#### CORPORATE DISCLOSURE STATEMENT

Amicus curiae Computer & Communications Industry Association, through the undersigned counsel, hereby states that it does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

Amicus curiae Consumer Electronics Association, through the undersigned counsel, hereby states that it does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

Amicus curiae Information Technology Industry Council, through the undersigned counsel, hereby states that it does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

Amicus curiae TechAmerica, through the undersigned counsel, hereby states that it does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

Amicus curiae Center for Democracy & Technology, through its undersigned counsel, hereby states that it does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

Amicus curiae Digital Liberty Project is a special project of Americans for Tax Reform and hereby states, through the undersigned counsel, that Americans for Tax Reform does not have a parent corporation and that no publicly held company owns 10% or more of its stock.

#### TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENTi
TABLE OF AUTHORITIESiv
INTEREST OF AMICI CURIAE1
INTRODUCTION AND SUMMARY OF ARGUMENT4
ARGUMENT 6
I. THIS CASE COULD HAVE A SIGNIFICANT IMPACT IN THE ONLINE ENVIRONMENT, AND THE COURT'S ONLINE "USER EMPOWERMENT" JURISPRUDENCE SHOULD GUIDE ITS DECISION HERE 6
A. The Court's Decision in This Case Could Have a Direct Impact on Online Gaming 6
B. In the Online World, Promotion of User Empowerment Tools Represents the Least Restrictive Means of Protecting Minors from Unwanted Content9
C. User Empowerment Tools Can Be Very Effective in Protecting Minors, Even from Violent Content
D. User Empowerment Tools Are Also the Solution to Regulating Children's Access to Violent Content in <i>Offline</i> Video Games 14
II. AN AGE-BASED VIOLENT CONTENT RESTRICTION WOULD BE HIGHLY PROBLEMATIC IN THE ONLINE WORLD BECAUSE OF THE INABILITY TO RELIABLY DETERMINE OR VERIFY THE AGES OF ONLINE USERS

A. "Age Verification" Technologies Do Not	
Establish the Ages of Internet Users with	
the Level of Accuracy Needed to Avoid an	
Unconstitutional Chill on Speech1	7
B. A Government Mandate on Websites to	
Implement Age Verification Technologies	
Would Infringe on Adults' First	
Amendment Rights 2	1
C. Any Requirement that Online Video Game	
Providers Implement Age Verification	
Would Be an Unconstitutional Burden on	
Their Speech24	4
CONCLUSION	6

#### TABLE OF AUTHORITIES

Cases
ACLU v. Ashcroft, 322 F.3d 240 (3d Cir. 2003)21, 23
ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007)passim
ACLU v. Mukasey, 534 F.3d 181 (3d Cir. 2009)11, 17, 21, 23
ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996)
American Amusement Machine Ass'n v. Kendrick, 244 F.3d 572 (7th Cir. 2001)7
Ashcroft v. ACLU, 542 U.S. 656 (2004) passim
Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727 (1996)21
Entertainment Merchants Ass'n v. Henry, No. CIV-06-675-C, 2007 WL 2743097 (W.D. Okla. Sept. 17 2007)7
Entertainment Software Ass'n v. Blagojevich, 404 F. Supp. 2d 1051 (N.D. Ill. 2005)7
Entertainment Software Ass'n v. Blagojevich, 469 F.3d 641 (7th Cir. 2006)
Entertainment Software Ass'n v. Foti, 451 F. Supp. 2d 823 (2006)7
Entertainment Software Ass'n v. Granholm, 426 F. Supp. 2d 646 (E.D. Mich. 2006)

McIntyre v. Ohio Elections Comm'n,
514 U.S. 334 (1995)21
Mukasey v. ACLU, 129 S. Ct. 1032 (2009)11, 17
Reno v. ACLU, 521 U.S. 844 (1997)
Simon & Schuster, Inc. v. Members of the New York State Crime Victims Board, 502 U.S. 105 (1991)24
United States v. Playboy Entertainment Group, Inc., 529 U.S. 803 (2000)
Video Software Dealers Ass'n v. Maleng, 325 F. Supp. 2d 1180 (W.D. Wash. 2004)7
Video Software Dealers Ass'n v. Webster, 773 F. Supp. 1275 (W.D. Mo. 1992)7
Video Software Dealers Ass'n v. Webster, 968 F.2d 684 (8th Cir. 1992)7
Statutes
47 U.S.C. § 231(c)(1)18
Cal. Civ. Code § 1746
Okla. Stat. title 21, § 1040.756
Wash. Code, Title 9, Chapter 91, § 1807
Other Authorities
Adam Thierer, Parental Controls & Online Child Protection: A Survey of Tools & Methods, 94 (2009)14
Alexander Sliwinski, NPD: PC retail and digital distribution sales reaching parity, JOYSTIQBETA, Jul. 21, 20106

Android Market, http://www.android.com/market/ (last visited Sept. 16, 2010)6
Apple - Web apps – Games, http://www.apple.com/webapps/games/ (last visited Sept. 16, 2010)
ENTERTAINMENT SOFTWARE RATING BOARD,  Setting Parental Controls (2008),  http://www.esrb.org/about/news/downloads/  ESRB_PTA_Brochure-web_version.pdf
GETNETWISE, Tools filtering violent content, http://kids.getnetwise.org/ tools/blockviolence12
INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES (Dec. 31, 2008)17, 20
Ken Sweet, <i>The Video-Game Industry's Big Digital Shift</i> , FOXBUSINESS, June 11, 20106
MICROSOFT, Introduction to Family Settings, http://www.xbox.com/en- US/support/familysettings/xbox360/ familysettings-intro.htm
Mike Musgrove, A Computer Game's Quiet Little Extra: Parental Control Software, WASH. POST, Dec. 23, 2006
NINTENDO, Parental Controls, http://www.nintendo.com/consumer/systems/ wii/en_na/settingsParentalControls.jsp13
SONY, <i>Using the Parental Control Settings</i> , http://manuals.playstation.net/document/en/ ps3/3_15/ basicoperations/parentallock.html13

#### INTEREST OF AMICI CURIAE<sup>1</sup>

Amicus curiae Computer & Communications Industry Association (CCIA) is a trade association dedicated to open markets, open systems and open networks. CCIA members participate in many sectors of the computer, information, and communications technology industries, and range in size from small entrepreneurial firms to the largest in the industry. CCIA's members collectively employ nearly one million people and generate annual revenues exceeding \$200 billion.

Amicus curiae Consumer Electronics Association (CEA) is the preeminent trade association promoting growth in the \$165 billion U.S. consumer electronics industry. Among our more than 2,000 corporate members are manufacturers, distributors, and retailers of video game hardware and software.

Amicus curiae the Information Technology Industry Council (ITI) is a leading voice, advocate, and thought leader for the information and communications technology (ICT) industry. Its membership includes companies which are active participants in offering hardware and software products to enable robust Internet communications. ITI and its members are leaders in both

<sup>&</sup>lt;sup>1</sup> Pursuant to Rule 37.6, counsel for *amici curiae* authored this brief in whole. No counsel for a party authored this brief in whole or in part, and no counsel or party made a monetary contribution intended to fund the preparation or submission of this brief. No person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission. The parties have consented to the filing of this brief, and letters reflecting the consent of the parties have been filed with the Clerk.

technological innovation and public policy advocacy, urging adoption of policies which maximize private sector growth and responsibility. ITI members' combined global sales exceed 1 trillion dollars.

Representing approximately 1,200 member companies of all sizes from the public and commercial sectors of the economy, amicus curiae TechAmerica is the technology industry's largest organization. Its members advocacv manufacturers and suppliers of broadband networks and equipment, consumer electronics companies, software and application providers, Internet and ecommerce companies, and Internet service providers, among others, many of which are directly involved in the video game industry.

Amicus curiae Center for Democracy Technology (CDT) is a non-profit public-interest Internet policy organization. CDT represents the public's interest in an open, decentralized Internet reflecting constitutional and democratic values of free expression, privacy, and individual liberty. CDT's has conducted extensive policy research, published academic papers, and testified before Congress on the impact of content regulations on freedom of expression and the availability of alternative methods, including user empowerment technology tools, for protecting individuals who use the Internet.

Amicus curiae the Digital Liberty Project (DLP) is a special project of Americans for Tax Reform that promotes free-market technology and telecommunications policy. In support of this goal, DLP advocates for limited regulation of the Internet,

including issues impacting freedom of speech. Americans for Tax Reform is a 501(c)(4) non-profit organization dedicated to reducing the size and scope of government and its influence on the economy and Americans' day-to-day lives.

#### INTRODUCTION AND SUMMARY OF ARGUMENT

Amici urge the Court to affirm the Ninth Circuit's decision holding that the California statute at bar violates the First Amendment. Collectively, amici represent some of the leading participants in the Internet and online industry, including service providers and equipment manufacturers, and leading public interest organizations concerned with the First Amendment and online civil liberties. While the California statute does not, on its face, seek directly to regulate online video gaming activity, the Court's decision in this case will have a direct impact on online gaming and other constitutionally protected content accessed via the Internet. In light of this impact, amici present the Court with two considerations:

Promotion of user empowerment continues to represent a less restrictive means to controlling minors' access to content that inappropriate for them. This Court has already addressed the question of regulating minors' access to online content in the Reno v. ACLU and COPA which extended full First Amendment protection to Internet speech. In those cases, this Court concluded that the promotion of the use of voluntary user empowerment tools was a less restrictive means than government regulation for allowing parents to control their children's access to indecent content. In the gaming context, industry has voluntarily integrated user empowerment tools into gaming consoles and offline gaming systems; these tools, as well, point to a less restrictive means

than government regulations prohibiting minors' access to constitutionally protected speech.

2. Amici agree with Respondents that the statute in this case is unconstitutional in the offline context. But if the statute were to be upheld and then applied in the online context, compliance would be even more challenging. Age-based restrictions on access to content are prohibitively difficult to implement online. Information about a user's age is not transmitted during a typical Internet transaction, and age verification technologies are generally not effective online. Further, requiring websites to implement age verification technologies would burden the First Amendment rights of adults to access online content anonymously, and would have an unconstitutional chilling effect on the speech of video game providers and website operators.

The Internet has been a significant engine for innovation and expression, and much of this activity has greatly benefited from the fact that speakers can reach a global audience with a minimum of barriers. *Amici* — many of which have been directly involved in creating this medium — urge the Court to exercise caution in considering how the issues raised in this case might impact the continued expansion of speech online.

#### **ARGUMENT**

I. THIS CASE COULD HAVE A SIGNIFICANT IMPACT IN THE ONLINE ENVIRONMENT, AND THE COURT'S ONLINE "USER EMPOWERMENT" JURISPRUDENCE SHOULD GUIDE ITS DECISION HERE.

Although on its face this case does not involve online gaming, the Court should carefully consider how the issues raised here would play out in the online environment, for at least two reasons. First, although the California statute here does not cover online games, similar statutes in other states have sought to do so, and through its influence on future legislation the Court's decision here will have an impact in the online world. Second, the online context can also provide helpful guidance to the Court in reaching its determination on the constitutionality of the California statute. The Court should look at the robust development and voluntary adoption of parental and empowerment tools in the offline video gaming context, which can serve as the foundation for less restrictive means to protect children, enabling parents to control minors' access to content, just as such technology has played a pivotal role in online First Amendment jurisprudence.

#### A. The Court's Decision in This Case Could Have a Direct Impact on Online Gaming.

While Cal. Civ. Code § 1746 (the "Act") is focused on video game *devices*, the future of video

gaming is moving toward both online gameplay and online distribution of game software.<sup>2</sup> Other states have included "computer software" in their attempts regulate violent video game content, and the Court's decision in this case will influence how California and other states approach regulation of online gaming in the future.

The Act defines "video game" to be "any electronic amusement *device* that utilizes . . . its own monitor, or is designed to be used with a television set or a computer monitor . . . " Cal. Civ. Code § 1746 (emphasis added). This definition appears to cover only physical game systems, cartridges, and discs, and would not reasonably cover video or other games that are available only over the Internet to be played on a general-purpose computer. Other comparable state and local regulations – all of which have been overturned on similar First Amendment grounds as are presented here – have sought to regulate video games broadly enough to include the online environment. *See, e.g.*, Okla. Stat. title 21, § 1040.75 (effective Nov. 1, 2006) (found to be

<sup>&</sup>lt;sup>2</sup> See, e.g., Ken Sweet, The Video-Game Industry's Big Digital Shift, FOXBUSINESS, June 11, 2010, http://www.foxbusiness.com/markets/2010/06/11/video-game-industrys-big-digital-shift/; Alexander Sliwinski, NPD: PC retail and digital distribution sales reaching parity, JOYSTIQBETA, Jul. 21, 2010, http://www.joystiq.com/2010/07/21/npd-pc-retail-and-digital-distribution-sales-reaching-parity/. Increasing numbers of games are also available for download from the Internet as applications for mobile phones. See, e.g., Apple - Web apps – Games, http://www.apple.com/webapps/games/ (last visited Sept. 16, 2010) (offering over 1,000 game applications); Android Market, http://www.android.com/market/ (last visited Sept. 16, 2010).

unconstitutional in *Entertainment Merchants Ass'n v. Henry*, No. CIV-06-675-C, 2007 WL 2743097 (W.D. Okla. Sept. 17 2007)); Wash. Code, Title 9, Chapter 91, § 180 (effective July 27, 2003) (found to be unconstitutional in *Video Software Dealers Ass'n v. Maleng*, 325 F. Supp. 2d 1180 (W.D. Wash. 2004)).<sup>3</sup>

Moreover, the broad movement of the gaming industry has been toward online games – sometimes in connection with physical gaming systems, but often games that are *only* available online. In light of the migration of gaming online, and the repeated efforts of states and localities to regulate gaming, it is highly likely that, were the Court to uphold the Act in this case, future regulations would directly target the online environment. It is thus appropriate for the Court to consider the potential impact of this case on online gaming (as well as the influence that the Court's online jurisprudence can have on the issues raised here).

<sup>&</sup>lt;sup>3</sup> In fact, every statute attempting to regulate video game content, whether that content is accessed online or offline, has been struck down as a violation of the First Amendment. Beyond the Act in this case and the cases cited above, at least five other courts have struck down as unconstitutional efforts to regulate gaming. See, e.g., Video Software Dealers Ass'n v. Webster, 773 F. Supp. 1275, 1276 (W.D. Mo. 1992), aff'd, 968 F.2d 684, 687 (8th Cir. 1992); American Amusement Machine Ass'n v. Kendrick, 244 F.3d 572 (7th Cir. 2001); Entertainment Software Ass'n v. Granholm, 426 F. Supp. 2d 646 (E.D. Mich. 2006); Entertainment Software Ass'n v. Blagojevich, 404 F. Supp. 2d 1051 (N.D. Ill. 2005), aff'd, 469 F.3d 641 (7th Cir. 2006); Entertainment Software Ass'n v. Foti, 451 F. Supp. 2d 823 (2006).

As discussed below, concerns about minors' exposure to inappropriate content online are most appropriately addressed through the use of "userempowerment" tools that allow parents to make and enforce their own decisions about what is and is not suitable for their children to access. That approach has worked well in the online environment, being both less restrictive and more effective than direct government regulation, and it is an appropriate approach to apply to offline gaming. And, as discussed in Part II below, while this type of contentbased regulation of violent content fails strict scrutiny no matter what the medium, applying this type of regulation in the online context would present some significant additional difficulties. because, unlike in a bricks-and-mortar storefront, there is no effective way for content providers on the Internet to know whether a user visiting their sites is an adult or a minor.

#### B. In the Online World, Promotion of User Empowerment Tools Represents the Least Restrictive Means of Protecting Minors from Unwanted Content.

This case raises the question of whether government regulation can be imposed to shield minors from content depicting violence. We agree with Respondents that the Court should not create a new category of content that is placed outside of the First Amendment's protection. But even if the Court were to find that the government has a permissible interest in regulating minors' access to violent content, that interest would be best addressed by promoting the use of user empowerment tools that

allow parents to control what content is available to their children.

In the online and cable contexts, the Court has considered the goal of shielding minors from unwanted sexual content and has found that user empowerment tools provide a "less restrictive means" of achieving the governmental interests. See Ashcroft v. ACLU, 542 U.S. 656, 660 (2004) (COPA II). Applying strict scrutiny, see id., the Court has found that government-mandated restrictions on access to content are not the "least restrictive means" of achieving the government's interest to protect children. A plethora of user empowerment tools – developed through voluntary industry efforts to respond to consumer demand - give parents effective means to protect their own children while not unconstitutionally infringing First Amendment rights of adults to publish and access material online.

In the Communications Decency Act decision, Reno v. ACLU, 521 U.S. 544 (1997), the Court noted that parental control tools can provide a "reasonably effective method by which parents can prevent their children from accessing sexually explicit and other material which parents may believe is inappropriate for their children," id. (emphasis in original) (citing ACLU v. Reno, 929 F. Supp. 824, 842 (1996)). Subsequently in the context of cable TV, the Court held that "the objective of shielding children does not suffice to support a blanket ban if the protection can be accomplished by a less restrictive alternative." United States v. Playboy Entertainment Group, Inc., 529 U.S. 803, 814 (2000). In that case, the Court

concluded that parents' ability to protect their children on a targeted basis meant that a broader governmental regulation could not withstand strict scrutiny. *Id.* at 815.

The Court continued develop to jurisprudence concerning user empowerment tools in determining the constitutionality of the Child Online Protection Act (COPA), which prohibited making any communication for commercial purposes available online to a minor that included any material that is harmful to minors. In Ashcroft v. ACLU (COPA II), the Court upheld a preliminary injunction of COPA based on the Act's likely violations of the First Amendment. COPA II, 542 U.S. at 670-71. In that case, the Court noted that "[b]locking and filtering software is an alternative that is less restrictive than COPA and, in addition, likely more effective as a means of restricting children's access to materials harmful to them." Id. at 666-67. These user empowerment tools "impose selective restrictions on the receiving end, speech not universal restrictions at the source." Id. at 667. The Court noted that the District Court, in its fact-finding capacity, found that "blocking or filtering technology may be at least as successful as COPA would be in restricting minors' access to harmful material online without imposing the burden on constitutionally protected speech that COPA imposes on adult users or Web site operators." Id. at 663 (internal citation omitted).

### C. User Empowerment Tools Can Be Very Effective in Protecting Minors, Even from Violent Content.

After upholding the preliminary injunction against the COPA statute, this Court remanded the case so the District Court could make a final determination of whether filters are more effective than the challenged law. COPA II, 542 U.S. at 672-73. The District Court found that filters are "at least as effective, and in fact, are more effective than COPA in furthering Congress' stated goal for a variety of reasons." ACLU v. Gonzales, 478 F. Supp. 2d 775, 815 (2007). The Third Circuit concurred that the evidence produced at trial confirmed the initial determination that user empowerment tools were a constitutionally less restrictive alternative to the direct governmental regulation of speech in that case, see ACLU v. Mukasev, 534 F.3d 181, 188, 203-04 (3d Cir. 2009), and this Court denied certiorari review, see Mukasey v. ACLU, 129 S. Ct. 1032 (2009).

User empowerment tools remain the most successful — and constitutionally appropriate — approach to allowing parents to choose whether and how to control minors' online access to inappropriate content. The District Court on remand in the COPA case did extensive fact-finding on online filtering technology. Although that case of course focused on sexual content, the court noted in its findings of fact that some filters:

are highly customizable, allowing a parent to make detailed decisions about what to allow and what to block. Filtering products do this by, among other things, enabling parents to choose which categories of speech they want to be blocked (such as sexually explicit material, illicit drug information, information on violence and weapons, and hate speech) and which age setting they want the product to apply."

Gonzales, 478 F. Supp. 2d at 791. See also id. at 797 (noting that some filters block violent content); GETNETWISE, Tools filtering violent content, http://kids.getnetwise.org/tools/blockviolence. After extensive expert testimony and a review of the relevant research, the COPA trial court concluded that online filtering is highly effective in allowing parents to block children's access to unwanted sexual content. See Gonzales, 478 F. Supp. 2d at 794-97.

have concluded that Just as the courts filtering tools are the most effective and constitutionally appropriate approach to protecting sexual children from content, such user empowerment tools also provide the most appropriate answer for violent content. To the extent that parents are concerned about violent content online, industry has developed a broad range of filtering tools that enable parents to shield their children from such content. In light of these alternatives, direct government regulation of violent would online content not likely survive

constitutional scrutiny (if the Court were to conclude that such content could in any situation be regulated under the First Amendment).

### D. User Empowerment Tools Are Also the Solution to Regulating Children's Access to Violent Content in Offline Video Games.

Similar to filtering and blocking software for web browsers, user empowerment tools are already integrated into the console- and computer-based gaming systems contemplated in the California statute. The video game industry has made a concerted, and successful, effort to provide parents with options for controlling their children's access to certain types of content. The three major consoles – Nintendo Wii, Sony PlayStation 3, and Microsoft Xbox 360 – all include software tools designed to give parents control over what their children play.4 The Microsoft and Nintendo consoles allow parents to use the Entertainment Software Rating Board rating level to control children's access to inappropriate games. Adam Thierer, Parental Controls & Online Child Protection: A Survey of Tools &

<sup>&</sup>lt;sup>4</sup> See Mike Musgrove, A Computer Game's Quiet Little Extra: Parental Control Software, WASH. POST, Dec. 23, 2006, at D1, available at http://www.washingtonpost.com/wp-dyn/content/ article/2006/12/22/AR2006122201278.html; seealsoMicrosoft. Introduction toFamily Settings. http://www.xbox.com/en-US/support/familysettings/xbox360/ familysettings-intro.htm; NINTENDO, Parental http://www.nintendo.com/consumer/systems/wii/en\_na/settings ParentalControls.jsp; Sony, Using the Parental Control Settings, http://manuals.playstation.net/document/en/ps3/3\_15/ basicoperations/parentallock.html.

METHODS, 94 (2009), www.pff.org/parentalcontrols. These parental controls work with embedded flags in software, which allow consoles to automatically recognize a game's rating and restrict access. *Id.* at 95. Sony's PlayStation 3 console and PlayStation Portable handheld gaming system let parents use a numeric scale to determine the level of a game or DVD content they will allow their children to play. *Id.* at 96. Parental controls also allow parents "to manage who [their] kids play with, how and when they play, and for how much time." Entertainment Software Rating Board, *Setting Parental Controls*, 5 (2008), http://www.esrb.org/about/news/downloads/ESRB\_PTA\_Brochure-web\_version.pdf.

These tools go further than the California statute, which attempts to restrict the sale of games, by allowing parents to control what games are played on the system, no matter how they were obtained. These user empowerment tools, just like filters in the online space, are in many ways more effective than restrictions on sale, and they represent the least restrictive means of controlling minors' access to material in the offline space. As it considers the issues in this offline case, the Court should look to its online jurisprudence for guidance, and should conclude that efforts to promote parental empowerment tools are a less restrictive alternative to governmental regulation.

VIOLENT II. AN AGE-BASED CONTENT RESTRICTION WOULD BEHIGHLY PROBLEMATIC IN THE ONLINE WORLD BECAUSE OF THE INABILITY RELIABLY **DETERMINE** VERIFY OR THE AGES OF ONLINE USERS.

Depictions of violence have traditionally received the highest degree of protection afforded to speech under our Constitution. But if this Court were to declare, in a significant deviation from established precedent, that violent content receives lesser First Amendment protection and were to uphold the Act in this case, restrictions aimed at the online world would quickly follow. As noted above, some violent video game statutes have already sought to target online gaming, and game play and distribution is increasingly incorporating online platforms. It is thus appropriate for the Court to consider how its decision here could impact the online world. To that end, it is vital that the Court understand a critical characteristic of the online environment: the extreme difficulty (or even, in some contexts, impossibility) of reliably determining or verifying a minor's age online.

As discussed below, "age verification" technology does not function with the necessary level of accuracy in most online contexts and cannot effectively be used to separate minors from adults online. While age restrictions may be more feasible to apply in a bricks-and-mortar store — where the age of the customer can be gauged by sight and verified by reference to a driver's license or identification card (as occurs during the sale of

alcohol or tobacco) – age-based restrictions on access to content cannot be applied in the online environment with anything close to the same degree of certainty. The data transmitted to complete communications via the Internet does not include detailed identity information and the various purported "age verification" systems simply cannot establish the age of particular Internet users with the level of accuracy the Constitution would require of a content-based restriction on speech.

Further, a government mandate on website operators to implement these age verification systems would chill speech among adults and and would constitute website operators impermissible burden on speech. It is critical to acknowledge that any effort to "age verify" users to exclude minors would require that all users be raising significant additional issues. Because of these and other concerns, the Court in this case should be very cautious about going down a path that would lead to later practical and constitutional problems in the online world.

#### A. "Age Verification" Technologies Do Not Establish the Ages of Internet Users with the Level of Accuracy Needed to Avoid an Unconstitutional Chill on Speech.

Online age verification processes have been assessed by a range of courts and task forces, all of which have reached the same conclusion: Age verification technology does not work at all in some contexts, and in others does not work accurately

enough to satisfy the First Amendment concerns raised by age-based restrictions on access to constitutionally protected material. See, e.g., ACLU v. Gonzales, 478 F. Supp. 2d 775 (E.D. Pa. 2007); INTERNET SAFETY TECHNICAL TASK FORCE, ENHANCING CHILD SAFETY AND ONLINE TECHNOLOGIES (Dec. 31, 2008) ("ISTTF Report"). Indeed, this Court first acknowledged limitations of online "age verification" in its 1997 decision on the Communications Decency Act. See Reno v. ACLU, 521 U.S. 844, 855 (1997) (citing ACLU v. Reno, 929) F. Supp 824, 845 (E.D. Pa. 1996)).

Ten years later, the District Court in the COPA case looked more broadly and in greater detail at the issue of online "age verification." There, the court found that "there is no evidence of age verification services or products available on the market to owners of Web sites that actually reliably establish or verify the age of Internet users." Gonzales, 478 F. Supp. 2d at 800, aff'd sub nom.; Mukasey, 534 F.3d 181, cert. den. 129 S. Ct. 1032 (2009). The court reviewed several commonly cited methods of verifying a user's age and concluded, "[c]redit cards, debit accounts, adult access codes, and adult personal identification numbers do not in fact verify age." Gonzales, 478 F. Supp. 2d at 811.

The shortcomings of various approaches to age or identity verification online have been well documented. Requiring Internet users to pay for access to content with a credit card is often proposed as a solution,5 but credit card transactions do not verify that the user providing the information is an adult. Credit card-based "verification systems may be subject to evasion and circumvention, for example, by minors who have their own credit cards." COPA II, 542 U.S. at 668. "[M]inors under 17 have access to credit cards, debit cards, and reloadable prepaid cards. . . . [P]ayment card issuers are increasingly marketing credit cards, debit cards, and prepaid cards to minors as young as 13." Gonzales, 478 F. Supp. 2d at 801. In addition to minors who have legitimate access to their own credit cards or are authorized to use their parent's card, some minors may use a credit card belonging to a parent or other adult without that adult's knowledge or consent. Id. at 801.6 And the only information that is actually verified when a credit card is charged during an online transaction is that the user has access to a valid credit card number.

Services that match user-provided data to databases of public information also "do not verify the age or identity of an individual; instead, they

<sup>&</sup>lt;sup>5</sup> See, e.g. Child Online Protection Act, 47 U.S.C. 231(c)(1) ("It is an affirmative defense to prosecution . . . that the defendant, in good faith, has restricted access by minors to material that is harmful to minors by requiring use of a credit card, debit account, adult access code, or adult personal identification number. . . .").

<sup>&</sup>lt;sup>6</sup> Recognizing these shortcomings, "payment card associations in this country prohibit Web sites from claiming that use of a payment card is an effective method of verifying age, and prohibit Web site owners from using credit or debit cards to verify age. . . . Payment card associations in this country advise consumers not to offer payment cards to merchants as a proxy for age. . . ." *Gonzales*, 478 F. Supp. 2d at 801 (E,D, Pa. 2007).

merely verify the data entered by an Internet user." *Gonzales*, 478 F. Supp. 2d at 802. These types of data verification services cannot ensure that the person entering the data is in fact the person whose data is being verified. *Id.*<sup>7</sup> Moreover, these services are limited by the type, quality, and accuracy of the databases they can access and will not be able to provide information about people who are not U.S. citizens. *Id.* at 803.

The problem of online age verification is made all the harder because most minors lack *any* recognized formal identification. The district court on remand in COPA noted that it is "especially difficult for [data verification services] to verify young adults (between the ages of 17 and 21) or minors, because there is little data available on younger adults, and very little, if any, data available on minors." *Id*.

Another weakness in age verification systems is the potential for supposedly "verified" information to be used for circumvention. Some age verification

<sup>&</sup>lt;sup>7</sup> Online transactions that involve the sale of regulated items, including alcohol and tobacco, require the online merchants to verify the age of the purchaser. In these circumstances, adults have an incentive to verify their age correctly, and such purchases usually require an adult to receive delivery of the item (and thus verify his age in person). See Internet Safety and Technical Task Force, Enhancing Child Safety and Online Technologies 29 (Dec. 31, 2008). But "without a physical delivery of goods and an accompanying visual age verification, neither [a data verification service] nor the Web page operator can know whether an adult or a child provided the information. Attempting to verify age with this information in a consumernot-present transaction is therefore unreliable." *Id.* at 803.

systems verify the data that a user submits, and then create a login ID or other credential that the user can use to access age-restricted content in the future. See ISTTF Report, Appendix D at 9. These logins and credentials can be shared among users as a way to circumvent the age verification process. *Id.* at 29.8

There remain significant questions about the practicality and effectiveness of "age verification" technology in the online environment. The validity of any government prohibition on minors' access to constitutionally protected content would depend in part on the ability to accurately distinguish between minors and adults. As this Court considers how the statute in this case might be applied online, it should not assume that "age verification" technology is any more of a viable option today than it was in the 1990s during the CDA appeal or in the recently concluded COPA litigation.

## B. A Government Mandate on Websites to Implement Age Verification Technologies Would Infringe on Adults' First Amendment Rights.

Attempts to restrict minors' access to violent video games online would require websites to implement age verification technologies, requiring adults to disclose personal information in order to

<sup>&</sup>lt;sup>8</sup> "Unlike in financial contexts, users in online social settings may have reduced incentives to maintain the confidentiality of login IDs and credentials, and members of the [the ISTTF research board] report that sharing [login] credentials is common among young people." ISTTF Report at 29-30.

access that same material. This is an impermissible burden on free speech. The First Amendment protects the right to anonymous speech,9 which includes the right to send and receive material online without verifying one's identity. Mandatory age verification procedures would have significant chilling effects on adults' speech, as at least some adults would be deterred from accessing constitutionally protected material because they are unwilling to provide personal information in order to gain access to the content. 10 Age verification procedures would require adults to compromise their anonymity to access protected speech, which would have a particularly deterrent effect with regard to sensitive or controversial content that users may not want linked with their identities. See Denver Area Educ. Telecomm. Consortium, Inc. v. FCC, 518 U.S. 754 (1996) (striking down identification 727,requirement because it would "further restrict viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the 'patently offensive' channel"); Gonzales, 478 F. Supp. 2d at 812.11

McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995)
 See ACLU v. Ashcroft, 322 F.3d 240, 259 (3d Cir. 2003), aff'd, 542 U.S. 656 (2004).

<sup>&</sup>lt;sup>11</sup> See also ACLU v. Mukasey, 534 F.3d 181, 197 (3d Cir. 2009) (discussing the difference between online and offline methods of restricting minors' access to material that is constitutionally protected as to adults: "Blinder racks do not require adults to pay for speech that otherwise would be accessible for free, they do not require adults to relinquish their anonymity to access protected speech, and they do not create a potentially permanent electronic record. Blinder racks simply do not involve the privacy and security concerns that" age verification

As the District Court on remand in COPA found:

Requiring users to go through an age verification process would lead to a distinct loss of personal privacy. Many people wish to browse and access material privately and anonymously.... Web users are especially unlikely to provide a credit card or personal information to gain access to sensitive, personal, controversial, or stigmatized content on the Web. As a result of this desire to remain anonymous, many users who are not willing to access information non-anonymously will be deterred from accessing the desired information.

Gonzales, 478 F. Supp. 2d at 805-06. Age verification requirements would also produce a chilling effect among adults who have security concerns about providing site operators with sensitive information such as credit card numbers: "Requiring Internet users to provide payment card information or other personally identifiable information to access a Web site would significantly deter many users from entering the site, because Internet users are concerned about security on the Internet and because Internet users are afraid of fraud and identity theft on the Internet." *Id.* at 806.

As the Third Circuit concluded in the COPA case, age verification technology would "burden [material] which is constitutionally protected for adults" and would "drive this protected speech from the marketplace of ideas on the Internet." *Mukasey*, 534 F.3d at 193 (citing *ACLU v. Ashcroft*, 322 F.3d 240, 260 (3d Cir. 2003)). That court concluded that "[t]his type of regulation is prohibited under the First Amendment." *Id*.

# C. Any Requirement that Online Video Game Providers Implement Age Verification Would Be an Unconstitutional Burden on Their Speech.

Restricting minors' access to violent video games online through mandatory age verification processes would also place unconstitutional burdens on the First Amendment rights of the game developers and website operators who provide these games online. See Mukasey, 534 F.3d at 197. The costs associated with an age verification mandate would result in a twin infringement on game providers' First Amendment rights: the chilling effect on the game providers' constitutionally protected speech, and some decrease in the audience for their websites and games as a result of this self-censorship.

Age verification systems, though ineffective, are costly to implement. <sup>12</sup> "A statute is presumptively inconsistent with the First

<sup>&</sup>lt;sup>12</sup> See Reno, 521 U.S. at 856-57.

Amendment if it imposes a financial burden on speakers because of the content of their speech." Simon & Schuster, Inc. v. Members of the New York State Crime Victims Board, 502 U.S. 105, 115 (1991). Small game providers, start-up companies, individual designers creating games for an online-only audience, game developers and websites that want to offer their games for free, all would likely censor themselves in the face of a burdensome government mandate to implement age verification systems on their sites.

Moreover, game providers are also likely to lose some of the audience for their constitutionally protected speech if they implement age verification systems. Due to the costs associated with these systems, game providers would likely have to charge fees for their content. See Gonzales, 478 F. Supp. 2d at 804. Web users are often reluctant to provide personal information or to pay for content when there are other, free alternatives available; thus, one likely result of an age verification mandate would be to drive traffic to sites and games hosted outside of the United States, where any state or federal regulation would not apply. As the district court found in the COPA remand, "[b] ecause requiring age verification would lead to a significant loss of users, content providers would have to either self-censor, risk prosecution, or shoulder the large financial burden of age verification." Id. at 804-05. "Many users who are not willing to access information nonanonymously will be deterred from accessing the desired information. Web site owners . . . will be deprived of the ability to provide this information to those users." *Id.* at 806. Age verification procedures

"place substantial economic burdens on the exercise of free speech because all of them involve significant cost and the loss of Web site visitors, especially to those . . . who provide their content for free." *Id.* at 812-13.

\* \* \*

Any regulation of online content that imposes age-based requirements will encounter very significant practical and constitutional problems. A decision upholding such requirements in the offline world — for a new type of content previously unregulated — would be sure to lead to constitutional problems in the online context.

#### CONCLUSION

Amici appreciate that many parents would like to limit their children's access to certain types of content — including violent content — in both the online and offline worlds. Amici have strongly supported the development of user- and parental-empowerment tools that provide this type of control, to be used on a voluntary basis in the households that choose to use them. As Respondents make clear in their brief, the video game industry has been a leader in promoting parental control tools. Amici urge this Court to affirm the judgment below, and hold that these voluntary tools — and not governmental regulation of a new category of less-protected speech — are the best approach to achieve the social goals at issue here.

Respectfully submitted,

JOHN B. MORRIS, JR.

Counsel of Record

EMMA J. LLANSÓ

Center for Democracy & Technology
1634 I Street NW, Suite 1100

Washington, DC 20001
(202) 637-9800
jmorris@cdt.org

September 17, 2010