if it works "most of the time." Cranor Testimony, 10/24/06 at 113:5-9. She also does not consider the issue of overblocking to be relevant in evaluating whether a filter is effective. Cranor Testimony, 10/24/06 at 52:19 – 53:6. By any reasonable definition, however, a filtering program that allows a minor access to almost half of the available adult content on the Web, and that also blocks a wide range of legitimate content, cannot be considered to be an effective filter.

138. Because Professor Cranor does not believe that the issue of overblocking is a relevant consideration, she cited a passage from the National Research Council's report and concluded that that body found filters to be effective. Cranor Testimony, 10/24/06 at 75:22 – 76:3. In fact, the passage carries the opposite meaning: "Filters can be highly effective in reducing the exposure of minors to inappropriate content if the inability to access large amounts of appropriate material is acceptable." Pls.' Ex. 54 at 0040. In considering whether the expanded use of filtering software would be a less restrictive alternative to COPA, however, the blocking of "large amounts of appropriate material" cannot be deemed to be acceptable.

139. Second, it is apparent that Professor Cranor selectively cited materials that she considered to be favorable to her opinion, and incompletely considered those materials. For example, she disregarded several studies that reached conclusions contrary to her own because she could not determine that their methodologies were reliable. Cranor Testimony, 10/24/06 at 145:23 – 147:11. At the same time, she relied on several studies favorable to her conclusion with incomplete methodologies, and she determined that those studies were reliable precisely because they reached conclusions similar to her own. Cranor Testimony, 10/24/06 at 147:13 – 149:23.

140. She also failed to fully consider the materials that she did purport to rely upon. For example, she believed that the COPA Commission's report rated filtering software to be very effective. She did not, however, read that report, but instead only gave it a " cursory look." Cranor Testimony, 10/24/06 at 151:13-19. She believed that the Commission rated filtering on a 20-point scale, from negative 10 to positive 10, and that the positive ratings given to filtering software thus represented a very favorable judgment. Cranor Testimony, 10/24/06 at 152:25-153:2, 170:3-14. In fact, the Commission used only a 10-point scale, and the ratings given to filtering software were not particularly high. Stark Testimony, 11/8/06 at 120:4-22; Pls.' Ex. 6 at 15. In any event, the ratings used by the Commission represented only the subjective opinions of its members, and not the results of empirical tests. Stark Testimony, 11/8/06 at 121:1-12.

141. Professor Cranor also cited to a study conducted by the NetAlert organization, and opined that that study found a filtering product to be 100% effective. Cranor Testimony, 10/24/06 at 65:6-16. In fact, she reviewed only a black-and-white copy of the study, and the original color version revealed that her interpretation was incorrect. Stark Testimony, 11/8/06 at

129:4-130:7; Defendant's Demonstrative Exhibit 9. In any event, the NetAlert study did not use random sampling of web sites and it used data that is over five years old. For that reason, it is of little relevance in evaluating the present-day performance of filtering software. Stark Testimony, 11/8/06 at 127:11 – 130:12.

142. In her testimony, Professor Cranor offered her opinion that filtering software can effectively use artificial intelligence techniques to classify pornography, and claimed that the NRC's report supported her conclusion. In fact, the NRC reached the opposite conclusion. It instead concluded that filtering software inevitably will underblock and overblock pornographic materials, and that significant improvements in the software are not expected in the near future. Stark Testimony, 11/8/06 at 122:3 – 123:9; Pls.' Ex. 54 at 0447.

143. Third, the various studies that Professor Cranor did choose to rely upon are of limited relevance to this case. She relied upon an article in the Consumer Reports magazine, even though she acknowledged that it did not use a reliable methodology in assessing the performance of filters. Cranor Testimony, 10/24/06 at 69:11-22. The testing described in that article cannot be generalized to state any broader conclusions regarding the effectiveness of filters. Stark Testimony, 11/8/06 135:7 -136:14. She also cited to a report prepared for the Department of Commerce; that report, however, did not undertake any empirical testing of filters, or of any other methods of protecting minors from exposure to sexually explicit materials. Cranor Testimony, 10/24/06 at 96:9-15; Stark Testimony, 11/8/06 at 123:17-25.

144. She also cited studies conducted by E-Testing Labs and by Corey Finnell in support of her opinion. Cranor Testimony, 10/24/06 at 55:24 – 58:25, 59:9 – 61:25. Those studies tested, however, the effectiveness of enterprise filtering software, not filters that are used

in residential settings. As explained in more detail below, enterprise filtering software and residential filtering software are very different. Further, neither study used random samples of web pages, so the results of those studies cannot be extrapolated to a broader universe in the manner that Mr. Mewett's and Dr. Stark's study can. Stark Testimony, 11/8/06 at 125:11-19. The data in both studies is also several years old, and so is of limited use in assessing the performance of filters today. Stark Testimony, 11/8/06 at 125:20 – 126:6. In particular, Professor Cranor cited to Mr. Finnell's study to conclude that the overblocking rates of filtering products are low. Cranor Testimony, 10/24/06 at 60:9 – 61:25. That study, however, did not compare the ratio of incorrectly blocked "clean" material to unblocked "clean" material. Instead, it compared the rate of incorrectly blocked "clean" material to correctly blocked adult material. Because that ratio depends entirely on the sample sizes of the "clean" and adult material that were used in the tests, no broader conclusions can be drawn from those reported results in the manner that conclusions can be drawn from Mr. Mewett's and Dr. Stark's study. Stark Testimony, 11/8/06 at 132:9 – 133:3.

145. Professor Cranor also relied in her report (but not in her testimony) upon certain claims made by the RuleSpace company regarding the effectiveness of its filtering product. As the NRC has cautioned, however, claims made by filtering software companies regarding the effectiveness of their own products should be discounted. Stark Testimony, 11/8/06 at 139:15 – 140:11; Pls.' Ex. 54 at 0305. RuleSpace, in particular, apparently manually selected the web pages that is used in its testing, and thus could have manipulated the pages that it used for its testing. Mewett Testimony, 11/7/06 at 169:7-21. Mr. Mewett and Dr. Stark, in contrast, tested the Verizon filtering software product, which uses RuleSpace technology, against random sets of

web pages, and found that that filter performed particularly poorly. Mewett Testimony, 11/7/06 at 169:22 – 172:4; Def.’s Exs. 68, 74, 78.

146. Professor Cranor also offered her opinion regarding filtering software that will be included in the forthcoming Microsoft Vista operating system. Cranor Testimony, 10/23/06 at 212:18 – 213:7. She did not personally conduct any testing of that software, nor did she review any independent testing of that software. Cranor Testimony, 10/24/06 at 123:8-15, 135:16-25. She was unaware of the methodology that Microsoft used as the basis for its claims that its filtering software will be effective. Cranor Testimony, 10/24/06 at 136:1-4. As is the case with RuleSpace’s claims, the claims made by Microsoft regarding its own product’s effectiveness should be viewed with skepticism. Stark Testimony, 11/8/06 at 139:15 – 140:11; Pls.’ Ex. 54 at 0305.

147. In sum, Professor Cranor selectively cited her source materials, and the materials that she did rely upon are of limited relevance. In contrast, Mr. Mewett’s and Dr. Stark’s study used newer data, and the results of that study can be extrapolated to a broader universe. That study, in contrast to Professor Cranor’s opinion, reveals that filtering software programs fail to block vast amounts of adult material, and that even the programs that do block more adult material can do so only by also blocking substantial portions of the “clean” material available in the World Wide Web.

**G. Testimony Regarding Enterprise Filtering Is Not Relevant**

148. Filtering software products used in institutional settings, such as schools, libraries, and workplaces, are different from the type of filtering products that are available for residential use. Typically, institutions that use enterprise filters also devote expenditures for

computer infrastructures, along with the programs, that will improve the software's performance. Mewett Testimony, 11/7/06 at 165:8 – 166:5. For example, enterprise filters use additional devices known as "proxy servers," which are separate devices from the end-user's computer. Mewett Testimony, 11/7/06 at 166:6-25. Further, institutions typically assign technicians to operate the enterprise filters and to monitor their effectiveness. Mewett Testimony, 11/7/06 at 167:7-24.

149. Professor Cranor offered her opinion that any differences between enterprise filter and residential filters would not be relevant because, with the right kind of computer and operating system, there is no technical reason that a parent could not use an enterprise filter in the home. Cranor Testimony, 10/24/06 at 46:12-19. This is not plausible. For example, the enterprise filter offered by SurfControl costs \$1500 per year, with an additional expenditure of \$500 to \$1000 for necessary training on the use of that filter. Testimony of Jim Murphy, at 243:9-24, 245:2-16 (Nov. 1, 2006).

150. As a practical matter, therefore, home users are restricted by the cost of the devices from using enterprise filtering products. Mewett Testimony, 11/7/06 at 166:24 – 167:6. The markets for enterprise filters and for residential filters are two very different markets, and one product is not a reasonable substitute for the other; if the products were comparable, one would expect institutions to substitute the much cheaper residential products for the enterprise products, but they do not do so. Eisenach Testimony, 11/13/06 at 162:10 – 163:11. It is thus unsurprising that Professor Cranor was unaware of a single family in the United States that actually used an enterprise filtering product in its home. Cranor Testimony, 10/24/06 at 167:1-4.

151. The experiences of institutions, such as Department of Justice offices, or such as

the three school districts described by some of the witnesses at trial, that use enterprise filters, thus are not relevant in evaluating the effectiveness of filter products in the home setting. In particular, the testimony offered by plaintiffs from several school librarians is of little relevance. Their school districts had technicians assigned to monitor the operation of the filters. Kirk Testimony, 11/1/06 at 96:9-17; Taylor Testimony, 11/1/06 at 178:21 – 179:8; Testimony of Tava Smathers, at 25:17 – 26:15 (Nov. 2, 2006) (“Smathers Testimony”). None of the librarians was aware of any systematic testing of the effectiveness of the enterprise filters that their school districts use. Kirk Testimony, 11/1/06 at 97:24 – 99:20; Taylor Testimony, 11/1/06 at 180:14 – 181:12; Smathers Testimony, 11/2/06 at 26:20 – 28:4. Further, they would have been aware of adult material being delivered only if that fact had been reported, and those reports were not routinely generated. Kirk Testimony, 11/1/06 at 99:17-24; Smathers Testimony, 11/2/06 at 28:14-24.

**H. Filtering Products Fail to Address Access to the Web from Mobile Devices**

152. As has been demonstrated above, filtering products fail to block significant amounts of adult material, and, when they do block more adult material, they can do so only by also blocking vast amounts of non-sexually explicit material. These failings of filtering products are inherent in the types of techniques that the software programs use. Moreover, these defects will become more acute with the growing use of alternative devices, such as mobile phones, to access the Web.

153. Alternative devices, such as mobile phones, are increasingly being used to access the Internet. For example, the Center for the Digital Future reports that 14.5 percent of those surveyed in 2003 reported accessing the Internet through an alternative device, up from 9.2

percent in 2002. Def.'s Ex. 4 at ¶ 44.

154. Despite the growing use of these devices, no mobile phone company currently offers any product that filters content from the World Wide Web. Mewett Testimony, 11/7/06 at 182:1 – 183:2. Mobile phone vendors instead offer products such as controls that shut off access to the Web entirely, or that offer access only to very restrictive “walled gardens,” which contain only material that has been specifically identified by the vendor to be available. Mewett Testimony, 11/7/06 at 185:4-12; Testimony of Jonjie Sena, at 65:9-24 (Nov. 2, 2006) (“Sena Testimony”).

155. Some vendors claim to have filtering products that may be available in the future, but there has been no independent testing of the effectiveness of those products. Felten Testimony, 10/25/06 at 57:18 – 58:8; Sena Testimony, 11/2/06 at 63:12 – 64:4.

156. There are a number of technical difficulties with mobile devices that indicate that the filtering products that may someday be offered for those devices will perform more poorly than filtering products for home computers. First, mobile phone filters cannot rely on blacklists to block content, because the same URL for a mobile phone could generate adult content or “clean” content at different times. Testimony of Alistair Allan, at 221:23 – 222:16 (Nov. 2, 2006) (“Allan Testimony”).

157. The other technique used by filtering software programs, dynamic filtering, is also less effective on mobile devices. Web pages that appear on mobile phones have far fewer features that the filtering software can attempt to analyze than do standard web pages. Allan Testimony, 11/2/06 at 218:10 – 219:3. Therefore, the dynamic filtering processes are less likely to correctly analyze the content of the web page. Mewett Testimony, 11/7/06 at 185:13 – 186:6.

158. In addition, mobile phones have less processing power than home computers do, and thus the capabilities of the filtering software programs for mobile phones will always lag behind the capabilities of programs available for home computers. Felten Testimony, 10/25/06 at 21:9-20.

159. In notable contrast to the inability of mobile phones to deploy effective filtering products, mobile phone vendors can, and already do, use age verification services to restrict the access of minors to pornographic material through those devices. Testimony of John Dancu, at 154:16 – 155:16 (Nov. 9, 2006) (“Dancu Testimony”).

#### **IV. COPA PROVIDES THE MOST EFFECTIVE SOLUTION TO THE PROBLEM**

160. Congress built several affirmative defenses into COPA to ensure that adults could access material deemed harmful to minors, while restricting minors from such speech. It is an affirmative defense under COPA for a web site to restrict access by minors to material that is harmful to minors by requiring the use of a “credit card, debit account, adult access code, or adult personal identification number,” “by accepting a digital certificate that verifies age,” or by “any other reasonable measures that are feasible under available technology.” 47 U.S.C. § 231(c)(1).

##### **A. Credit Card Verification on the Web**

161. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a credit card. Joint Ex. 1 at ¶ 117.

162. It is an affirmative defense to prosecution under COPA to restrict, in good faith, access by minors to material that is harmful to minors by requiring use of a debit card, including a reloadable prepaid card. Joint Ex. 1 at ¶ 118.

163. “Traditional payment cards” consist of credit, debit, and reloadable prepaid cards. A credit card is essentially a loan from a card issuing company. Testimony of Arthur E. Clark, Jr., at 17:4-5 (Nov. 14, 2006) (“Clark Testimony”). A debit card is a payment card that is tied to a deposit account, primarily a checking account; purchases of goods and services on a debit card are deducted from the individual's checking account. Clark Testimony, 11/14/06 at 17:5-8. A prepaid card is a payment card that an individual loads with cash and then proceeds to purchase goods and services. Clark Testimony, 11/14/06 at 16:24-25. Reloadable prepaid cards can be purchased for cash and after that amount is used up more money can be added; non-reloadable prepaid cards are one-time use cards. Clark Testimony, 11/14/06 at 48:11-24.

164. “Traditional payment cards” have five unique characteristics that make them a valid affirmative defense under COPA: (1) high adoption rates on the World Wide Web, (2) widespread access by adults, (3) limited access by children, (4) a transaction record that parents can review, and (5) worldwide operating policies that allow card companies to “turn off” merchants that do not comply with terms of the card companies’ merchant agreements. Clark Testimony, 11/14/06 at 159:16 – 160:3; Def.’s Ex. 93 at 00025-26.

165. Consumers are quite comfortable with using all types of payment cards on the Web. Clark Testimony, 11/14/06 at 66:20-22, and payment cards are used by the vast majority of adults to purchase goods, services, and access to content on the Web. Clark Testimony, 11/14/06 at 62:7-8.

166. Traditional payment cards are accepted by the vast majority of commercial web site operators that sell goods, services, and access to content on the Web. Clark Testimony, 11/14/06 at 229:23 – 230:4; Def.’s Ex. 93 at 25.

167. Traditional payment cards are accessible to the vast majority of adults. Clark Testimony, 11/14/06 at 77:17 – 78:1. Adults have or can obtain a credit card, debit card, or reloadable prepaid card. Clark Testimony, 11/14/06 at 80:25 – 81:7.

168. Even many undocumented immigrants can obtain traditional payment cards. Clark Testimony, 11/14/06 at 79:10-16, 79:24 – 80:2.

**1. Minors Do Not Have Traditional Payment Cards Under Their Own Control**

169. Card issuers will not issue credit and debit cards directly to minors because of state age-of-majority laws because the debt is unenforceable against minors; debit cards have risk of unenforceable debt through overdraft. Clark Testimony, 11/14/06 at 118:7 – 120:3. Each state has a law that defines the “age of majority.” Def.’s Ex. 93 at 0017. That is the age when an individual who enters into a contract can not be released from the commitment due to age. *Id.* This is important to the financial institution to ensure that it can collect an outstanding balance (e.g., credit card, debit card tied to a checking). *Id.* Most states set the “age of majority” at 18. *Id.*

170. Discover Financial Services does not issue credit cards to persons below age 18 because it cannot hold them legally responsible for their credit card charges. Testimony of Patricia M. Rinchiuso, at 241:16 – 242:6 (Nov. 6, 2006).

171. Eleven percent of minors age 12 to 17 have a card issued from the parents’ account, or a parent co-signed card, although these cards are “in their own name.” Clark

Testimony, 11/14/06 at 83:17-25, 91:8-22. Another eleven percent of minors age 12 to 17 may borrow traditional payment cards on a per transaction basis. Clark Testimony, 11/14/06 at 84:6 – 85:9, 96:2 – 96:12. These figures lead to a total of approximately 22 percent of minors age 12-17 that may have access to traditional payment cards. Clark Testimony, 11/14/06 at 114:11-15.

172. Even the small subset of minors with some access to a credit card does not have unsupervised access. The traditional payment cards used by minors are cards held by adults, and adults can supervise the use of the payment card. Clark Testimony, 11/14/06 at 92:3-14, 117:9-18.

173. Parents of minor children who borrow their parent's payment cards to make online purchases can ask their children what they are going to purchase. Joint Ex. 1 at ¶ 99.

174. Data from Teenage Research Unlimited, credited as reliable by plaintiffs' payment card expert, Professor Ronald Mann, *see* Testimony of Professor Ronald Mann at 111:17 – 112:13 (Nov. 6, 2006) ("Mann Testimony"), supports these findings. Clark Testimony, 11/14/06 at 104:17 – 107:5, 114:6-10. Data from Teenage Research Unlimited showed that 2.2 percent of teens had a credit card "in their name;" 5.5 percent had a debit card "in their name;" 5.1 percent had "access" to a parent's card; 4.4 percent had access to a parent's debit card. Clark Testimony, 11/14/06 at 107:6-24. Similarly, data from Teenage Research Unlimited shows that 35.5 percent of minors age 12-16 have made online purchases. 166:23 – 168:2. The data showed that, of minors age 12-16 who made online purchases, about 59 percent used a parent's credit card to pay for the purchase; about seven percent used a debit card; about 11 percent used an online buying service such as PayPal; about 1.6 percent used "their own" credit card; and about seven percent used an online gift certificate. Clark Testimony, 11/14/06 at 168:3-21.

175. Regardless of whether children have a payment card in their own name tied to their parents' account or whether they borrow a payment card on a per transaction basis, all transactions are records on the billing statement, which card issuers encourage all customers to review so they can investigate unauthorized transactions. Clark Testimony, 11/14/06 at 91:17 – 92:14, 94:5 – 95:8, 117:4-18. Plaintiffs' payment card expert admits that parents may supervise the transaction. Mann Testimony, 11/6/06 at 169:5-9, 184:16 – 185:2.

176. Billing statements are sent in the mail to a residential address, and can be reviewed almost immediately online and by telephone. Clark Testimony, 11/14/06 at 92:5-14.

177. Card issuers of reloadable prepaid cards interpret regulations promulgated to enforce the Know Your Customer Provisions of the Bank Secrecy Act, as amended by the U.S.A. Patriot Act, which require all card issuers to verify the identity of all new customers to whom they issue credit and debit cards, 31 C.F.R. § 103.121, as applying to them. Clark Testimony, 11/14/06 at 130:21 – 131:1, 132:19 – 133:22. Plaintiffs' payment card expert, Professor Ronald Mann, did not dispute the applicability of these provisions to reloadable prepaid cards. Mann Testimony at 133:25 – 134:4, 196:15-23. Professor Mann only claimed, erroneously as a matter of law, that nothing in the provisions require the customer to be an adult. *Compare* Mann Testimony, 11/6/06 at 134:19-21 *with* 31 C.F.R. § 103.121(a)(3)(i) (“Customer means: (A) A person that opens a new account; and (B) An individual who opens a new account for: (1) An individual who lacks legal capacity, such as a minor. . .”).

178. Card issuers must verify and maintain records of a customer's name, date of birth, residential address, and Social Security Number/Taxpayer Identification Number. 31 C.F.R. § 103.121(b)(2)(i)(A). Further, card issuers must obtain this information either (a) by verifying the

customer's driver's license or passport and other documents or (b) by "contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or other source; checking references with other financial institutions; and obtaining a financial statement." *Id.* § 103.121(b)(2)(ii)(A) and (B). Finally, card issuers must maintain records documenting the verification procedures they relied on. *Id.* § 103.121(b)(3).

179. There is no evidence that card issuers will issue credit cards, debit cards or reloadable prepaid cards to minors; plaintiffs admit that reloadable prepaid card issuers obtain name, address, date of birth, and Social Security number. Mann Testimony, 11/6/06 at 134:3-11, 196:15-23. There is no evidence that children generally know their own or their parents' Social Security Number. Mann Testimony, 11/6/06 at 197:24 – 198:17; Russo Testimony, 10/26/06 at 19:5-9.

**2. The Existence of Non-Reloadable Gift Cards Does Not Undermine COPA's Credit Card Affirmative Defense**

180. Non-reloadable gift cards are another type of payment card that can be used to purchase good services, and access to content on the Web; they include: (a) closed system gift cards, (also known as online gift certificates); and (b) "open system" gift cards. Clark Testimony, 11/14/06 at 133:24 – 135:15.

181. Closed system gift cards can only be used to purchase gifts from the store that issued the card. Clark Testimony, 11/14/06 at 135:16 – 136:6. These closed system cards constitute the vast majority of non-reloadable prepaid cards. Clark Testimony, 11/14/06 at 86:20 – 89:1.

182. Open system cards can be used to purchase goods, services, and access to content online, but they do not have a billing address. Clark Testimony, 11/14/06 at 136:7-20, 142:10-12.

183. Open system gift cards constitute less than one percent of payment dollar volume compared to credit and debit card volume. Clark Testimony, 11/14/06 at 137:10 – 138: 4.

184. Because open gift cards lack a billing address, online merchants can and, for reasons of fraud prevention, generally do, decline open gift cards for payment of goods, services, or content. Clark Testimony, 11/14/06 at 138:5 –139:24, 141:22 – 143:22. High risk merchants collect billing address information and use address verification for fraud control purposes. Clark Testimony, 11/14/06 at 174:25 – 175:23; Def.'s Ex. 93 at 0020; Russo Testimony, 10/25/06 at 226:13-18, 227:9-11.

**3. The Conclusions of Plaintiffs' Payment Card Experts Are Not Supported by Their Reliance Material**

185. Plaintiffs' payment card expert, Professor Ronald Mann, didn't do any research about any aspect of his report. Mann Testimony, 11/6/06 at 161:10-12.

186. The only support for Plaintiffs' claim that surveys of teen card access under-report actual access is a citation from a work by Plaintiffs' payment card expert, Professor Ronald Mann, which states only that people do not *understand* how much debt they hold. Mann Testimony, 11/6/06 at 161:13 – 163:13. Moreover, there is no evidence about the accuracy or reliability of an article reporting that 52% of teens shop online; there is no evidence that the report on which the article was based used a non-random sample or that it even reported the number of teens who shop online. Mann Testimony, 11/6/06 at 164:3 – 166:7. Further, there is no basis for relying on a study by Junior Achievement showing higher teen card access because

the study was not based on a random sample. Mann Testimony, 11/6/06 at 166:8 – 167:19. In addition, Plaintiffs have no basis for a demonstrative calculation that 37% of 16-year-olds have access to payment cards because Plaintiffs' payment card expert may have over-counted 16-year-olds who responded in the numerator of his calculation and may have undercounted the number of 16-year-old respondents in the denominator of his calculation. Mann Testimony, 11/6/06 at 168:12 – 174:22.

187. There is no evidence that traditional payment cards are marketed to teens. Mann Testimony, 11/6/06 at 180:25 – 183:5, 185:7-10. There is evidence of “family cards” such as the VISA BUXX card or JP-Morgan Chase FIRM card that are marketed to teens but only issued to co-signing parents. Mann Testimony, 11/6/06 at 185:24 – 188:1, 189:10 – 194:13. There is evidence that, one reloadable prepaid card, the NetSpend card, is marketed to unbanked adults. Mann Testimony, 11/6/06 at 188:2-25. Moreover, there is no evidence that NetSpend issues reloadable prepaid cards to minors despite their official policy. Mann Testimony, 11/6/06 at 195:20 – 196:24 (official policy).

188. There is only one anecdote about a teen obtaining a card from a false application, and that teen had the consent of this father. Mann Testimony, 11/6/06 at 203:3 – 213:14. There is no other evidence on false applications. Mann Testimony, 11/6/06 at 213:15-18.

189. There is no evidence or data that card companies erroneously issue credit, debit, or reloadable prepaid cards to minors, even if they do mistakenly send card applications to babies, dogs, and dead people. Mann Testimony, 11/6/06 at 215:11 – 219:15.

190. There is no evidence or data that children use stolen card information to obtain access to harmful-to-minors content. Mann Testimony, 11/6/06 at 213:22 – 214:19.

191. There is no evidence that minors have access to payment cards that is unsupervised by adults; in fact, plaintiffs' expert, Michael Russo, expressly admitted that "this particular issue is not anything that [he] considered one way or the other." Russo Testimony, 10/26/06 at 5:1-16. Plaintiffs' expert Mr. Russo had no data about minors' access to payment cards. Russo Testimony, 10/26/06 at 7:5-11.

192. Plaintiffs' only evidence that not all U.S. adults have access to payment cards is one hearsay anecdote from one adult entertainment provider. Russo Testimony, 10/26/06 at 7:12 – 8:9. Plaintiffs had no evidence or data on adults' access to payment cards. Russo Testimony, 10/26/06 at 8:10-14. Plaintiffs had no evidence or data on world wide adult access to payment cards. Russo Testimony, 10/26/06 at 8:15 – 9:2.

193. The COPA Commission's findings regarding payment cards are obsolete and/or incomplete. Clark Testimony, 11/14/06 at 149:7 – 156:20. No members of the Commission were associated with the payment card industry. Clark Testimony, 11/14/06 at 152:17-19. The Commission had significant financial and time constraints and did not conduct independent research. Clark Testimony, 11/14/06 at 152:20 – 153:4. Professor Mann has no basis for his assertions about the reliability of the COPA Commission's findings on credit cards; Mann attributed statements to the COPA Commission that it did not make. Mann Testimony, 11/6/06 at 222:11 – 226:1.

**B. Micro-Payment Technology Facilitates the Purchase of Content**

194. Bitpass offers a product that allows Web purchases to monetize online digital content. Testimony of Doug Knopper, CEO of Bitpass, at 93:7-14 (Nov. 9, 2006) ("Knopper Testimony"). Bitpass offers a stored-value account that consumers can use to purchase access to

digital content offered by Web publishers. Knopper Testimony, 11/9/06 at 108:9-14. Bitpass has five large Web publishers and 4000 small Web publishers as clients. Knopper Testimony, 11/9/06 at 93:15-22. Bitpass created its product because it believes that sales of digital content is growing and will grow dramatically. Knopper Testimony, 11/9/06 at 94:4-10, 95:16-20.

195. Consumers can set up a Bitpass account at no cost, Knopper Testimony, 11/9/06 at 103:15-17, and can fund the account with as little as \$3. Knopper Testimony, 11/9/06 at 105:6-8. U.S. consumers can fund the account with a payment card or PayPal. Knopper Testimony, 11/9/06 at 103:24-25. After they have established the account, consumers can purchase access to content by typing in their name and password and clicking the mouse. Knopper Testimony, 11/9/06 at 99:14-21, 102:18-24, 105:17-20. The purchasing system is anonymous and does not interrupt the flow of the consumers' Web site visiting experience. Knopper Testimony, 11/9/06 at 102:18-24, 105:9-16, 109:6-7. Bitpass has about 500,000 consumer accounts. Knopper Testimony, 11/9/06 at 93:23-24.

196. Web publishers can set up accounts for free and can install the Bitpass "buy" Button onto their Web sites in a few hours. Knopper Testimony, 11/9/06 at 105:21 – 106:15. The cost of operating the product generally runs from 5% to 15% of sales. Knopper Testimony, 11/9/06 at 106:14-22. Web publishers can charge as little as one cent for access to content. Knopper Testimony, 11/9/06 at 109:16-21. Web publishers can provide one time access or subscription access to content. Knopper Testimony, 11/9/06 at 97:20 – 99:13.

197. Bitpass has considered and prepared the specs for a feature that allow Web publishers to accept only those Bitpass accounts that are tied to a payment card. Knopper Testimony, 11/9/06 at 111:22 – 115:14. Bitpass could offer the feature in three to six months if

there was a demand for it. Knopper Testimony, 11/9/06 at 116:13-17.

**C. Online Age Verification Services Are Highly Effective**

198. Age verification services can prevent minors from accessing harmful content.

Dancu Testimony, 11/9/06 at 174:8 – 175:20.

199. One technologically feasible manner in which web sites can screen for age is through age verification services (“AVS products” or “AVS technologies”). AVS products currently are used for online wine and tobacco sales, and similar identity verification services are used by many industries, such as the financial service industry, to reduce the risk of fraud on the Internet. Dancu Testimony, 11/9/06 at 143:20 – 144:9, 152:19 – 154:15, 157:2 – 158:10; Def.’s Ex. 464.

200. Age verification services are currently used to restrict access by minors to pornographic material through mobile phones. Dancu Testimony, 11/9/06 at 154:16 – 155:16.

201. AVS products can require a consumer to enter personal information such as name, address, and the last four digits of their Social Security number. The information is then verified using commercially available databases that aggregate public records. The process is completed in less than a second. Dancu Testimony, 11/9/06 at 160:15 – 161:3, 162:20 – 166:1, 171:8-15; Def.’s Ex. 109.

202. IDology’s historical records demonstrate that AVS products are able to verify the age of online consumers well over 90 percent of the time. AVS companies do not validate the age of a consumer when bogus information is inputted. Dancu Testimony, 11/9/06 at 224:14 – 226:14.

203. IDology was certified as a provider of age verification services for the wine

industry by the State of Michigan after passing a test of the product's effectiveness. Dancu Testimony, 11/9/06 at 226:19 – 227:12.

204. The age verification process is configured to address the most common reasons that inputted data does not perfectly match the data records, such as typographical errors, a change in last name, or an address change. Dancu Testimony, 11/9/06 at 171:16-174:7.

205. AVS products are sophisticated enough to ensure that a customer is not using someone else's personal information. The AVS products generate questions based on personal historical information, such as the color of a given car or the address of a previous home. AVS companies tailor these quiz products to meet the needs of their consumers. Obviously, the more questions that are asked, the more effective the verification process will be. Dancu Testimony, 11/9/06 at 177:7 – 181:3; Def.'s Ex. 109-0005.

206. IDology offers its clients the ability to set "velocity limits," which limit the number of times someone can complete the age verification process from the same location. This feature allows web site operators to protect themselves against hostile attempts to drive up costs. A web site operator also can use this feature to require that a customer answer biographical historical questions after failing an initial attempt to verify his age. Dancu Testimony, 181:4 – 182:15; Def.'s Ex. 109-0006.

207. AVS products can restrict access to a web site based on the geographic location of a web site visitor. Access by web site visitors in specified zip codes can be blocked entirely or can be granted only after a more robust screening process, which can include use of biographical historical questions. Dancu Testimony, 11/9/06 at 182:16 – 184:7; Def.'s Ex. 109-0007.

208. Age verification can be completed at little cost, which can be absorbed by the

web site operator. The cost, with a list price as low as 37 cents, depends on the volume of transactions. The cost of verification can drop dramatically when there is a high volume of transactions, which reasonably can be anticipated if COPA were to go into effect. Dancu Testimony, 11/9/06 at 221:20 – 222:2, 223:4 – 223:21.

209. AVS products are currently used by commercial web sites to restrict access to Internet content. An age verification password can be issued to certify that a consumer is not a minor and can be reused over a specified period of time on the same web site or on affiliated web sites. Dancu Testimony, 11/9/06 at 184:20 – 185:18.

210. In addition to the commonly used methods of online age verification, some promising “digital wallet” technologies are on the horizon, such as Verisign’s Personal Identity Provider and Microsoft’s CardSpace, which will streamline the online age verification process. After a consumer’s age and identity have been verified by an AVS product, the consumer can store a record of this verification in his “digital wallet” and subsequently gain access to any web site with age restricted content or products without the need for re-verification. This new use of *existing* AVS technology will eliminate not only the cost of verification but also the need to provide personal information to gain access to every web site that is visited. Dancu Testimony, 11/9/06 at 191:24 – 192:5, 204:20 – 207:21, 217:11 – 220:4.

211. Although AVS products are the most reliable existing method, the options for online identity and age verification are becoming more numerous as online verification technology continues to develop. Dancu Testimony, 11/9/06 at 190:15-192:5, 221:11-221:19.

212. Plaintiffs’ expert Michael A. Russo has no basis for his opinion on the effectiveness of age verification companies such as ID Response. Mr. Russo did not disclose the

companies he evaluated. Russo Testimony, 10/26/06 at 9:3-11:23. Mr. Russo had no methodology for his evaluation. Mr. Russo kept no records of his evaluation. *Id.* at 15:10-15. Mr. Russo was not qualified to make his evaluation. Mr. Russo's opinions on the effectiveness of the product are not consistent with his own claimed testing. *Compare* Russo Testimony, 10/26/06 at 13:11-14:1 *with* Russo Testimony, 10/26/06 at 24:20-25:18. Mr. Russo has no evidence of whether children have access to their parents' Social Security numbers. *Id.* at 19:5-23. Mr. Russo has no basis for comparing age verification technologies with real-world ID checks. *Id.* at 22:19-24:19. Mr. Russo does not know all the data sources age verification companies check. *Id.* at 26:8-10. Mr. Russo admitted he has no basis for opining on password trading of age verification companies. *Id.* at 27:10-28:7.

213. Mr. Russo's experience and expertise is confined to the adult entertainment industry. Russo Testimony, 10/26/06 at 50:9-11.

**D. Implementation of COPA Will Not Materially Affect the Web**

**1. Businesses Can Adapt to a Minor Regulatory Change in the Adult Entertainment Industry**

214. COPA will have no significant negative impact on commercial web sites on the Internet. Testimony of Dr. Scott M. Smith, at 43:16-43:20 (Nov. 15, 2006) ("Smith Testimony"); Def.'s Ex. 91 at 5-11.

215. Commercial web sites will not lose revenue because individuals who are unwilling to provide a method of verification, by definition, will not make a purchase. Smith Testimony, 11/15/06 at 100:16-101:3.

216. In order to provide web site visitors with a "preview" of the material that is available beyond the verification screen, commercial web sites that use wise business strategy

will display pages that do not have explicit pornographic content. Smith Testimony, 11/15/06 at 179:11-180:6.

217. Commercial web sites that profit in whole or in part from advertising revenue also have an incentive to provide web pages without explicit pornographic content in order to sustain a higher level of traffic in the relatively “clean” teaser section. Smith Testimony, 11/15/06 at 102:12-103:9, 180:7-180:21.

218. The Internet is a stable, established business communications tool, and COPA will not require the creation of a new business model. COPA will have no negative effect on commercial innovation or business models used in Internet commerce. Smith Testimony, 11/15/06 at 42:17-43:20; 64:16-65:14; Def.’s Ex. 91 at 5-11.

219. In addition, a web site operator can set up a merchants account directly with payment card companies for 2.5 to 5 percent of sales dollar volume, or with a third-party payment processor for 8 to 15 percent of sales dollar volume. Clark Testimony, 11/14/06 at 239:19 – 240:15; Def.’s Ex. 93:0027.

220. Although requiring the use of a payment card to access online content might reduce the number of web site visitors, such visitors were unlikely to make a purchase and are unlikely to affect business results. Clark Testimony, 11/14/06 at 250:8-11. Visitors intending to make a purchase are not likely to be deterred by entering payment card information because they are likely to see the benefits of convenience and anonymity. Clark Testimony, 11/14/06 at 250:13-16. Moreover, requiring the use of a payment card should lead to repeat visits to the web site where the visitor has registered the payment card and should thus improve revenue levels. Clark Testimony, 11/14/06 at 250:19-24.

221. Plaintiffs' adult entertainment expert, Michael A. Russo, testified that putting less explicit content before a payment screen is an effective way to generate sales of explicit content. Russo Testimony, 10/25/06 at 218:20-23.

222. Web sites that utilize the services of a financial security company like Verisign will have a competitive advantage over other web sites because consumers will be more comfortable providing personal information on such web sites. Smith Testimony, 11/15/06 at 184:25-186:8. In fact, some of the Plaintiffs have availed themselves of these services, such as Condomania. The web site provides a secure server for the security of the online purchases and advises the purchasers that it meets security requirements against "hackers." Glickman Testimony, 10/30/06 at 145:25-146:8, 148:18-25.

**2. Consumers Are Adaptable and Increasingly Willing to Provide Personal Information on the Internet**

223. Internet commerce is thriving, and consumers are becoming increasingly comfortable with providing personal information on the Internet. Smith Testimony, 11/15/06 at 187:7-187:10, 189:16-190:9; Def.'s Ex. 91 at 4-11.

224. Consumers are increasingly willing to register or provide a credit card in order to gain access to web sites. Def.'s Ex. 91 at 8-9.

225. COPA will not inhibit qualified consumers from viewing online content. COPA's qualification standards, which require a password, registration or a purchase, are used successfully in many businesses where controlled products and services are purchased and consumed. Smith Testimony, 11/15/06 at 99:21 – 100:7; Def.'s Ex. 91 at 11-12.

226. Barriers are common in successful everyday shopping activities on the Internet. COPA's regulation of access to certain content by minors under the age of 17 will have no

significant adverse effect on adults who access, search for information, or use the Internet.

Def.'s Ex. 91 at 11-14.

227. The privacy protection required by COPA will increase consumer comfort with providing personal information on the Internet. Smith Testimony, 11/15/06 at 187:11-188:1.

228. Consumers are willing to provide credit card information on the Internet if they receive guarantees of privacy. A web site can increase consumer comfort with providing credit card information if it utilizes a service like Verisign to protect the security of online transactions. Smith Testimony, 11/15/06 at 182:17-184:19.

229. The modest burdens associated with COPA's affirmative defenses are analogous to the burdens associated with obtaining access to adult material in other settings, such as entries to nightclubs, adult bookstores, or NC-17 movies. Def.'s Ex. 91 at 11-14.

230. The willingness of consumers to provide personal information in order to achieve a goal is directly related to the perceived need to provide that personal information. As a result, a consumer may be unwilling to provide personal information to a stranger on the street, but willing to provide the information in order to access adult content on the Internet. Smith Testimony, 11/15/06 at 182:4-182:16. For example, web site visitors who wish to view premium content on Nerve.com must provide their name, address, email address, gender, credit card information, and a billing address. Griscom Testimony, 10/23/06 at 95:15-98:19; Def.'s Exs. 132-33, 139.

231. Visually consumed products are traditionally paid for prior to consumption. Consumers pay in advance to see movies, Broadway plays or musicals, art museum tours, and even national parks. Consumers expect to pay the required fee for visually consumed products

prior to consumption. Because COPA allows qualification by methods other than credit card use, the merchant retains the option to not require purchase before viewers can access content. Def.'s Ex. 91 at 12-13.

232. Consumers are willing to tolerate economic barriers in the form of time, inconvenience, or money to achieve a goal. From an economic perspective, this inelasticity of demand may be high where loyalty to a product is high, or where the consumer derives sufficient value from the product. Def.'s Ex. 91 at 13-14.

233. Although some consumers express concerns about providing personal information on the Internet, what consumers *do* is a better measure of actual consumer behavior than what consumers *say*. Behavioral data indicates that consumers are increasingly willing to provide personal information on the Internet. Smith Testimony, 11/15/06 at 186:9-187:16.

234. The pornography industry traditionally has faced both social and technological barriers that have not reduced industry demand. Every time a new medium for the dissemination of pornography is created, the technological advances have required not only a shift in consumer use behavior, but a shift in the business model within the industry. Yet there has not been a decrease in demand for the product category. Def.'s Ex. 91 at 13-14.

235. The consumption of pornography requires a motivated user, one who actively seeks access to web site pornography. The minimal qualification standards required by COPA are smaller than the barriers required to access pornography through any other medium because the purchase can be made in the privacy of one's home. Def.'s Ex. 91 at 13-14.

**3. Commercial Web Sites Easily Can Comply with COPA**

236. There is no technical obstacle that would prevent commercial adult pornography sites from utilizing one or more of the screening mechanisms set out in COPA for limiting access to harmful to minors material. Smith Testimony, 11/15/06 at 186:2-8; Def.'s Ex. 91 at 13.

237. Some commercial adult pornography sites do block all access to materials on their site unless and until a valid credit card or other form of adult identification (including adult password) is supplied; however, many adult pornography sites, numbering in the thousands, voluntarily choose to provide access to free sample images and texts. H.R. Rep. No. 105-775, at 10; Pls.' Ex. 25 at 0012-13.

238. COPA's affirmative defenses reflect Congress's understanding of the business model of commercial pornography to present "teasers" to garner business, and Congress's desire to ensure that the adult content is not contained in such publicly-accessible "teasers," but is restricted to the audience for which it is intended – adults. Congress noted that the affirmative defenses already "represent standard procedures for conducting commercial activity on pornographic Web sites," and that the affirmative defenses simply ensure that "the commercial pornographer . . . put sexually explicit images 'behind the counter.'" H.R. Rep. No. 105-775, at 13.

239. COPA's affirmative defenses are technologically feasible and readily available to commercial pornographers. Even though they are not covered by COPA, the Plaintiffs in this litigation would have no difficulty restricting access to content by minors. Indeed, most of the Plaintiffs currently accept payment cards or link to second-party sellers who do. Joint Ex. 1 at ¶¶ 100-09. For example, Condomania has permitted online purchases via credit card since 1996,

which has been successful. Glickman Testimony, 10/30/06 at 147:2-11; Def.'s Exs. 170, 171, 286 at 8. The web site provides a secure server for the security of the online purchases; it advises the purchasers that it meets security requirements against "hackers." Glickman Testimony, 10/30/06 at 145:25-146:8, 148:18-25.

240. Several Plaintiffs also currently offer subscriptions for content. In fact, Heather Corinna places the most explicit photographs on her Femmerotic web site behind a subscription barrier. Corinna Testimony, 11/2/06 at 123:14-16. Likewise, Nerve.com places its most explicit photographs behind a subscription barrier. Griscom Testimony, 10/23/06 at 65:10-13, 98:23-100:4.

241. Several Plaintiffs also delineate adult material within their websites. For example, Condomania has a splash page to warn viewers that they are entering a more explicit area of their web site. Glickman Testimony, 10/30/06 at 127:5-12. Likewise, Scarlet Letters places a symbol by the more adult content available on the web site. Corinna Testimony, 11/2/06 at 118:4-9; Def.'s Ex. 188. Salon also provides a warning when it feels that the subject matter calls for such a warning. Walsh Testimony, 10/23/06 at 179:2-10.

**E. COPA Provides a Worldwide Solution**

242. Plaintiffs have alleged that COPA does not apply to foreign web sites, and that this fact undermines its effectiveness. Plaintiffs are wrong as a matter of law and fact. As a legal matter, COPA can be applied worldwide, but, even if COPA did not apply overseas, it would still reach a vast majority of pornography on the Web.

**1. COPA Applies to Domestic and Foreign Websites**

243. COPA applies equally to operators of both foreign and domestic web sites.

COPA applies to anyone who “knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors . . .” 47 U.S.C. § 231(a)(1). Congress did not limit COPA’s application on the basis of the residency of the web site operator or the geographic location of the server hosting the web site.

244. The United States has entered into more than fifty bilateral Mutual Legal Assistance Treaties (MLATs) with other countries. These agreements provide the United States with the power, in investigating a violation of its laws that may have been committed by a resident of another country, to request the assistance of a signatory country to summon witnesses, to compel the production of evidence, to issue search warrants, and to serve process. *See, e.g.*, Treaty Doc. 105-12, 105th Cong., 1st Sess., Exec. Rpt. 105-22, 105th Cong., 2d Sess. (U.S.-Poland MLAT).

245. Credit card companies require their card-acquiring banks to monitor high risk merchants; this requirement includes the monitoring of the web sites of adult content web site operators. Clark Testimony, 11/14/06 at 173:17 – 174:24; Testimony of Ginger Bergman, at 31:1-9, 32:11-17 (Nov. 7, 2006) (“Bergman Testimony”); Testimony of Ira Cadwell, at 188:21-25 (Oct. 31, 2006) (“Cadwell Testimony”).

246. Card companies have embedded U.S. law into their merchant agreements; these agreements require foreign merchants doing business with U.S. customers to follow those

policies. Clark Testimony, 11/14/06 at 144:9 – 147:3. Indeed, testimony from the payment card companies confirms that a foreign merchant doing business with a U.S. customer is required by the payment card companies' foreign merchant agreement to comply with all applicable U.S. laws. Testimony of Joshua Peirez, MasterCard International, at 250: 24 – 251:4 (Oct. 31, 2006). There is no evidence that the card companies would exclude COPA from their world wide merchant agreements; Plaintiffs' payment card expert's entire analysis on the subject is flawed because he assumed that COPA is unconstitutional. Mann Testimony at 220:2 – 221:1.

247. Card companies can, and do, fine and even terminate merchants for failure to comply with card company policies. Clark Testimony, 11/14/06 at 148:20-23, 173:17 – 174:24.

248. Payment card companies recently joined with the National Center for Missing and Exploited Children to create the Financial Coalition Against Child Pornography to identify, investigate and terminate merchant agreements of web site merchants around the world that sell child pornography. Clark Testimony, 11/14/06 at 147:12 – 148:23. The Coalition has established a "cyber tip line" which the card companies themselves may use to report suspicious activity. Clark Testimony, 11/14/06 at 148: 12-16. In addition, card companies can terminate their merchant agreements with web site operators that are engaged in illegal activity. Clark Testimony, 11/14/06 at 148:18-23. The Financial Coalition could easily be expanded to identify, investigate and terminate merchants selling access to harmful-to-minors material in violation of COPA. Def.'s Ex. 93 at 46-47.

**2. Commercial Web Sites Can Tailor Their Sites to Different Geographic Regions**

249. Quova, Inc. is a provider of IP geolocation data and services to online businesses. Quova's patented technology provides the geographic location of web site visitors in real time, enabling businesses to detect fraud, manage digital rights, target content, conduct site analysis and ensure regulatory compliance. Quova's customers and partners include Major League Baseball, Cisco Systems, Dell, Amazon, and eBay. Testimony of Marie Alexander, at 5:5 – 5:9; 7:25 – 8:25; 9:20 – 10:4; 10:5 – 11:5; 19:18 – 20:19; 21:19 – 22:10 (Nov. 13, 2006) (“Alexander Testimony”).

250. Quova is used, *inter alia*, to comply with FFIEC guidance and the Office of Foreign Assets Control (OFAC) regulations, each of which have made knowing the location of online bank and credit union customers more important than ever. Quova is also used by the online gaming industry, which is subject to regulations restricting where they can offer their products and services. Alexander Testimony, 11/13/06 at 10:5 – 15:22.

251. Quova can be used for content localization to customize web site content to reflect the cultural preferences and priorities of online visitors from different regions and different countries. For example, a web site, when accessed from the United States, can contain different images than the same web site, when accessed from outside the United States. Similarly, content can be customized more narrowly such that web site visitors from San Francisco will see different images than visitors from Alabama. Alexander Testimony, 11/13/06 at 22:11 – 24:11.

252. Testing and audit results confirm that Quova can successfully ascertain the geographic location of a viewer to a web site, identifying the viewer's metropolitan service area,

within a 20- to 30-mile radius. Alexander Testimony, 11/13/06 at 27:8 – 28:6.

253. Quova can provide data on the geographic location of website visitors, even when such viewers are accessing a website through a proxy server, via a satellite connection or through a mobile device, such as a cell phone. Alexander Testimony, 11/13/06 at 19:3-20:19, 21:19-22:10. Previously, it was difficult to identify the location of website visitors accessing a website via such connections. For example, a proxy server may be put in place to hide the identity or location of a viewer to a website. Alexander Testimony, 11/13/06 at 16:2-17:22. In addition to its basic services, Quova provides geolocation products and services to ascertain the location of viewers accessing websites through such previously unidentifiable connections. Alexander Testimony, 11/13/06 at 37:14-38:1, 38:6-12.

**3. The Majority of Commercial Pornography Comes from the United States, or Has Ties to the United States**

254. The vast majority of adult web sites that are returned to search engine queries are hosted in the United States. For examples, 88.4% of the adult web pages that were returned in response to the random samples of search engine queries in Mr. Mewett's and Dr. Stark's study are domestically hosted, and 87.4% of the adult web pages returned in response to the most popular queries are domestically hosted. Def.'s Ex. 65. Large portions of these domestically-hosted adult web pages are not blocked by filtering software. Def.'s Exs. 72, 74, 78.

255. Plaintiff's witness, Matthew Zook, agrees with these calculations. His analysis has found that approximately 85% of all adult membership web sites are hosted in the United States. He also has found that 93.3% of all of what he called "feeder" adult web sites are hosted in the United States. Zook Testimony, 10/26/06 at 119:7-15; Pls.' Ex. 32 at 0016.

256. Adult web sites require the use of specialized hosting services that can provide large amounts of bandwidth and that can accommodate peaks in demand. Zook Testimony, 10/26/06 at 117:18 – 118:3. It is therefore unsurprising that the vast majority of adult websites would rely on locations in the United States for their hosting.

257. The connection of adult sites to hosting locations within the United States is important for purposes of the enforcement of COPA. Hosting data, unlike registration data, cannot be falsified. Def.'s Ex. 83 at ¶ 33. The fact that an adult site is hosted in the United States thus establishes that the operator has ties to the United States sufficient to establish personal jurisdiction. Further, in rem jurisdiction, and other forms of enforcement, can be exercised over the entities that provide hosting services to websites that violate COPA. For example, one tool available to law enforcement authorities would be the issuance of cease-and-desist orders to hosting services, requiring them to cease hosting websites that violate COPA's requirements. Mewett Testimony, 11/7/06 at 88:1-21.

258. Even for adult websites that are hosted outside the United States, the vast majority of those sites have a commercial link to the United States, that is, they are linked to a sales or billing mechanism to United States customers. Mewett Testimony, 11/7/06 at 191:8 – 192:1. For each of the sets of data that Mr. Mewett and Dr. Stark studied, even among the adult web sites that do not themselves directly solicit subscriptions or sales, between 88.2% and 95.9% of the "feeder" sites alone have commercial connections to the United States. Stark Testimony, 11/8/06, at 152:1 – 153:6; Def.'s Ex. 79.

259. Plaintiffs have questioned these calculations because some of the web pages that Mr. Mewett identified required several links to a web page with a pay mechanism. However, he

used precisely the same methodology that he uses for his law enforcement clients in determining whether nominally foreign child pornography sites actually have commercial links to the United States. Mewett Testimony, 11/8/06 at 68:20 – 69:5.

260. These commercial links to the United States are important for the purposes of the enforcement of COPA, as it establishes the range of adult web sites that would be subject to the provisions of credit card companies' merchant agreements requiring merchants to comply with United States law. *See* ¶¶ 246-48 *supra*. In addition, because the pay adult sites monitor their feeder affiliates to confirm compliance with applicable laws, these commercial links establish the enforceability of COPA against those sites. Russo Testimony, 10/26/06 at 38:11 – 39:4.

261. Plaintiffs have offered the testimony of Matthew Zook to claim that the proportion of adult sites in the United States is relatively low. Professor Zook's testimony is entitled to no weight, for three reasons. First, instead of relying on hosting data, he relied on registration addresses that have been self-reported by website operators. This registration data is frequently inaccurate, and indeed is frequently obviously falsified. Mewett Testimony, 11/7/06 at 188:13 – 189:7.

262. Professor Zook believed that a correlation could be drawn between registration data and the actual location of website operators. For this purpose, he relied on research he had performed finding such a correlation for the web sites of high-technology firms. Zook Testimony, 10/26/06 at 124:17 – 125:2. He did not consider whether such a correlation exists for the operators of adult web sites. Zook Testimony, 10/26/06 at 125:10-14. For obvious reasons, it is more likely that an adult web site operator would wish to disguise its locations than a high-technology firm would. Zook Testimony, 10/26/06 at 126:21 – 127:12.

263. Second, no reliable conclusions can be drawn from any of Professor Zook's data. He did not use random, representative samples of web sites, but instead used only web sites that he found on certain lists that he chose to use for his analysis. Those lists are not representative of any larger universe in the manner that Dr. Stark's samples are, and no conclusions can be reliably drawn from them. Stark Testimony, 11/8/06 at 141:9 – 142:22, 178:18 – 180:3. Professor Zook believed that, because his samples were “non-random cluster samples,” conclusions could be extrapolated from them. Zook Testimony, 10/26/06 at 134:14-22. As Dr. Stark explained, a wide range of authorities from the field of statistics reveal that Professor Zook is incorrect in his belief. Stark Testimony, 11/8/06 at 142:23 – 145:6.

264. Third, in addition to his use of unreliable registration data and his failure to use representative, random samples, Professor Zook used a methodology that cannot produce reliable results. He used a computer program to convert the individual web sites on his lists to “domain names,” for which he attempted to locate registration data. The registration data of what he called “domain names” does not bear any necessary relationship with the identity of the person who placed adult material on the web sites that are supposedly the basis of his study, however. Zook Testimony, 10/25/06 at 140:9-19.

265. More fundamentally, numerous errors arose as a result of this process of converting web sites to “domain names.” Many of the sites in his database are not adult web sites, and many more of them are not even web sites at all. Stark Testimony, 11/8/06 at 147:1 – 148:3. Because his initial data was not preserved, it is not possible to determine how many errors were included in Professor Zook's data. There are certainly many errors, however, and it

is possible that there are tens of thousands or even hundreds of thousands of errors. Stark Testimony, 11/8/06 at 147:10 – 148:17.

266. For these reasons, it is not possible to calculate the relative proportions of domestic adult web sites and foreign adult web sites, or the relative proportions of pay adult web sites and “feeder” adult web sites, from Professor Zook’s data. Stark Testimony, 11/8/06 at 148:18 – 150:5. It is also impossible to calculate from his data whether or not adult web sites are migrating overseas with time, as Professor Zook’s calculations to that effect depend entirely on the relative distributions of the sites on the lists that he chose to view at different times, and those distributions do not correlate to anything other than the lists themselves. Stark Testimony, 11/8/06 at 150:6 – 151:15.

267. In sum, no reliable conclusions can be drawn from Professor Zook’s data at all. Similarly, Mr. Russo, Plaintiffs’ adult entertainment expert proffered no data on the percentage of adult entertainment coming from overseas. Russo Testimony, 10/26/06 at 33:12-23. Mr. Mewett’s and Dr. Stark’s study, in contrast, is reliable, and it reveals that the vast majority of adult web pages are domestically hosted, or have commercial links to the United States.

## **PROPOSED CONCLUSIONS OF LAW**

### **I. STATUTORY INTERPRETATION**

#### **A. COPA Contains Statutory Limits to Ensure That It Is Narrowly Tailored to Commercial Pornography on the World Wide Web**

1. COPA’s objective is to prevent commercial pornography web sites from permitting access by minors to the material on their web sites. H.R. Rep. No. 105-775, at 15 (1998). This intent is reflected in the statutory language of COPA.

2. COPA establishes criminal and civil penalties when a person “knowingly and

with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors.” 47 U.S.C. § 231(a)(1)-(3).

3. COPA applies only to harmful-to-minors Web transmissions made by an entity “knowingly and with knowledge of the character of the material.” 47 U.S.C. § 231(a)(1).

Therefore, it does not apply to material that may have been placed on a web site by a user (such as on a message board, etc.), if the web site operator does not have knowledge of the material.

4. A person communicates “for commercial purposes” only if he “is engaged in the business of making such communications,” 47 U.S.C § 231(e)(2)(A), and a person is engaged in the business of making such communications only if he “devotes time, attention, or labor” to making harmful-to-minors communications “as a regular course of [his] trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person’s sole or principal business or source of income).” *Id.* at § 231(e)(2)(B).

5. COPA applies only to persons who seek to profit from placing harmful-to-minors material on their web sites as a regular course of business. 47 U.S.C. § 231(a)(1), (e)(2). This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

6. Only a person who “knowingly causes the material that is harmful to minors to be posted on the World Wide Web or knowingly solicits such material to be posted on the World Wide Web” will be considered to be “engaged in the business of making, by means of the World Wide Web, communications for commercial purposes that include material that is harmful to

minors.” 47 U.S.C. § 231(e)(2)(B).

7. COPA does not apply to Internet access service providers (commonly referred to as “ISPs,” such as America Online or Cox Communications) or Internet information location tool providers. 47 U.S.C. § 231(b)(2)-(3). An Internet information location tool is “a service that refers or links users to an online location on the World Wide Web. Such term includes directories, indices, references, pointers, and hypertext links.” *Id.* at § 231(e)(5). In addition, COPA does not apply to those “similarly engaged in the transmission, storage, retrieval, hosting, formatting, or translation . . . of a communication made by another person, without selection or alteration of the content of the communication.” *Id.* at § 231(b)(4).

**B. COPA’s Harmful-to-Minors Definition Narrowly Tailors COPA’s Restrictions to Material That Is Obscene for Minors**

8. COPA defines “material that is harmful to minors” as “any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind” that is “obscene” or that:

(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;

(B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

(C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

47 U.S.C. § 231(e)(6). Each of these prongs must be met in order for material to be deemed harmful to minors.

9. The first prong of COPA's harmful-to-minors definition focuses on the fact that the material is designed to appeal to the prurient interest. The standard of "appealing to the prurient interest" is well accepted in the regulation of obscene speech and requires that the material's "predominate appeal is to a shameful or morbid interest in nudity [or] sex." *Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 498 (1985). The term "prurient interest" refers to "sexual responses over and beyond those that would be characterized as normal." *Id.* It does not include material that, "taken as a whole, does no more than arouse good, old fashioned, healthy interest in sex." *Id.* at 499 (internal citation omitted).

10. The first prong of COPA's harmful-to-minors definition also contains a scienter requirement – the material must be "designed to" appeal to the prurient interest. 47 U.S.C. § 231(e)(6)(A). Therefore, unless a web site operator has the intent of appealing to the prurient interest, it will not be liable under COPA. This further narrows the reach of COPA to commercial pornography.

11. The language of the second prong of COPA's harmful-to-minors definition – the patently offensive prong – has been authoritatively interpreted by decisional law. Courts have indicated that these limitations are to be narrowly construed. *Osborne v. Ohio*, 495 U.S. 103, 113 (1990); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214 (1975). Mere nudity is not enough to render material harmful to minors. *See Osborne*, 495 U.S. at 112 ("depictions of nudity, without more, constitute protected expression"); *Erznoznik*, 422 U.S. at 213 n.10 ("It is clear . . . that under any test of obscenity as to minors not all nudity would be proscribed. Rather, to be obscene 'such expression must be, in some significant way, erotic.'") (quoting *Cohen v. California*, 403 U.S. 15, 20 (1971)).

12. The second prong of COPA's harmful-to-minors definition sets forth the specific acts or depictions necessary to bring material within the scope of the statute. It specifies that the depictions must contain sexual acts or contact, or a lewd exhibition of the genitals or post-pubescent female breast. 47 U.S.C. § 231(e)(6)(B). This description of what material is covered in the second prong distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be unconstitutional. *ACLU*, 521 U.S. at 879. This prong also further narrows the reach of COPA to target commercial pornography.

13. The third prong of COPA's harmful-to-minors definition is that the material, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors. In determining whether a given work has value, the proper inquiry is "whether a reasonable person would find such value in the material, taken as a whole." *Pope v. Illinois*, 481 U.S. 497, 501 (1987). Works with value are protected "regardless of whether the government or a majority of the people approve of the ideas whose those works represent." *Miller*, 413 U.S. at 34. This prong of COPA's harmful-to-minors definition further limits the reach of the statute to commercial pornography.

14. The third prong of COPA's harmful-to-minors definition – whether the work has value – is not determined by community standards, but, instead, sets a "national floor" of societal value. *Reno*, 521 U.S. at 873. The value of a work does not "vary from community to community based on the degree of local acceptance it has won." *Pope*, 481 U.S. at 500.

15. Although community standards are likely to be reasonably constant nationwide, this issue need not be considered at length because the Supreme Court determined that COPA's reference to community standards does not render the statute unconstitutional. *Ashcroft v.*

*ACLU*, 535 U.S. 564 (2002). In any event, as a factual matter, existing technology can be used to tailor access to web sites on a geographic basis. Age verification technology can be utilized to segregate access to a web site on a zip code basis. Dancu Testimony, 11/9/06 at 182:16 – 184:7; Def.’s Ex. 109 at 7. Geolocation software also can be used to achieve similar results on a regional or country-by-country basis. Alexander Testimony, 11/13/06 at 22:11 – 24:11.

16. Established precedent from state harmful-to-minors laws that contain definitions similar to COPA provides guidance as to the scope of harmful-to-minors material under COPA. *See, e.g., Reno v. ACLU*, 521 U.S. 844, 887 n.2 (1997) (listing state “harmful to minors” statutes) (O’Connor, J., concurring in part and dissenting in part); *Ginsberg v. State of New York*, 390 U.S. 629 (1968); *Am. Booksellers Ass’n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989); *Athenaco, Ltd. v. Cox*, 335 F. Supp. 2d 773, 781-82 (E.D. Mich. 2004). Works that have been found to have value for minors (and therefore, have been found not to be harmful to minors) under state harmful to minors laws include: *Lolita*, *Sanctuary*, *Of Mice and Men*, *The Catcher in the Rye*, *Portnoy’s Complaint*, *Joy of Sex*, Judy Blume’s *Forever*, *Hollywood Wives*, *Changing Bodies*, *Changing Lives*, and *Our Bodies, Ourselves*. *See Athenaco, Ltd.*, 335 F. Supp. 2d at 781; *Virginia v. Am. Booksellers Ass’n*, 372 S.E.2d 618, 622 & 625 (Va. 1988).

17. If material has serious value for older minors, it will be considered to have value for all minors. *See, e.g., Am. Booksellers v. Webb*, 919 F.2d 1493, 1504-05 (11th Cir. 1990) (in construing a statute defining minors as under 18 years old, concluding that “if any reasonable minor, including a seventeen-year-old, would find serious value, the material is not ‘harmful to minors’”); *Am. Booksellers Ass’n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989) (“if a work is found to have a serious literary, artistic, political, or scientific value for a legitimate minority of

normal, older adolescents, then it cannot be said to lack such value for the entire class of juveniles taken as a whole”) (quoting *Virginia v. Am. Booksellers Ass’n*, 372 S.E.2d 618, 624 (Va. 1988)); *Davis-Kidd Booksellers, Inc. v. McWherter*, 866 S.W.2d 520, 533 (Tenn. 1993) (finding material has serious value for minors within the meaning of that State’s display law, if it has serious value for “a reasonable seventeen year old minor”).

18. Both the first and third prong of COPA’s harmful-to-minors definition require that the material be judged “as a whole.” In *Kois v. Wisconsin*, the Court held that the “as a whole” language requires a “reviewing court [to] look at the context of material, as well as its content.” 408 U.S. 229, 231 (1972). This contextual analysis has been a mainstay of obscenity law since the 1950s. See *Roth v. United States*, 354 U.S. 476, 490 (1957) (requiring examination of “entire context” of books, pictures and circulars alleged to be obscene); *Kois*, 408 U.S. at 231 (holding that, even if particular photographs in a newspaper would be obscene “by themselves,” they could not be the basis for an obscenity prosecution where, “in the context in which they appeared in the newspaper they were rationally related to an article that itself was clearly [not obscene]”).

19. Because the determination of whether a web site is harmful to minors incorporates the “as a whole” language from obscenity law, the determination of whether a web site is harmful to minors cannot be made based on one page of a web site (or one image on a web site) alone. Rather, the context of the entire web site ordinarily must be taken into account in order to make the legal determination of what is harmful to minors.

20. Web sites are analogous to magazines, in which individual pictures or articles are examined in the context of the entire magazine. *Manual Enterprises, Inc. v. Day*, 370 U.S. 478,

489 (1962); *Ginzburg v. United States*, 383 U.S. 463, 466 n.5 (1966). Plaintiffs such as Salon and Nerve are online magazines. Walsh Testimony, 10/23/06 at 107:14-16; Griscom Testimony, 10/23/06 at 61:15-21.

21. The fact that COPA applies to the Internet does not obviate the need or ability to view the material in context, generally looking to the web site as a whole. A constitutional method for evaluating content does not become unconstitutional merely because it is applied to a new medium. Material on the Internet can be viewed, and has been viewed by the courts, in context. For example, in a defamation action, the Ninth Circuit applied the non-Internet defamation standards to material found on the Internet, which included looking at the allegedly defamatory web page in context with other web pages on the defendant's web site. *Knievel v. ESPN*, 393 F.3d 1068, 1076-77 (9th Cir. 2005).

22. The legal analysis of evaluating work as a whole is not affected by the testimony of fact witnesses. Plaintiffs seek to rely on Defendant's expert, Paul Mewett, to support their argument that individual web pages are the legally determinative factor to consider in determining the legal interpretation of COPA's "as a whole" language. Closing Argument, 11/20/06 at 17:17 – 19:1. Such a conclusion would be in error. Mr. Mewett was asked to perform a study of the effectiveness of filters for Defendant. He performed this study by identifying web pages to ascertain if filters would block them, based on criteria commonly followed by the filtering companies themselves. Mr. Mewett is not an attorney and was not tasked with making the determination of what material falls under the legal definition of "harmful to minors" pursuant to COPA, or how COPA's "harmful to minors" definition is properly interpreted. Mewett Testimony, 11/7/06 at 200:19-23.

23. The issue of the meaning of COPA's harmful-to-minors definition, including the "as a whole" language, is one of legal interpretation for the Court to determine, and the Court follows the well-established legal standards from obscenity case law to do so.

24. Interpreting COPA's "as a whole" language to include context from the website is consistent with COPA's "engaged in the business" requirement. Web sites engaged in the business of distributing harmful-to-minors material would, taken as a whole, meet COPA's harmful-to-minors definition. Web sites with only isolated images of explicit material are, most likely, not engaged in the business of distributing harmful-to-minors material.

25. Subsequent to the passage of COPA, some state harmful-to-minors laws have been deemed unconstitutional by some courts on Commerce Clause and other grounds. *See, e.g., PSINet v. Chapman*, 362 F.3d 227 (4th Cir. 2004); *ACLU v. Johnson*, 194 F.3d 1149 (10th Cir. 1999); *Am. Booksellers Found. v. Dean*, 342 F.3d 96 (2d Cir. 2003); *Cyberspace Communications, Inc. v. Engler*, 142 F. Supp. 2d 827, 830 (E.D. Mich. 2001). None of these cases invalidated state harmful-to-minors laws based on the vagueness of the harmful-to-minors definitions. In fact, courts continue to uphold the *Ginsberg/Miller* state harmful-to-minors definitions. *See Athenaco, Ltd. v. Cox*, 335 F. Supp. 2d 773, 781-82 (E.D. Mich. 2004) ("The Court is constrained to agree with Defendants that Plaintiffs have operated under the definitions codified in [Michigan's harmful to minors law] since 1978, and do not credibly establish how the Act's recent amendments . . . throws [sic] any section of the harmful to minors' definition, and by extension, the category of materials to which that definition applies, into doubt."); *State of Texas v. Stone*, 137 S.W.3d 167, 181 (Tex. Ct. App. 2004) ("Section 43.24 of the Texas Penal Code is a constitutionally permissible variable obscenity statute of the type approved in

*Ginsberg and Reno.*”).

26. COPA defines a minor as “any person under 17 years of age.” *Id.* at § 231(e)(7).

This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

**C. COPA’s Affirmative Defenses**

27. COPA provides “an affirmative defense to prosecution” if a person, “in good faith, has restricted access by minors to material that is harmful to minors.” 47 U.S.C. § 231(c)(1). A person qualifies for this affirmative defense by (A) “requiring use of a credit card, debit account, adult access code, or adult personal identification number,” (B) “accepting a digital certificate that verifies age,” or (C) taking “any other reasonable measures that are feasible under available technology.” *Id.*

28. COPA prohibits the disclosure of “any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older.” 47 U.S.C. § 231(d)(1)(A). Further, the statute requires that a company that verifies the age of an adult who accesses harmful-to-minors material to “take such actions as are necessary to prevent unauthorized access to such information by a person other than the [company] and the [adult].” *Id.* at § 231(d)(1)(B). Anyone who willfully or knowingly violates these provisions is subject to criminal penalties. *See* 47 U.S.C. § 501. This privacy protection provision will increase consumer comfort with providing personal information on the Internet. Smith Testimony, 11/15/06 at 187:11-188:1.

## II. PLAINTIFFS LACK STANDING

### A. Web Site Plaintiffs Lack Standing

29. Plaintiffs maintain the burden of establishing standing at each stage of the litigation. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992).

30. None of the Plaintiffs has standing to maintain this action. In order to maintain standing, a party must show that he has sustained or is immediately in danger of sustaining some direct injury due to the challenged conduct and this injury or threat of injury must be real and immediate, not conjectural or hypothetical. *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983).

31. Allegations of subjective chill do not suffice to maintain standing. *Laird v. Tatum*, 408 U.S. 1, 13-14 (1972); *Aiello v. City of Wilmington*, 623 F.2d 845, 857 (3d Cir. 1980); *Am. Library Ass'n v. Barr*, 956 F.2d 1178, 1194 (D.C. Cir. 1992).

32. The only testimony offered by Plaintiffs at trial was that they have a subjective fear of COPA's potential impact on their speech, which is insufficient to confer standing.

33. Plaintiffs cannot maintain standing for their vagueness claim (Count Four). In the Third Circuit, "a vagueness attack requires the plaintiff to show that he himself was injured by the vague language of the regulation." *Gibson v. Mayor & Council of Wilmington*, 355 F.3d 215, 225-26 (3d Cir. 2004). None of the Plaintiffs demonstrated at trial that they would be injured by the allegedly vague language of COPA.

34. The testifying Plaintiffs did not establish that their web sites met all three prongs of COPA's harmful-to-minors definition. For example, many of the Plaintiffs' websites are educational or health-related in nature. See Glickman Testimony, 10/30/06 at 138:19-141:20;

Tepper Testimony, 10/30/06 at 176:18-177:5, 179:24-180:16; Corinna Testimony, 11/2/06 at 73:25-74:2. Moreover, each Plaintiff testified as to the serious value of his or her web site. Griscom Testimony, 10/23/06 at 58:14-59:4; Walsh Testimony, 10/23/06 at 138:11-16; Glickman Testimony 10/30/06 at 131:18-23; Tepper Testimony, 10/31/06 at 6:8-17; Testimony of Aaron Peckham, at 28:10-23 (Oct. 31, 2006) (“Peckham Testimony”); Corinna Testimony, 11/2/06 at 73:6-11, 73:25 – 74:9, 91:23 – 92:3, 93:11-20.

35. Professor Reichman testified that Plaintiffs reasonably feared prosecution under COPA on the basis of anecdotal evidence of challenges to material in public schools and libraries. Professor Reichman’s experience is based on parental concerns in a very different situation – that of how parents want their children educated in public schools and what materials they want available to their children in public libraries. Testimony of Henry Reichman, at 24:5-20, 48:2-18, 52:9-16 (Oct. 30, 2006) (“Reichman Testimony”). COPA does not purport to regulate everything that parents might be concerned with regarding their children. Instead, in furtherance of a compelling government interest, COPA regulates a narrow category of speech that is deemed to be obscene as to minors. 47 U.S.C. § 231(e)(6).

36. Professor Reichman states that certain Plaintiffs fear prosecution because certain material in schools and libraries is challenged by parents. However, these challenges are not tied to the language of the statute. Therefore, Professor Reichman’s conclusions based on generalized concerns raised by parents in the public school and public library contexts are inapposite to the issue before the Court. Reichman Testimony, 10/30/06 at 53:14 – 54:8, 72:8-13. Professor Reichman is not a lawyer and cannot testify as to the scope of material that falls within COPA’s harmful-to-minors definition. *Id.* at 17:11-12.

37. Professor Reichman's conclusions also should be given little weight because they are internally inconsistent. In many instances, Professor Reichman did not know the outcome of the challenges upon which he reported. Reichman Testimony, 10/30/06 at 59:10-23, 62:22 – 63:3, 67:10 – 68: 25, 73:10 – 74: 4. Professor Reichman never opined that the examples of challenges cited in his report were harmful to minors. In fact, in several instances, Professor Reichman does *not* believe that the examples of challenged material would fall within COPA's harmful-to-minors definition. *Id.* at 61:7 – 62:3, 72:18 – 73:6, 74:19-25, 78:12 – 79:15. In addition, Professor Reichman states that certain material is challenged by parents because parents deem the material obscene, although Professor Reichman opines that Plaintiffs do not reasonably fear prosecution under obscenity laws. *Id.* at 77:11 – 78:11, 79:1-21. Therefore, the fact that a parent may label material in a certain manner as it relates to school curricula or libraries does not have a correlation to the legal meaning of "harmful to minors."

38. Professor Reichman concluded that, in his opinion, there is nothing on the Plaintiffs' websites that could be deemed harmful to minors. Reichman Testimony, 10/30/06 at 80:2-8.

**B. Non-Testifying Plaintiffs Lack Standing**

39. Several Plaintiffs have not demonstrated standing because they did not participate at trial and did not present evidence as to the requisite injury to maintain standing. *See City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983). The following Plaintiffs did not present evidence in support of their claims, and therefore lack standing: Free Speech Media, Philadelphia Gay News, Powells' Bookstores, and the Electronic Privacy Information Center. Each of these Plaintiffs must be dismissed from this lawsuit for lack of standing. *Lujan v.*

*Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (party asserting jurisdiction needs to prove it at each stage of litigation).

40. Likewise, the associations involved in this lawsuit lack standing because there was no testimony from their members regarding any injury, which is a requirement for standing. *City of Los Angeles v. Lyons*, 461 U.S. 95, 101-02 (1983). An association has standing to sue on behalf of its members when: (a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit. *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977).

41. There are three associations that are suing on behalf of their members in this lawsuit: the American Civil Liberties Union ("ACLU"), the Electronic Frontier Foundation ("EFF"), and the American Booksellers' Association for Free Expression ("ABFFE"). ACLU asserted that it was suing on behalf of its members Patricia Nell Warren and Lawrence Ferlinghetti, among others. EFF asserted that it was suing on behalf of its member Bill Boushka, among others. ABFFE asserted that it was suing on behalf its members. None of the members of the Plaintiff organizations testified at trial.

42. Because of the lack of evidence from members of associational plaintiffs ACLU, ABFFE and EFF, these associations have not demonstrated that their members would have standing to sue in their own right. *Hunt v. Washington State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977). Because this is a requirement of standing for associations, these associational Plaintiffs must be dismissed for lack of standing.

43. ACLU, ABFFE, and EFF have also sued on behalf of co-called “listener” members, who alleged that COPA violated their right to access speech on the web. The associations have not produced evidence sufficient to state a claim on behalf these so-called “listener” members. There has been no trial testimony by any individual asserting that his or her rights as a listener has been or will be infringed by COPA. Any listener Plaintiffs should have come forward with evidence to prove his standing, and cannot rest on the allegations of the Complaint to establish standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (party asserting jurisdiction needs to prove it at each stage of litigation); *Hunt v. Washington State Apple Adver. Comm’n*, 432 U.S. 333, 343 (1977) (association must show members have standing to sue in their own right for associational standing). Therefore, the associations bringing claims on behalf of “listener” members must be dismissed for lack of standing.

44. ACLU alleges to represent members that are older minors seeking to access speech. There was no evidence at trial from ACLU members that are older minors to establish the requisite injury to sustain standing. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (party asserting jurisdiction needs to prove it at each stage of litigation); *Hunt v. Washington State Apple Adver. Comm’n*, 432 U.S. 333, 343 (1977) (association must show members have standing to sue in their own right for associational standing). Therefore, ACLU cannot maintain standing based on injuries to its members that are minors.

### **III. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON PLAINTIFFS’ FIRST AMENDMENT OVERBREADTH CLAIM**

45. When addressing an overbreadth challenge, the Court “should, of course, construe the statute to avoid constitutional problems, if the statute is subject to such a limiting construction.” *New York v. Ferber*, 458 U.S. 747, 769 n.24 (1982).

46. The Court will invalidate a statute as facially overbroad only as a last resort and only if the Act has a substantial number of impermissible applications. *United States v. Knox*, 32 F.3d 733, 751-52 (3d Cir. 1994).

47. The Supreme Court has noted that facial challenges are “to be discouraged,” and it has “recognized the validity of facial attacks alleging overbreadth . . . in relatively few settings, and, generally, on the strength of specific reasons weighty enough to overcome our well-founded reticence.” *Sabri v. United States*, 541 U.S. 600, 609-10 (2004).

**A. Because COPA Regulates Only Commercial Entities, Intermediate Scrutiny Should Be Applied**

48. The statutory text and legislative history demonstrate that COPA applies to commercial speech. COPA regulates only “communication[s] for commercial purposes,” 47 U.S.C. § 231(a)(1), and “person[s] engaged in the business of making such communications.” *Id.* at § 231(e)(2)(A). As Congress noted when it passed COPA, pornography on the Internet is inherently commercial in nature, and free teasers are used to entice a consumer into making a commercial transaction. S. Rep. No. 105-225, at 1-2 (1998).

49. Some commercial pornography web sites propose a commercial transaction directly to the consumer on their own site, while others do so through advertisements on affiliated sites. The latter are so-called “feeder web sites.” Zook Testimony, 10/26/06 at 114:16-115:10; Pls.’ Ex. 29 at 3-4. COPA regulates the advertising on both types of web sites because both business models make “communication[s] for commercial purposes.” 47 U.S.C. § 231(a)(1).

50. COPA does not reach non-commercial speech, even on the World Wide Web. 47 U.S.C. § 231(a)(1), (e)(2)(A). Joint Ex. 1 at ¶ 119. As a result, the web site operated by

Plaintiffs' witness Wayne Snellen, which is a 501(c)(3) non-profit organization, would not be subject to COPA. Testimony of Wayne Snellen, at 160:10 – 161:23 (Nov. 2, 2006); Def.'s Ex. 461 at 2. Similarly, the web site operated by Plaintiffs' witness Barbara DeGenevieve would not be regulated by COPA because it does not sell content or goods and does not contain any advertisements. Testimony of Barbara DeGenevieve, at 61:22 – 63:10 (Nov. 1, 2006).

51. Because COPA regulates commercial speech, such as the content of “free teasers” and “feeder web sites” that serve as advertisements for the enticement of a subsequent sale, it should be reviewed using intermediate scrutiny. Laws regulating commercial speech are permissible if the government has a “substantial interest” that is directly advanced by “narrowly drawn” regulation. *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of N.Y.*, 447 U.S. 557, 564-65 (1980). In other words, there must be a “reasonable fit” between the statute's ends and the means chosen to accomplish those ends. *Florida Bar v. Went For It, Inc.*, 515 U.S. 618, 632 (1995).

52. COPA easily satisfies this test. As shown below, Defendant has not only a substantial interest, but a compelling one, in protecting minors from exposure to sexually explicit material on the World Wide Web. COPA will help protect minors to a material degree: there is a reasonable fit between Congress's ends in enacting COPA and the commercial pornography that it regulates.

53. As an initial matter, “the overbreadth doctrine does not apply to commercial speech.” *Vill. of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 497 (1982). *See also Excalibur Group, Inc. v. City of Minneapolis*, 116 F.2d 1216, 1225 (8th Cir. 1997). Therefore, Plaintiffs cannot raise a facial overbreadth challenge to COPA, as the issue of

whether COPA applies in an overbroad manner to speakers other than Plaintiffs is “irrelevant” for constitutional purposes. *Vill. Of Hoffman Estates*, 455 U.S. at 497.

**B. COPA Satisfies Even Strict Scrutiny**

**1. Legal Standards**

54. Even if the Court considers COPA to be a content-based restriction for which strict scrutiny applies, Defendant is able to meet his burden. In such a situation, the statute at issue “must be narrowly tailored to promote a compelling Government interest” to be constitutional under the First Amendment. *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 813 (2000).

55. If strict scrutiny were to apply to COPA, in order to succeed on their overbreadth challenge, Plaintiffs must demonstrate that “no set of circumstances exists under which the Act would be valid.” *United States v. Salerno*, 481 U.S.739, 745 (1987), or that COPA is “substantially overbroad.” *New York State Club Ass’n v. City of New York*, 487 U.S. 1, 11 (1988). “The overbreadth claimant bears the burden of demonstrating, from the text of [the law] and from actual fact,” that substantial overbreadth exists. *Virginia v. Hicks*, 539 U.S. 113, 122 (2003).

56. For a law to be unconstitutionally overbroad, its impermissible applications must be “‘substantial,’ not only in an absolute sense, but also relative to the scope of the law’s plainly legitimate applications.” *Virginia v. Hicks*, 539 U.S. 113, 120 (2003).

57. The legal standards to demonstrate overbreadth are not the same as that which is required to demonstrate standing. While a plaintiff can demonstrate standing based on a credible fear of prosecution under a reasonable interpretation of the statute, it must show more to prevail

in an overbreadth claim. Even if a plaintiff has standing, if he does not demonstrate substantial overbreadth of a statute, his overbreadth claim must fail. *See Nitke v. Gonzales*, 413 F. Supp.2d 262, 272-73 (S.D.N.Y. 2005) (finding that plaintiffs met standing requirements but failed to present evidence of substantial overbreadth), *aff'd* 126 S. Ct. 1566 (2006).

58. Plaintiffs have failed to meet their burden of showing that COPA has no constitutional applications or is “substantially overbroad.” *See New York v. Ferber*, 458 U.S. 747, 769 n.24 (1982).

## **2. The Government Has a Compelling Interest in Protecting Minors**

59. The Defendant has a compelling interest in protecting minors from exposure to sexually explicit material on the World Wide Web. *Ashcroft v. ACLU*, 542 U.S. 656, 675 (2004). The Supreme Court has firmly established that the government has “a compelling interest in protecting the physical and psychological well-being of minors” and that “[t]his interest extends to shielding minors from the influence of literature that is not obscene by adult standards.” *Sable Comm’n of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989). *See also Reno v. ACLU*, 521 U.S. 844, 864-65 (1997); *Ginsburg v. New York*, 390 U.S. 629, 639 (1968).

60. There are two components to the compelling government interest in the protection of minors. The government has an interest in aiding parents who wish to protect their children from the harmful effects of pornographic material. *Reno v. ACLU*, 521 U.S. 844, 865 (1997). In addition, the government has an independent interest in the well being of the nation’s minors. *Id.*

### 3. COPA Is Narrowly Tailored

61. COPA's definition of "harmful to minors," found at 47 U.S.C. § 231(e)(6), is directly derived from the tests for obscenity as to minors developed by the Supreme Court in *Miller v. California*, 413 U.S. 15 (1973), and *Ginsberg v. New York*, 390 U.S. 629 (1968), and patterned after the narrowly interpreted state harmful-to-minors statutes with harmful-to-minors definitions that have been upheld by numerous courts. H.R. Rep. No. 105-775, at 27-28 (1998).

62. As the decisional law surrounding the regulation of obscenity-related speech makes evident, the harmful-to-minors standard employed in COPA reaches only materials that are clearly pornographic and inappropriate for minors. COPA does not apply to materials that merely contain nudity or profanity or that merely espouse controversial political or sexual viewpoints, as those materials would not fall within the established definition of "harmful to minors" adopted by COPA. *See* H.R. Rep. No. 105-775, at 28; *see also Osborne v. Ohio*, 495 U.S. 103, 112 (1990); *New York v. Ferber*, 458 U.S. 747, 765 n.18 (1982); *Board of Education v. Pico*, 457 U.S. 853 (1982); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 214 n.10 (1975); *Jenkins v. Georgia*, 418 U.S. 153, 161 (1974).

63. In drafting COPA, Congress addressed the specific concerns raised by the Supreme Court to ensure the law would be narrowly tailored. COPA applies only to material posted on the World Wide Web, where age screening is both technologically feasible and affordable. 47 U.S.C. § 231(a)(1); H.R. Rep. No. 775 at 13-14. This narrow tailoring distinguishes COPA from the Communications Decency Act, which the Supreme Court found to be overbroad. *ACLU*, 521 U.S. at 879.

64. COPA defines minors as those under the age of 17, an age distinction that the

Supreme Court has upheld in the harmful-to-minors context. 47 U.S.C. § 231(e)(7). *Ginsberg v. N.Y.*, 390 U.S. 629 (1968).

65. As described in Section I.B, *supra*, COPA's definition of "harmful to minors" is narrowly tailored to reach only that speech that is obscene as to minors. 47 U.S.C. § 231(e)(6).

66. Because COPA does not apply to hosting entities, Plaintiffs' concerns regarding both the content of Web sites to which they provide links, and materials that are posted on their sites by persons other than themselves through the various Web-based interactive fora they purport to include on their sites are invalid and unwarranted. 47 U.S.C. § 231(b)(4).

67. COPA does not ban or significantly restrict protected speech by adults. The requirement that COPA-regulated speech be placed behind an age-verification "curtain" is no more restrictive than state-law display requirements that require harmful-to-minors speech to be physically segregated, placed behind blinder racks, or accessed only by a token or other device intended to verify adult access. *See Crawford v. Lungren*, 96 F.3d 380 (9th Cir. 1996); *American Booksellers v. Webb*, 919 F.2d 1493 (11th Cir. 1990); *Upper Midwest Booksellers Ass'n v. City of Minneapolis*, 780 F.2d 1389 (8th Cir. 1986); *M.S. News Co. v. Casado*, 721 F.2d 1281 (10th Cir. 1983). COPA is akin to an electronic bouncer and, accordingly, is constitutional.

68. COPA does not "ban" online communications that are harmful to minors. Instead, COPA regulates only the manner in which such communications can be displayed so as to restrict minors' access to them.

69. The Supreme Court has repeatedly held that Congress has authority to enact laws that are narrowly tailored to protect minors from harmful material. *Reno v. ACLU*, 521 U.S. at 864-865; *Sable*, 492 U.S. at 126; *Ginsberg*, 390 U.S. at 639. That authority necessarily includes

the power to place reasonable burdens on adults when it is necessary to protect minors from harmful material. *Id.* at 639-40. Any other rule would strip Congress of the ability to vindicate that compelling interest.

70. Congress borrowed from a solid foundation of cases upholding similar measures in formulating a structure that places the burden on the information content provider to restrict access to harmful-to-minors communications, rather than on the parent or child to avoid those communications. *See Dial Information Servs. v. Thornburgh*, 938 F.2d 1535 (2d Cir. 1991) (citing *Sable Communications of California, Inc. v. FCC*, 492 U.S. 115 (1989)); *Information Providers' Coalition for Defense of the First Amendment v. FCC*, 928 F.2d 866 (9th Cir. 1991). Such a scheme is clearly constitutional.

#### **4. Plaintiffs' Arguments that COPA's Narrow Tailoring Renders COPA Ineffective Are Without Merit**

71. Plaintiffs assert that COPA is not effective because it applies only to the Web, and not to other aspects of the Internet, such as e-mail, Usenet newsgroups, Instant Messaging, chat, and peer-to-peer. Plaintiffs are judicially estopped from raising this argument, because it runs contrary to a position that Plaintiffs successfully took in earlier litigation. *See New Hampshire v. Maine*, 532 U.S. 742, 749 (2001). Before the Supreme Court in *Reno v. ACLU*, Plaintiff ACLU successfully argued that the Communications Decency Act was unconstitutionally overbroad, in part because it applied both to non-commercial speech as well as commercial speech, and also in part because it applied to e-mail, chat rooms, newsgroups, and other forms of communication on the Internet beside the World Wide Web. Br. of Appellees, *Reno v. ACLU*, No. 96-511, at 28-29 (filed Feb. 20, 1997) (available at 1997 WL 74738). Plaintiffs cannot reverse course and argue that COPA will be effective only if it regulates a broader range of speech, and if it regulates

other forms of Internet communication.

72. The testimony of Plaintiffs' witnesses regarding other Internet applications for which COPA does not apply – e-mail, voice over IP protocol, chat, and instant messaging – is legally irrelevant. These are applications that are not publicly accessible in the same manner as the World Wide Web and, therefore, they do not pose the same concerns for Congress as does commercial pornography on the Web. COPA addresses the specific problem of commercial pornography on the Web, and COPA is not unconstitutional because it focuses on this specific problem. The Web is an appropriate legislative focus because it is so widely used by minors; the majority of teenagers go online daily (Pls.' Ex. 17 at 0002), and spend 1-5 hours a week surfing the Web (Pls.' Ex. 54 at 0192). The Supreme Court has noted that, even in First Amendment cases to which strict scrutiny applies, "reform may take one step at a time, addressing itself to the phase of the problem that seem most acute to the legislative mind." *McConnell v. Federal Election Comm'n*, 540 U.S. 93, 207-08 (2003).

73. Plaintiffs' argument that COPA does not cover peer-to-peer networks is legally irrelevant. The Supreme Court has noted that, even in First Amendment cases to which strict scrutiny applies, "reform may take one step at a time, addressing itself to the phase of the problem that seem most acute to the legislative mind." *McConnell v. Federal Election Comm'n*, 540 U.S. 93, 207-08 (2003). There has been no testimony at trial that commercial pornography is distributed through peer-to-peer networks, or that it encompasses the problems of widespread distribution of pornography such as is available on the Web. Peer-to-peer communications are *not* commercial in nature. Instead, files are shared directly by users on a non-commercial basis. Pls.' Ex. 54 at 0160. Plaintiffs' own expert was unable to provide data regarding commercial

adult entertainment on peer-to-peer networks. Russo Testimony, 10/26/06 at 31:12-21.

74. Plaintiffs' proffered testimony about the Internet protocols other than HTTP is also legally irrelevant. Plaintiffs' expert Dr. Felten offered his opinion that some harmful-to-minors materials available on the Internet could be distributed through protocols other than hypertext transfer protocol (HTTP), and thus be beyond the reach of COPA. Dr. Felten, however, is not an expert in statutory construction. Felten Testimony, 10/25/06 at 43:2-9. He erred in two important ways in his interpretation of COPA, and thus significantly understated the extent to which COPA would regulate harmful-to-minors materials on the Internet.

75. First, Dr. Felten apparently assumed that, in order to be subject to COPA, a web site operator must use HTTP, or a successor protocol, in placing harmful-to-minors material on to the Internet. But, in COPA's definition of material that is available "by means of the World Wide Web," the phrase "using hypertext transfer protocol or any successor protocol" does not modify any action taken by the web site operator. Instead, that phrase modifies the viewer's means of accessing that material. 47 U.S.C. § 231(e)(1) ("... so that it is publicly accessible, over the Internet, using hypertext transfer protocol or any successor protocol."). *See, e.g., Barnhart v. Thomas*, 540 U.S. 20, 26 (2003) (under "rule of the last antecedent," limiting clause or phrase should be read to limit only the noun or phrase that it immediately follows). Thus, so long as the viewer of a web site uses – or could use – HTTP or a successor protocol in the course of accessing the particular file, the material in that file will be subject to COPA's regulatory requirements.

76. Second, Dr. Felten also assumed that a particular file containing harmful-to-minors material must be accessed through the use of HTTP. He testified that a particular file that

could be accessed through the use of a different protocol (such as audio or video streaming) would not be subject to COPA, even if that file had also been placed on to a web site that uses the HTTP protocol. Felten Testimony, 10/25/06 at 49:9 -51:5. COPA, however, does not require that a particular file must be *accessed* through the use of HTTP to be subject to its regulatory terms. Instead, a file that is “*accessible*” using HTTP is subject to COPA, even if the same file may also be accessible through another method, so long as it is a “publicly accessible” file. 47 U.S.C. § 231(e)(1). Thus, the particular example cited by Dr. Felten – a file containing streaming audio that is accessible through the whyy.org web site – would, contrary to his opinion, be subject to COPA if it contained harmful-to-minors material. Pls.’ Ex. 119 at 0010.

77. Dr. Felten testified that it is technically possible for an adult web site operator to use the FTP protocol to distribute adult content. Dr. Felten’s supposition that web sites may convert to a non-HTTP protocol is legally irrelevant. COPA addresses a current problem, and Congress need not legislate to address theoretical possibilities. *See McConnell*, 540 U.S. at 207-08. If and when theoretical possibilities become real problems, Congress has the ability to address these problems through additional laws. In any event, any commercial pornography that is placed on the Internet through the FTP protocol, but for which the viewer would use the HTTP protocol in the course of reaching that material, is covered by COPA. Given numerous practical considerations, it is very unlikely that commercial pornographers would choose to use the FTP protocol to distribute their material, even if it is technically possible for them to do so. Mewett Testimony, 11/7/06 at 179:20-24.

78. Adult material distributed through the use of protocols such as peer-to-peer file-trading protocols can be blocked through the use of application-blocking software. Joint Ex. 1 at

¶ 95. Application-blocking software cannot block access to the whole of the World Wide Web in its entirety in the same manner, however, without raising serious concerns as to the overblocking of all of the legitimate content on the Web. It is therefore appropriate for COPA's regulatory regime to be focused on material distributed over the Web.

**5. Plaintiffs' Argument that COPA Is Ineffective Because It Does Not Apply to Overseas Web Sites Is Incorrect as a Matter of Law**

79. COPA applies equally to operators of both foreign and domestic web sites. COPA applies to anyone who “knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors . . .” 47 U.S.C. § 231(a)(1). Congress did not limit COPA's application on the basis of the residency of the web site operator or the geographic location of the server hosting the web site. The statute is replete with references to the World Wide Web and Internet—terms which by definition have no geographic limitation. For example, the Internet is defined as the “combination of computer facilities and electromagnetic transmission media . . . comprising the interconnected worldwide network of computer networks . . .” *Id.* at § 231(e)(3).

80. Under established law, courts have jurisdiction to enforce COPA against foreign web site operators. The Third Circuit has applied other pornography-related statutes abroad when the goal is to “contain the evils caused on American soil by foreign as well as domestic suppliers” of pornography. *United States v. Harvey*, 2 F.3d 1318, 1327 (3d Cir. 1993) (internal citation omitted); *see also United States v. Thomas*, 893 F.2d 1066 (9th Cir. 1990), *cert. denied*, 498 U.S. 826 (1990) (same).

81. COPA would be effective in protecting minors from exposure to sexually explicit material on the World Wide Web, whether that material is produced in the United States or in other countries. A significant portion of that material is found on web sites hosted in the United States, and the most popular pornography is disproportionately found within the United States. Def.'s Ex. 65; Stark Testimony, 11/8/06 at 182:4-11. Nonetheless, United States laws governing the Internet can be directly enforced even against operators of web sites that are hosted abroad. 47 U.S.C. § 231(a)(1).

82. COPA also can be enforced abroad indirectly through the payment card industry's enforcement of terms in payment agreements. Clark Testimony, 11/14/06 at 144:9 – 147:3. The payment card industry can require foreign producers of sexually explicit material who make that material available to minors in the United States over the World Wide Web to comply with United States laws. The vast majority of adult sites have commercial links to the United States. Stark Testimony, 11/8/06 at 152:1 – 153:6; Def.'s Ex. 79. In the unlikely event that the payment card industry does not voluntarily comply with United States law, nothing prevents Congress from enacting legislation to ensure that COPA is enforced by the industry worldwide.

**6. COPA Is the Most Effective Way to Prevent Minors from Accessing Harmful Material**

83. COPA provides affirmative defenses to prosecution that are feasible and not burdensome. 47 U.S.C. § 231(c)(1)(A)–(C). COPA will be effective in protecting minors from exposure to sexually explicit material on the World Wide Web.

84. Congress reasonably listed credit cards as an affirmative defense to COPA. Congress noted that credit cards are an affirmative defense in the FCC's dial-a-porn regulations, which has been upheld by the courts. *See* H.R. Rep. 105-775 at 14 (citing *Dial Info. Serv's*

*Corp. v. Thornburgh*, 938 F.2d 1535 (2d Cir. 1991), *cert. denied*, 502 U.S. 1072 (1992), and *Sable*, 492 U.S. 115 (1989)).

85. Congress also took note of the Supreme Court's approval of affirmative defenses (such as credit cards) within laws protecting minors from sexually explicit material when it stated, "the FCC's technological approach to restricting dial-a-porn messages to adults who seek them would be extremely effective, and only a few of the most enterprising and disobedient young people would manage to secure access to such messages." H.R. Rep. 105-775, at 14 (quoting *Sable*, 492 U.S. at 130).

86. Even if using credit cards would place an economic burden on commercial web sites, such a burden does not render COPA unconstitutional, as "there is no constitutional impediment to enacting a law which may impose such costs on a medium electing to provide [indecent] messages." *Sable*, 492 U.S. at 125. *See also Mitchell v. Comm'n on Adult Entertainment Establishments*, 10 F.3d 123, 144 (3d Cir. 1993) (when availability of adult content is not significantly impaired, law's effect on plaintiff's revenue is not material to First Amendment analysis); *Matney v. County of Kenosha*, 86 F.3d 692, 700 (7th Cir. 1996) ("The fact that [the ordinance] may have an incidental financial effect on adult entertainment speakers and not on others is of no consequence."). Any commercial web sites operators that publish adult sexual content but do not yet accept credit or debit cards can utilize one of COPA's other affirmative defenses.

87. Other technologies exist that will facilitate web site operators' ability to ensure that only adults would have access to harmful-to-minors material on their web sites. For example, Mr. Knopper testified about the technology that exists to permit web site operators to

process “micro-payments,” Knopper Testimony, 11/9/06 at 93:7-14, and that technology facilitates a payment card transaction in the restriction of minors’ access to harmful-to-minors material. 47 U.S.C. § 231(c)(1)(A).

88. In addition, there are effective age verification services that are available for a web site operator to use to ensure that only adults have access to his or her web site, or to portions of his or her web site. Dancu Testimony, 11/9/06 at 174:8 – 175:20. These services constitute “reasonable measures that are feasible under available technology” to “restrict[] access by minors to material that is harmful to minors.” 47 U.S.C. § 231(c)(1)(C).

89. COPA’s age verification measures would be effective in excluding most juveniles, and “only a few of the most enterprising and disobedient young people would manage to secure access.” (H.R. Rep. No. 105-775, at 14 (quoting *Sable Communications of Cal. v. FCC*, 492 U.S. 115, 130 (1989))).

#### **7. There Are No Less Restrictive Alternatives to COPA**

90. Plaintiffs have presented various proposed alternatives to COPA, many of which were raised for the first time in their initial proposed findings of fact, and some of which were presented for the first time only at closing argument at trial. Many of Plaintiffs’ proposed alternatives lack any evidentiary support in the record. None of them could be deemed to be both equally effective as, and less restrictive than, COPA.

**a. The Private Use of Filtering Software Is Not a Less Restrictive Alternative**

91. The use of Internet content filtering by parents in households with children is not an effective substitute to the direct regulation of commercial pornography affected by COPA. Filtering software will continue to exist, and will continue to be available for use by families, whether or not Defendant is permitted to enforce COPA.

92. The enforcement of COPA provides a more effective means of protecting children than such filtering alone.

93. The private use of filtering software cannot be deemed a “less restrictive alternative” for the purpose of constitutional analysis. The proper inquiry is whether alternatives available to the *government* “would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.” *Ashcroft v. ACLU*, 542 U.S. 656, 665 (2004) (quoting *Reno v. ACLU*, 521 U.S. 844, 874 (1997)).

94. Nor could any governmental efforts to promote the increased use of filtering software be deemed to be a less restrictive alternative to COPA. *Cf. Ashcroft*, 542 U.S. at 669-70 (identifying governmental efforts to promote use of filtering software as potential alternative to be considered on remand). All of the filtering products that were tested in Mr. Mewett’s and Dr. Stark’s study missed large portions of the adult material on the Web. Moreover, the filters that were marginally more successful at blocking adult material could only do so at the price of also blocking vast amounts of non-sexually explicit material. The AOL filter, for example, blocks as much as 19.6% of the “clean” material on the Web. Stark Testimony, 11/8/06 at 112:8-19; Def.’s Ex. 78. Any minimal “chilling effect” that COPA might have on web site operators pales in comparison to the vast range of non-sexually explicit web sites that would be

blocked by the expanded use of filtering software.

95. Plaintiffs contend that the private use of filtering software could be a less restrictive alternative to COPA, because parents could choose a filter product that blocks less of both adult material and non-sexually explicit material, or they could choose a product that blocks more of both adult material and non-sexually explicit material. But this is no choice at all. The products that perform poorly at blocking leave children exposed to a vast range of adult material, demonstrating the need for the solution that COPA offers. The products that block more adult material still allow a large amount of that material through, and they do so at the cost of blocking vastly larger amounts of “clean” material. The vast majority of the sites that are blocked by these filters are actually blocked in error. Stark Testimony, 11/8/06 at 106:3 – 107:2. It is therefore unsurprising that many parents find these filters to be unusable for this reason, despite the fact that they are greatly concerned about the exposure of their children to inappropriate material on the Web. Pls.’ Ex. 85 at 0005, 0009-10. Those parents need the additional assistance that COPA would provide.

96. Plaintiffs also propose the private use of application-blocking software as an alternative to COPA. This form of software may succeed at blocking access to sexually explicit materials through alternative technologies such as peer-to-peer file-sharing software. *See* Joint Ex. 1 at ¶ 95. However, application-blocking software cannot be used to block sexually explicit material on the Web without also blocking all non-sexually explicit material.

**b. Plaintiffs' Further Proposals Regarding the Use of Filters Are Not Less Restrictive Alternatives**

97. Plaintiffs have proposed a requirement that website operators tag, or label, their websites as containing "harmful-to-minors" material, presumably to make it more likely that a filter would block access that website. This cannot be a lesser restrictive alternative. Due to the large volume of material on the Web, any statute requiring the labeling of entire web sites in this manner would impose an "enormous expense" on web site operators, in the judgment of the National Research Council. Pls.' Ex. 54 at 0324.

98. Because the tagging system that plaintiffs propose would apply to an entire web site, a web site operator would not have the option of separating out harmful-to-minors material from other material, as COPA, in contrast, permits. A web site that is tagged in this manner, if keyed to filtering software that aims to block these labeled web sites, would be blocked in its entirety. Thus, by definition, this alternative is more restrictive than COPA would be. Web sites would be more significantly hindered in their operations if access were to be cut off to the entire site, including its front page, rather than particular portions of harmful-to-minors material. Smith Testimony, 11/15/06 at 179:11 – 180:6.

99. Plaintiffs' proposal assumes that filtering programs are universally used, and would be effective at screening tagged material while avoiding the blocking of other material. For this reason, Plaintiff ACLU successfully opposed a similar tagging scheme in the Communications Decency Act. *Reno v. ACLU*, 521 U.S. 844, 881 (1997); see Mewett Testimony, 11/08/06 at 149:8-24. In addition, two plaintiffs in this case – the Sexual Health Network, and the ACLU (through its Utah affiliate) – are currently also plaintiffs in pending

litigation challenging a state statute's web site labeling requirement. Def.'s Ex. 447 at 0003, 0026. Plaintiffs may not contradict their position here.

100. Plaintiffs also propose a requirement that filtering products create a separate "harmful to minors" category. This proposal would not be effective, because it assumes that filters are widely used, that they prevent minors from accessing harmful content, and that they avoid the blocking of "clean" content. Each of these assumptions is false. There is no reason to expect that the filtering software companies do not understand what kind of web sites they mean to block; instead, as explained above, the failures of the filtering programs are caused by the defects that are inherent in the use of blacklists and dynamic filtering techniques. Mewett Testimony, 11/7/06 at 103:8-14, 105:16-22. In any event, this alternative could be effective only if companies were *required* to block access to certain sites.

101. Plaintiffs next propose that the government compile a "black list" of harmful-to-minors sites, or that it fund a private entity's efforts to do so. This proposal, while raising many of the same (or more) constitutional objections presented by plaintiffs to COPA, would be ineffective for the same reasons that any black lists are ineffective when used with filtering software. Web sites are too numerous and change too frequently for the filtering software companies, the government, or any private business, to effectively separate harmful from non-harmful material. Mewett Testimony, 11/7/06 at 151:16 – 152:2; Pls.' Ex. 6 at 0024. Only a solution directed at the source of the problem can provide the incentive necessary to adequately protect children.

102. Plaintiffs further propose that the government be required to test filtering products, and publicly report the results of that study. This, too, could not be a less restrictive

alternative to COPA. There are already numerous studies that show the inadequacies of filtering products, and yet the defects in the filtering software market persist. Eisenach Testimony, 11/13/06 at 129:15 – 131:14, 138:12 – 139:21, 180:20 – 183:4. The addition of a further government study would not improve the overall information that is available to consumers, nor would it solve the imperfections in the filtering market. Eisenach Testimony, 11/13/06 at 193:11-16. In any event, such a study could only possibly be effective if there were some sufficiently effective products to which consumers could be alerted. However, Mr. Mewett's and Dr. Stark's study reveals that none of the filtering products are capable of blocking adult material while at the same time minimizing the blocking of "clean" material.

103. One further alternative that Plaintiffs have not proposed warrants brief discussion. Some entities have proposed the creation of a separate top-level domain (such as the .com or .edu domains) for adult material, or for material designated as child-friendly. The creation of an adult (.xxx) top-level domain would not be effective at prevent minors from being exposed to sexually explicit material on the World Wide Web. Russo Testimony, 10/25/06 at 218:24 – 221:17; Joint Ex. 1 at ¶ 98.

104. Similarly, a separate child-friendly top-level domain will not prevent the conveyance of harmful material to children. There is no need to speculate on this point, because Congress authorized such a domain in 2002, *see* 47 U.S.C. § 941, and NeuStar administers a top-level ".kids" domain. (<http://www.neustar.biz/addressing/kidsDom.cfm> and <http://www.kids.us/>). The domain "www.kids.us" contained a trivial number of web sites, thus guaranteeing that children will be unable to complete even basic homework tasks without accessing the traditional domains on the Web. Mewett Testimony, 11/7/06 at 152:3-7.

**c. Prosecutions Under the Obscenity Laws, or Under Other Existing Laws, Are Not a Less Restrictive Alternative**

105. An increase in obscenity prosecutions will not prevent minors from being exposed to sexually explicit material on the World Wide Web, because the scope of “harmful to minors” material is broader than the “obscene” material. Unlike criminal obscenity laws, however, COPA does not ban any material. It merely requires that consumers of harmful-to-minors material provide verification of their identity. Because the obscenity laws ban speech, while COPA only imposes regulatory requirements, by definition, obscenity prosecutions cannot be a less restrictive alternative than COPA.

106. Material is obscene, under the standard set forth in *Miller v. California*, 413 U.S. 15 (1973), if (a) an average person applying contemporary community standards finds that the material taken as a whole appeals to the prurient interest; (b) an average person applying contemporary community standards finds that the material depicts sexual conduct in a patently offensive manner; and (c) a reasonable person, viewing the material as a whole, finds that the material lacks serious literary, artistic, political or scientific value. *See id.* at 24.

107. Examples of web sites that have been prosecuted as obscene include, *inter alia*, child pornography, depictions of bondage and sadistic or masochistic behavior involving children, sexual contact between an adult woman and a dog, violent gang rapes of women, sexual intercourse between humans and animals, and sexual activity involving urination, defecation, or genital mutilation. Def.’s Ex. 283, No. 18.

108. Obscenity law bans a very narrow category of speech that is entitled to no First Amendment protection, while COPA has broader application, creating a category of regulated material that is obscene for minors, not adults. *Ashcroft v. ACLU*, 542 U.S. 656, 675 (Stevens,

J., concurring).

109. The “harmful to minors” standard used in COPA differs from the *Miller* test in two respects. First, it requires that each prong of the *Miller* test be analyzed with respect to older minors. In addition, the second prong of the harmful-to-minors standard provides a more detailed description of material that a judge or jury may find to be “patently offensive” than the *Miller* obscenity test. 47 U.S.C. § 231(e)(6)(B).

110. The *Miller* test provides a standard that is judged by reference to the reasonable adult, whereas COPA provides a standard with respect to older minors. *See Am. Booksellers v. Webb*, 919 F.2d 1493, 1506 (11th Cir. 1990). Because COPA regulates harmful material beyond that which adults find obscene, its effects cannot be replicated by other criminal statutes. *See ACLU*, 521 U.S. at 875 (noting a “governmental interest in protecting children from harmful materials” that do not meet the court’s definition of obscenity for adults).

111. Obscenity laws provide no protection for minors from harmful-to-minors material that is not obscene.

112. Even the most graphic photographs submitted on April 17, 2006 by Plaintiffs from Penthouse.com—depictions of full female nudity—are unlikely to be deemed to rise to the level of obscenity. Although this material may satisfy COPA’s definition of “patently offensive” with respect to minors (e.g., there is a graphic and lewd focus on the genitals), it is unlikely to be deemed patently offensive under the *Miller* test with respect to adults. Def.’s Ex. 283, No. 16. Enforcement of COPA is necessary in order to prevent minors from accessing material like the pages from Penthouse.com.

113. COPA defines a minor as “any person under 17 years of age.” *Id.* at § 231(e)(7).

Plaintiffs cite interrogatory responses regarding the application of COPA to 17 year-olds, despite the fact that 17 year-olds plainly are not covered by COPA. Counsel for Plaintiffs also incorrectly argues that the *obscenity* standard is applied with reference to 17 year-olds, despite Defendant's repeated clarifications that a determination of whether material is obscene is not made in reference to 17 year-olds and that neither the constitutional nor the statutory standard for obscenity requires reference to 17 year-olds. Closing Argument, 11/20/06 at 21:17 – 22:7; *see, e.g.*, Def.'s Ex. 284 at 5 & n.3. Plaintiffs' attempt to conflate the standard for obscenity with the harmful-to-minors standard by misstating the legal significance of COPA's (or the obscenity laws') application to 17 year-olds should be rejected.

114. In addition to the obscenity laws, plaintiffs also propose that prosecutions be pursued under the Misleading Domain Names statute, 18 U.S.C. § 2252B. That statute is not as effective as COPA because it applies only to web sites that entice visitors to a web site by deceptive means. 18 U.S.C. § 2252B. The statute does not address web sites that are, by name or reputation, indisputably pornographic. Further, it applies only to instances in which a domain name is typed directly into a browser, and thus does not protect minors from exposure to harmful-to-minors web sites that are accessed by other means. Further, the statute does not require that harmful-to-minors material be made accessible only after a web site visitor proves his or her age.

115. Relatively few adult web sites rely on the use of domain names – misleading or otherwise – to attract traffic. Mewett Testimony, 11/7/06 at 143:22 – 144:5. This is due, at least in part, to the growth of search engines as a tool to direct viewers to particular web sites. Pls.'

Ex. 13 at 0027-28. Thus, further prosecutions under Section 2252B would do nothing to deter those adult web sites that do not use misleading domain names.

116. Congress recently enacted another statute prohibiting the use of misleading metatags on website. 18 U.S.C. § 2252C. A large majority of adult web sites, however, do not rely on descriptive metadata – misleading or otherwise – to attract traffic to their sites. Mewett Testimony, 11/7/06 at 147:8 – 148:1. Thus, prosecutions under this statute would not fully address the problem of the exposure of minors to adult material on the Web.

**d. Plaintiffs' Suggestions for Narrowing the Application of COPA Would Undermine Its Effectiveness**

117. Plaintiffs propose that COPA be revised to apply only to images, or to impose civil penalties only. *See* Pls.' Disputed Facts at 65-68 (Doc. No. 319). These proposals would undermine the effectiveness of COPA. COPA applies a constitutionally-approved standard for variable obscenity. It is well-established that the government has a compelling interest in protecting minors from all harmful-to-minors material, and that category is not limited to images alone.

118. Moreover, because of the profitability of the commercial pornography industry, civil penalties alone will not suffice. The adult online industry generated approximately \$1 billion in revenues annually as of 2002, and that figure is anticipated to grow to between \$5 billion and \$7 billion by 2007. Pls.' Ex. 54 at 0101. Congress thus reasonably concluded that the threat of criminal prosecutions, in addition to the threat of civil penalties, would be necessary to deter online commercial pornographers.

**e. Educational Efforts Will Not Be as Effective as COPA in Protecting Children from the Exposure to Harmful Material**

119. Plaintiffs also propose that the government fund public education campaigns about techniques that parents can use to promote Internet safety. Compl. at 11 ¶ 9. This cannot be deemed a less restrictive alternative for at least two reasons. First, the government already does so, as required both in COPA itself, *see* 47 U.S.C. § 230(d), and in another recent statute. *See* Pub. L. No. 109-248, 120 Stat. 587 (July 27, 2006).

120. Second, this theory assumes that parents, when properly educated by the government, invariably can protect their children from the harmful material found on the World Wide Web. This argument fails because parents are unable to prevent accidental viewings of such materials, and the widespread availability of the Web subverts parental supervision and control. As the National Research Council cautions, while the promotion of parental supervision and education may be useful, “the expectations for such education and socialization should not be unrealistic.” Pls.’ Ex. 54 at 0398.

121. The NRC also notes that the use of techniques such as monitoring children’s internet usage, and education of children as to proper internet usage, may have limited effects because children may become inured to parental warnings. Further these techniques will do little or nothing to prevent minors from inadvertent access to sexually explicit material. Pls.’ Ex. 54 at 0336.

122. Techniques such as acceptable use policies, of or family contracts, are also of limited usefulness, as it is unlikely that most children will actually remember and adhere to those policies over the long term. Pls.’ Ex. 54 at 0263. As school librarian Tava Smathers put it when asked whether her school’s acceptable use policy is effective, “I can’t really say yes or no to that.

. . . It's good to have, I think you have to have it, but I think that's all the power it has."

Smathers Testimony, 11/2/06 at 16:10-24.

123. Any proposal to rely on parental supervision as an alternative to COPA assumes that parents actually are able consistently to be aware of, and monitor, their children's Internet activities. To the contrary, "[t]here is often a large gap in what parents perceive their children are doing on the Internet and what these children report they are actually doing." Pls.' Ex. 54 at 0193. For example, while 67% of parents report that an adult is always in the same room when their child is online, in fact 78% of children report that they sometimes use the Internet alone. Pls.' Ex. 54 at 0194.

124. With the many demands of modern life, it is not reasonable for the government to expect all parents to shoulder the burden to cut off every possible source of adult content for their children, rather than the government's addressing the problem at its source—the commercial pornographers. Many families simply lack the resources to pursue the obligations that plaintiffs aim to impose upon them. The NRC notes, "Parents in many families today face long workdays, long commutes, and considerable work-related overnight travel. Single-parent households are common, as are families in which both parents work full time. These facts suggest that continual in-person supervision of a child's Internet usage by a parent is not likely to be achieved by many families." Pls.' Ex. 54 at 0254.

125. As Terri Kirk put it, in describing her school district with a number of lower-income families: "That translates that we don't have a lot of parent involvement from those parents. That just sort of goes hand-in-hand." Kirk Testimony, 11/1/06 at 73:4-14. There are many different kinds of families in the United States, not all of whom have the time and

resources that would be required for them to constantly monitor their children's Internet activities.

126. Voluntary efforts by parents to monitor their children's Internet usage, or to educate their children about sexually explicit material on the World Wide Web, thus will not prevent minors from being exposed to such material.

127. Plaintiffs' proposal, at bottom, is to place the burden of protecting children not on commercial pornographers – who create, and profit from, the problem in the first place – but instead on parents, through the use of filtering software or through educational efforts such as those discussed above. These types of burdens on parents cannot be as effective as COPA's requirements, and they are inconsistent with Congress's judgment that any burdens associated with restricting minors' access to harmful to minors materials pursuant to COPA should be placed on the source of such materials, not on parents. Plaintiffs cannot demonstrate, therefore, that the less restrictive alternatives they propose are equally able to accomplish the Act's goals. *See Dial Information Servs. v. Thornburgh*, 938 F.2d 1535, 1542 (2d Cir. 1991).

**IV. JUDGMENT SHOULD BE GRANTED TO DEFENDANT ON COUNT TWO OF THE AMENDED COMPLAINT (ALLEGED VIOLATION OF OLDER MINORS' RIGHTS)**

128. Plaintiffs' second cause of action fails because there is no constitutional right for older minors to access harmful-to-minors material. *See Bellotti v. Baird*, 443 U.S. 622, 634 (1979) (“the constitutional rights of children cannot be equated with those of adults”); *Ginsberg*, 390 U.S. 629, 638 (“[E]ven when there is an invasion of protected freedoms the power of the state to control the conduct of children reaches beyond the scope of its authority over adults”) (internal quotations omitted); *Sable Comm'n of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989)

(finding that government has “a compelling interest in protecting the physical and psychological well-being of minors” and that “[t]his interest extends to shielding minors from the influence of literature that is not obscene by adult standards”). Under the *Ginsberg* concept of “variable obscenity,” material deemed harmful to minors is unprotected as to minors. *Ginsberg v. New York*, 390 U.S. 629, 638 (1968); *see also M.S. News Co. v. Casado*, 721 F.2d 1281, 1289 (10th Cir. 1983).

129. In addition, Plaintiffs’ second cause of action must fail because COPA does not restrict older minors’ access to material appropriate for older minors. *See, e.g., Am. Booksellers v. Webb*, 919 F.2d 1493, 1504-05 (11th Cir. 1990) (in construing a statute defining minors as under 18 years old, concluding that “if any reasonable minor, including a seventeen-year-old, would find serious value, the material is not ‘harmful to minors’”); *Am. Booksellers Ass’n v. Virginia*, 882 F.2d 125, 127 (4th Cir. 1989) (“if a work is found to have a serious literary, artistic, political, or scientific value for a legitimate minority of normal, older adolescents, then it cannot be said to lack such value for the entire class of juveniles taken as a whole”) (quoting *Virginia v. Am. Booksellers Ass’n*, 372 S.E.2d 618, 624 (Va. 1988)); *Davis-Kidd Booksellers, Inc. v. McWherter*, 866 S.W.2d 520, 533 (Tenn. 1993) (finding material has serious value for minors within the meaning of that State’s display law, if it has serious value for “a reasonable seventeen year old minor”).

130. In addition, Plaintiffs’ second cause of action must fail due to lack of evidence. Even if Plaintiffs were able to state a legal claim for Count II, Plaintiffs did not proffer any

evidence from older minors regarding any alleged injury, which is an essential prerequisite of stating a claim.

V. **JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON COUNT THREE OF THE AMENDED COMPLAINT (VIOLATION OF THE RIGHT TO COMMUNICATE AND ACCESS INFORMATION ANONYMOUSLY)**

131. There is no constitutional right to access material anonymously on the Web. While the Supreme Court has recognized a right to anonymous speech in certain circumstances, this line of cases is inapposite to the instant case. *See Buckley v. Am. Constitutional Law Found.*, 525 U.S. 182 (1999) (striking down statute requiring volunteers to wear identification badges); *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334 (1995) (allowing anonymous pamphleteering on political issues); *Talley v. Calif.*, 362 U.S. 60 (1960) (finding First Amendment to protect distribution of unsigned handbills urging the boycott of merchants); *Lamont v. Postmaster Gen.*, 381 U.S. 301, 305 (1965) (striking down law requiring recipients of “communist political propaganda” through mail to perform an “official act,” that is, to affirmatively request that post office deliver material). The rationale for these cases is that a speaker’s rights should be protected because public disclosure of unpopular viewpoints could stifle speech. *See, e.g., McIntyre*, 514 U.S. at 357 (“Anonymity is a shield from the tyranny of the majority”); *Lamont*, 381 U.S. at 307 (requirement of affirmative request to government, for material condemned by federal government, has deterrent effect and could raise concerns about retaining employment).

132. The Supreme Court cases regarding anonymous speech – and their rationale of protecting anonymous speech due to the potential chill in disclosing one’s identity – do not apply to the situation presented by COPA. COPA does not entail public disclosure of anyone’s identity, nor does it require identification to any government officials. To the contrary, absent

consent of that adult or a court order, COPA prohibits the disclosure of “any information collected for the purposes of restricting access to such communications to individuals 17 years of age or older.” 47 U.S.C. § 231(d)(1)(A). Further, the statute requires that a company that verifies the age of an adult who accesses harmful to minors material to “take such actions as are necessary to prevent unauthorized access to such information by a person other than the [company] and the [adult].” *Id.* at § 231(d)(1)(B). Anyone who willfully or knowingly violates these provisions is subject to criminal penalties. *See* 47 U.S.C. § 501.

133. Under COPA, an individual’s identity is disclosed only by providing a credit card or other adult verification in order to access harmful-to-minors material, and this information is disclosed only to the web site offering such material. This non-public disclosure does not implicate the type of policy concerns underlying the Supreme Court’s protection of anonymous speech. *Cf. Veterans & Reservists for Peace in Vietnam v. Reg. Comm’r of Customs*, 459 F.2d 676, 683 (3d Cir. 1972) (upholding statute that required a license to receive certain material from North Vietnam when there were no allegations “that the purpose of the recordation is to embarrass the recipient of materials or to chill the exercise of this right to receive them”).

134. COPA’s inclusion of a non-disclosure provision renders Plaintiffs’ contention that their speech or access to speech will be restricted because of loss of anonymity a constitutionally insignificant contention. *See Connection Distrib. Co. v. Reno*, 154 F.3d 281, 294 (6th Cir. 1998); *Fabulous Assoc., Inc. v. Penn. Public Utility Comm’n*, 896 F.2d 780, 788 (3d Cir. 1990).

135. Courts have upheld laws intended to restrict access by minors to sexually explicit material, even if such laws may require adults who desire such material to affirmatively request it or to identify themselves in some manner. *See Crawford v. Lungren*, 96 F.3d 380, 387-89 (9th

Cir. 1996) (upholding constitutionality of law regulating sale of “harmful to minors” material in vending machines which allowed access by adults who could verify their adulthood); *Information Providers’ Coalition for Defense of First Amendment v. FCC*, 928 F.2d 866, 872-74 (9th Cir. 1991) (upholding credit card or adult access code requirement in the “dial-a-porn” context); *Doe v. City of Minneapolis*, 693 F. Supp. 774, 783 (D. Minn. 1988) (finding no First Amendment right to anonymously view sexually explicit material in bookstore booths), *aff’d*, 898 F.2d 612 (8th Cir. 1990); *Upper Midwest Booksellers Ass’n v. Minneapolis*, 780 F.2d 1389, 1395 (8th Cir. 1986) (upholding constitutionality of display restriction in part because “[a]dults are still free to request a copy of restricted material to view from a merchant”).

136. Plaintiffs’ third cause of action must fail because Plaintiffs do not have a right to communicate or access harmful-to-minors content anonymously. *Cf. Connection Distributing Co. v. Reno*, 154 F.3d 281 (6th Cir. 1998) (rejecting anonymity claims raised by “swingers” magazine); *Fabulous Assoc., Inc. v. Pennsylvania Public Utility Comm’n*, 896 F.2d 780, 788 (3d Cir. 1990) (suggested dial-a-porn regulation that required customers to identify themselves to telephone companies in order to unblock access to services is constitutionally permissible where “there is evidence that the telephone company will not disclose such information”); *Crawford v. Lungren*, 96 F.3d 380, 387-89 (9th Cir. 1996) (upholding constitutionality of law regulating sale of “harmful to minors” material in vending machines which allowed access by adults who could verify their adulthood); *Information Providers’ Coalition for Defense of First Amendment v. FCC*, 928 F.2d 866, 872-74 (9th Cir. 1991) (upholding credit card or adult access code requirement in the “dial-a-porn” context); *Doe v. City of Minneapolis*, 693 F. Supp. 774, 783 (D. Minn. 1988) (finding no First Amendment right to anonymously view sexually explicit material

in bookstore booths), *aff'd*, 898 F.2d 612 (8th Cir. 1990); *Upper Midwest Booksellers Ass'n v. Minneapolis*, 780 F.2d 1389, 1395 (8th Cir. 1986) (upholding constitutionality of display restriction in part because “[a]dults are still free to request a copy of restricted material to view from a merchant”).

137. In addition, Plaintiffs’ third cause of action must fail due to lack of evidence. Even if Plaintiffs were able to state a legal claim for Count III, Plaintiffs did not proffer any evidence from web users seeking to access material anonymously regarding any alleged injury, which is an essential prerequisite of stating a claim.

**VI. JUDGMENT SHOULD BE ENTERED FOR DEFENDANT ON PLAINTIFFS’ FIRST AMENDMENT VAGUENESS CLAIM**

138. To survive a vagueness challenge, criminal statutes “need only give ‘fair warning’ that certain conduct is prohibited.” *San Filippo v. Bongiovanni*, 961 F.2d 1125, 1136 (3d Cir. 1992). A vagueness challenge is particularly difficult to sustain because COPA does not apply to entities that unknowingly make harmful to minors material available to minors by means of the World Wide Web. *See* 47 U.S.C. § 231(a)(1), (e)(2)(B).

139. Case law has narrowed and sharply defined material that can be regulated in order to protect children. *See, e.g., Am. Booksellers Ass’n*, 372 S.E.2d at 622 & 625 (finding that sixteen books, including Judy Blume’s *Forever*, *Hollywood Wives*, *Changing Bodies*, *Changing Lives* and *Our Bodies Ourselves*, had serious literary, artistic, political or scientific value for minors); *Athenaco, Ltd. v. Cox*, 335 F. Supp. 2d 773, 781 (E.D. Mich. 2004) (finding works including *Lolita*, *Sanctuary*, *Of Mice and Men*, *The Catcher in the Rye*, *Portnoy’s Complaint*, and *Joy of Sex* not to be harmful to minors); *Baker v. Glover*, 776 F. Supp. 1511, 1516 (N.D. Ala. 1990) (finding bumper sticker with phrase “Eat Shit” not to be harmful to minors).

140. The language of COPA gives fair warning about the regulated conduct covered by the statute. 47 U.S.C. § 231(e)(6). Mere nudity is not enough to render material harmful to minors. *See Osborne v. Ohio*, 495 U.S. 103, 112 (1990) (“depictions of nudity, without more, constitute protected expression”); *Erznoznik v. City of Jacksonville*, 422 U.S. 205, 213 n.10 (1975) (“It is clear . . . that under any test of obscenity as to minors not all nudity would be proscribed. Rather, to be obscene ‘such expression must be, in some significant way, erotic.’”) (quoting *Cohen v. California*, 403 U.S. 15, 20 (1971)). In *Osborne*, the Supreme Court upheld a state obscenity regulation where the term nudity was construed to require “a graphic focus on the genitals.” *Osborne*, 495 U.S. at 113. COPA incorporates this standard within the second prong and also defines the specific types of actions that must be present in a patently offensive manner. *See* H.R. Rep. 105-775 at 13, 28 (noting that COPA “modifies the ‘patently offensive’ language by explicitly describing material that is harmful to minors” and that “harmful to minors” test does not extend to “materials that merely contain nudity”).

141. The knowledge requirement of COPA renders the statute less vague. COPA does not apply to entities that unknowingly make harmful to minors material available to minors by means of the World Wide Web. *See* 47 U.S.C. § 231(a)(1), (e)(2)(B).

142. The “engaged in the business” requirement of COPA renders the statute less vague. Only entities that are engaged in the business of distributing harmful-to-minors material will be liable under COPA. *See* 47 U.S.C. 231(a)(1).

143. In discovery, Plaintiffs requested that Defendant opine on whether certain web pages from Playboy.com and Penthouse.com would be harmful to minors. Web pages from Penthouse.com that Defendant found likely to be deemed harmful to minors contain numerous

lewd depictions of full-frontal nudity in its free content area, including a photograph of a woman exposing her labia and clitoris and a photograph of a woman turned to her side, spreading her buttocks, and revealing her vagina and anus. This opinion was based on the conclusion that this material is designed to appeal to, or designed to pander to, the prurient interest and will likely be found to be patently offensive with respect to minors, and that a court or jury likely would find that they do not have serious literary, artistic, political, or scientific value for minors. Def.'s Ex. 283, No. 15.

144. Consistent with established law, Defendant has stated that many web pages with little, if any, nudity (such as certain images provided to Defendant from the Playboy.com web site) are not likely to be deemed harmful to minors. Although one web page identified by Plaintiffs on April 17, 2006 from Playboy.com contains one photograph depicting female breasts, the majority of the pictures do not contain any nudity, and there is no depiction of sexual activity or full frontal nudity. Counsel for Plaintiffs incorrectly argues that, "I guess – although they are not very clear in their answer, I guess they mean that that – I guess they mean that Playboy has value for minors. It has either artistic value for minors or literary value for minors." Closing Argument, 11/20/06 at 15:23 – 16:2. Reference to Defendant's discovery response would have made clear that Defendant's determination was reached because, *inter alia*, the specific photographs from the Playboy.com web site do not explicitly depict sexual acts or graphically focus on the genitals, thus failing to satisfy the second prong of the harmful-to-minors test. The third prong, accordingly, was not addressed. Def.'s Trial Ex. 283, No. 15.

145. The requirement to evaluate material "as a whole" makes COPA less vague. In determining whether a given work has value, the proper inquiry is "whether a reasonable person

would find such value in the material, taken as a whole.” *Pope v. Illinois*, 481 U.S. 497, 501 (1987). It is important to note that the value of a work does not “vary from community to community based on the degree of local acceptance it has won.” *Id.* at 500. Because this prong is not judged by community standards, but, instead, sets a “national floor” of societal value, *see Reno*, 521 U.S. at 873, Plaintiffs’ speculative fears that the harmful-to-minors test will be applied in vastly different ways by different communities is unavailing.

146. The *Miller* and *Ginsberg* standards repeatedly have been upheld over vagueness challenges. *See, e.g., Fort Wayne Books, Inc. v. Indiana*, 489 U.S. 46, 57 (1989).

147. Judgment should be entered for Defendant.

Respectfully submitted,

PETER D. KEISLER  
Assistant Attorney General

PATRICK L. MEEHAN  
United States Attorney  
RICHARD BERNSTEIN  
Assistant U.S. Attorney  
THEODORE C. HIRT  
Assistant Branch Director  
RAPHAEL GOMEZ  
Senior Trial Attorney

/s/ Eric J. Beane

ERIC J. BEANE  
ISAAC CAMPBELL  
JOEL McELVAIN  
KENNETH SEALLS  
JAMES TODD  
TAMARA ULRICH  
Trial Attorneys  
U.S. Department of Justice  
Civil Division, Federal Programs Branch  
20 Massachusetts Ave., N.W.  
Washington, DC 20530

(202) 616-2035

Attorneys for Defendant

CERTIFICATE OF SERVICE

I hereby certify that on December 8, 2006, I caused the foregoing Findings of Fact and Conclusions of Law to be filed electronically and therefore to be available for viewing and downloading from the Electronic Case Filing system. The electronic filing of this document constituted service of this document on the following liaison counsel:

Aden Fine  
American Civil Liberties Union  
125 Broad Street, 18<sup>th</sup> Floor  
New York, NY 10004

/s/ Eric J. Beane  
ERIC J. BEANE