

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Implementation of the Child Safe Viewing Act;) MB Docket No. 09-26
Examination of Parental Control Technologies for)
Video or Audio Programming)

COMMENTS OF AT&T INC.

CHRISTOPHER M. HEIMANN
GARY L. PHILLIPS
PAUL K. MANCINI

Attorneys For:
AT&T INC.
1120 20th Street, NW
Suite 1000
Washington, D.C. 20036
(202) 457-3058 – phone
(202) 457-3074 – facsimile

April 16, 2009

TABLE OF CONTENTS

I.	Introduction.....	1
II.	The Purpose of the Child Safe Viewing Act is to Encourage Development, Deployment and Use of Technologies that Empower Parents to Decide What Media Content their Children May Access.....	4
	A. A Plethora of Parental Controls Already Exist	5
	B. Encouraging Further Development and Use of Paternal Controls Will Require a Multifaceted Approach by All Stakeholders, With Government Providing Leadership, but Not Imposing Mandatory Rules or Standards.....	9
III.	Conclusion.....	12

**Before the
Federal Communications Commission
Washington, D.C. 20554**

In the Matter of)
)
Implementation of the Child Safe Viewing Act;) MB Docket No. 09-26
Examination of Parental Control Technologies for)
Video or Audio Programming)

COMMENTS OF AT&T INC.

I. Introduction.

AT&T welcomes the Commission's efforts to gather information and prepare a report to Congress on the existence and availability of parental control tools that enable parents to protect children from inappropriate content (as determined by such parents) online and via other digital communications, and to examine methods to encourage development, deployment and use of such tools, as required by the Child Safe Viewing Act.¹ AT&T is a leading provider of communications and entertainment services, both wireline and wireless, in the United States, and thus has long been committed to developing and providing consumers, and, in particular, parents, the tools they need to ensure their safety and security (and that of their families and children) online, while, at the same time, safeguarding freedom of expression on the Internet. We therefore support Congress's and the Commission's objective of promoting the development, deployment and use of parental control tools that will further empower parents to limit their

¹ Child Safe Viewing Act of 2007, P.L. 110-452, 122 Stat. 5025 (December 2, 2008) (Child Safe Viewing Act or Act).

children’s access to content while at the same time preserving freedom of expression and the ability of each of our customers to access the lawful content of their choice.

In preparing its report to Congress, the Commission must recognize that it is not writing on a blank slate. Members of the Internet community, parents groups, state and government officials and other organizations already have compiled a substantial body of work regarding the risks children face online, and the variety of parental control and online child protection tools and methods already available, as well as those on the horizon. These include, *inter alia*, a recent report on “Enhancing Child Safety & Online Technologies” prepared by the Internet Safety Technical Task Force on behalf of the State Attorneys General of the United States,² the work of the Family Online Safety Institute (FOSI),³ and a special report prepared and updated on an ongoing basis by Adam Thierer for the Progress and Freedom Foundation extensively surveying the plethora of tools and methods in the marketplace today to protect children online and empower parents to decide for themselves what media content is appropriate for their children, and to limit their children’s access accordingly.⁴ In addition, social science researchers at numerous institutions, such as the University of New Hampshire Crimes Against Children Research Center and the Pew Internet and American Life Project, have conducted a variety of survey-based research to analyze the social behaviors of children on the Internet, including both

² “Enhancing Child Safety & Online Technologies,” Final Report of the Internet Safety Technical Task Force to the Multi-State Working Group on Social Networking of State Attorneys General of the United States at 6 (December 31, 2008) (“Enhancing Child Safety”).

³ See Family Online Safety Institute, *Making Wise Choices Online – Online Safety Initiatives* (2008) (“*Making Wise Choices Online*”). www.fosi.org

⁴ Adam Thierer, *Parental Controls & Online Child Protection: A Survey of Tools and Methods*, Progress & Freedom Foundation v. 3.1 (Fall 2008) available at: www.pff.org/parentalcontrols/ (“Parental Controls”).

the challenges and substantial benefits children derive from access to the Internet and the use of new forms of communications technology.⁵

These efforts have not been limited to the domestic sphere. As the Internet itself is a global medium, the concerns of online safety transcend national boundaries and, as a result, a variety of relevant work has been produced internationally. For example, in March of last year, the United Kingdom released the seminal Byron Review, which analyzed comprehensively the risks faced by children online and the array of available solutions, and made specific recommendations for a multi-stakeholder, cooperative response, which the UK government began implementing in June of last year.⁶

The Commission should build on this body of work, and, in particular, should heed the growing consensus that there is no single silver bullet to keep children safe online, nor is there an “easy technological fix to shield children from harmful content or to keep them from behaving inappropriately online.”⁷ Rather, what is needed is a multifaceted approach with all stakeholders (parents, the Internet community, law enforcement, and other governmental entities) working collaboratively to make the Internet as safe as possible for minors.⁸ In particular, members of the Internet community should continue to work with child safety experts, law enforcement, public policy advocates and others to develop and enhance a variety of tools for empowering parents to protect children online, and to educate consumers regarding the many tools available.⁹ Federal, state and local governments should allocate resources to better educate parents and children

⁵ See Enhancing Child Safety, Appendix A.

⁶ See <http://www.dcsf.gov.uk/byronreview/>

⁷ See Family Online Institute, *Making Wise Choices Online* at 5.

⁸ Enhancing Child Safety at 6.

⁹ *Id.*

regarding the risks children face online and the tools available to protect them. Government also should continue to encourage development, deployment and use of parental controls by funding research, bringing together stakeholders to communicate regarding advances in parental control technologies and best practices, and educating consumers to demand more and better online safety tools.¹⁰ The government, however, should not endorse or mandate any particular technology or set of technologies for protecting minors online because doing so would “stifle future progress in this area” by encouraging service providers to build to the standard or rule rather than continuing to innovate and invest to meet new online threats and challenges as they appear.¹¹ Finally, parents and children themselves must become better educated about the risks and threats minors face online, as well as the tools available to keep children safe online.¹²

II. The Purpose of the Child Safe Viewing Act is to Encourage Development, Deployment and Use of Technologies that Empower Parents to Decide What Media Content their Children May Access.

The Child Safe Viewing Act requires the Commission to examine the existence, availability and use of parental empowerment tools already in the market that enable parents to protect children from inappropriate content online (as determined by such parents), and to identify methods of encouraging development, deployment and use of such tools by parents, without affecting the packaging and pricing of a content provider’s offering.¹³ The Act thus seeks to promote tools that empower parents to determine for themselves what constitutes

¹⁰ *Id.*; see also Parental Controls at 13; *Making Wise Choices Online* at 2.

¹¹ *Enhancing Child Safety* at 35.

¹² *Id.* at 6.

¹³ *Implementation of the Child Safe Viewing Act; Examination of Parental Control Technologies for Video and Audio Programming*, MB Docket No. 09-26, Notice of Inquiry, FCC 09-14 at ¶¶ 1, 4 (rel. Mar. 2, 2009) (NOI).

acceptable media content for their children and to limit their children's access to content that is consistent with their own values.

A. A Plethora of Parental Controls Already Exist.

As FOSI, the Internet Safety Technical Task Force, Adam Thierer and others have documented, a variety of Internet service providers, communications companies, entertainment and video service providers, and others already have deployed a broad array of parental control technologies to help parents keep children safe online and prevent them from accessing inappropriate content.¹⁴ Indeed, as Adam Thierer has rightly pointed out, “*there has never been a time in our nation’s history when parents have had more tools and methods at their disposal to help them decide what constitutes acceptable media content in their homes and in the lives of their children.*”¹⁵

As one of the leading providers of communications and entertainment services in the United States, AT&T has long been committed to ensuring that families and children are safe and secure online, while, at the same time, safeguarding free expression on the Internet. AT&T thus has sought to educate consumers (and, in particular, parents and children) regarding the potential risks of harm online, and to provide parents the tools they need to protect children online, and across the full-suite of AT&T services – wireless, wireline, high speed Internet access and video. These tools range from content controls to channel and phone number blockers, enabling parents to protect their children from undesirable content, take steps to shield their children from potentially harmful contacts with other people, and establish limits on the technology children use on a daily basis.

¹⁴ See *Making Wise Choices Online, Enhancing Child Safety & Online Technologies, and Parental Controls and Online Child Protection*.

¹⁵ *Parental Controls and Online Child Protection* at 11 (emphasis in original).

For example, two years ago, AT&T introduced “AT&T Smart Limits™,” which included a new suite of wireless parental controls and a new comprehensive online resource for parental control information, and brings together, in one online portal, information explaining all of the parental control features available for the full suite of AT&T services, including directions on how to use controls for wireless, Internet, video and home phone services provided by AT&T.¹⁶ In particular, AT&T Smart Limits for Wireless™ allows parents, through an easy online setup, to set a variety of limits on how and when their children can use their wireless phone, including: the number of text and instant messages they may send and/or receive; the amount they may spend on downloadable purchases (such as ringtones and games); the amount of web-browsing allowed per billing cycle; the times of day the wireless phone may be used for messaging, browsing and outbound calls; whom the wireless phone can call or text by blocking certain numbers; as well as access to content inappropriate for children.¹⁷

AT&T’s parental controls for U-verse Television, AT&T’s IP-based television service, allow parents to determine who may watch what; block certain channels, live programs, and recorded programs; and set limits on ordering and watching on-demand videos. With channel blocking, a user may prevent a channel, or VoD, from appearing in the electronic programming guide displayed on a particular set-top box. Because these controls are implemented via the set-top box, parents can individually set each set-top box with the level of controls/blocking they desire, and thus tailor controls by TV (*e.g.*, setting a different level of controls for TVs in a living room or child’s room from that in the parent’s room).¹⁸

¹⁶ www.att.com/smartlimits.

¹⁷ *Id.*

¹⁸ <http://www.att.com/gen/sites/smartlimits?pid=11663>.

AT&T has implemented similar controls for its Internet access service. Specifically, AT&T's parental controls allow parents, at no cost, to control the content to which their children may obtain access to the Internet. AT&T Parental Control features for Internet service include:

- Customizable profiles for Kids, Teens and Adults. Parents may set a unique profile for up to five family members & define access to websites;
- Filter and block access to specific websites;
- Allow or deny access to E-mail, Instant Messaging; Chat rooms; Message Boards, Newsgroups, Personals, and File Sharing activities;
- Time limits that allow parents to define how much time their children may spend online;
- Software controls that permit parents to determine who can access specific software or files on a computer;
- Access requests that allow children to request access to blocked websites and applications, and allow parents to decide whether to allow such access;
- Usage reporting, which allows parents to monitor each family members online activity; and
- The ability to update parental control settings from any computer through a web-based interface.¹⁹

In addition to providing parental control tools, AT&T works both internally and with a variety of outside organizations to promote online safety education and awareness to both adults and children. For example, AT&T developed the AT&T Hometown Tours program, which visited more than 100 communities nationwide and worked with more than 20,000 students on Internet safety lessons, programs and workshops geared toward elementary- and middle-school-

¹⁹ <http://www.att.com/gen/sites/smartlimits?pid=8953>.

aged children. These focused on key Internet safety skills, such as protecting computers against viruses, hackers and spam, as well as reviewing age-appropriate content, and the potential dangers associated with social networking. And, working with our partner organizations (OASIS and SeniorNet), AT&T has helped the seniors learn to operate their wireless devices safely and efficiently through one-on-one coaching sessions. AT&T also has launched a cyber safety educational program for mature adults – *Safe Surfing* – with the National Caucus and Center on Black Aged, and provides the presentation at various fairs and seniors events across the country. Through these programs, AT&T already has reached out to more than 4000 senior consumers in 2009.²⁰

In addition, AT&T has worked with such organizations as Enough is Enough, iKeepSafe Internet Safety Coalition, and the Ad Council’s Internet Safety Coalition, as well as elected officials in community forums and town halls to provide educational materials to schools, parents and children. AT&T also offers a full library of supportive Internet safety and security tips and interactive safety games to increase awareness of Internet safety issues among parents and children.²¹

AT&T also has played a leadership role in a variety of industry and other initiatives to create a safer online environment for children. These include the Internet Safety Technical Task Force (which provided technical advice regarding the extent to which technologies can help address online safety risks to the Multi-State Working Group on Social Networking of the State Attorneys General of the United States) and the Family Online Safety Institute,²² which works to

²⁰ See <http://www.att.com/gen/general?pid=13299>.

²¹ See www.att.com/safety.

²² See www.fosi.org

make the online world safer for kids and their families by identifying and promoting best practices, tools and methods in the field of online safety. In addition, AT&T is a founding partner in Project Online Safety, an educational campaign focused on promoting Internet safety for children. AT&T thus is fully committed to efforts to encourage development, deployment and use of technologies that further empower parents to control their children's on-line activities.

B. Encouraging Further Development, Deployment and Use of Parental Controls Will Require a Multifaceted Approach by All Stakeholders, With Government Providing Leadership, but Not Imposing Mandatory Rules or Standards.

As noted above, the government alone cannot ensure the safety of children using the Internet or digital communications more generally, nor will mandates that inevitably require narrowly-focused and static solutions truly encourage further development, innovation, deployment and use of advanced parental control technologies and methods. Rather, what is needed is a multifaceted approach with all stakeholders – private industry, government, law enforcement, social science researchers, social health experts, school officials, teachers, parents and children – working collaboratively to make the Internet and the use of digital communications as safe as possible for minors.²³ Private industry, for example, should continue to work with child safety experts, law enforcement, government officials, public policy advocates, social science researchers and others to develop and improve a variety of tools for empowering parents to protect children online, and to educate consumers regarding the many tools available.²⁴ Parents, teachers and other caregivers must become educated regarding the risks facing minors online and the tools available to protect them. They further must pass this knowledge on to children and teach them how to protect themselves.

²³ Enhancing Child Safety & Online Technologies at 6.

²⁴ *Id.*

Federal, state and local governments also have a critical role to play in helping to keep the Internet safe for families and children. Most importantly, government can and should allocate resources to promote online safety awareness and to better educate parents and children regarding the risks children face online and the tools available to protect them. Educational programs and other community outreach programs to increase awareness regarding online safety will enable consumers to understand the risks of online behavior and how to protect themselves. Better educated and more technically-savvy parents, children, and Internet users more generally, in turn, are more likely to demand more and better online safety controls, which, in turn, will encourage service providers to innovate and improve parental controls to meet that demand. AT&T notes, in this regard, that the Commission has a long history of informing the public through consumer alerts regarding a variety of consumer issues, and it could do so here as well. In addition, government has an important role to play by, *inter alia*, funding research; bringing together stakeholders to communicate regarding advances in parental control technologies and best practices; and coordinating state, local and federal government programs and initiatives relating to online safety.²⁵

Adopting uniform standards or mandatory rules relating to parental control technologies and methods would not achieve the objectives of the Child Safe Viewing Act. While cross-industry standards, and consistency and compatibility of advanced blocking technologies across devices and platforms may appear to be a desirable goal, differences between platforms and devices will make it difficult, if not impossible, to achieve that objective. But, even if uniform standards or controls were feasible, the benefits likely would be far outweighed by their detriments. As an initial matter, attempting to pursue uniform blocking or filtering technologies across platforms and devices likely would result in a lowest common denominator approach

²⁵ *Id.*; see also Parental Controls at 13; *Making Wise Choices Online* at 2.

because of the different capabilities offered by various technologies and platforms. Additionally, because devices and technologies – and the way in which consumers use those devices and technologies – are constantly and rapidly evolving, any standard or control likely would be obsolete before it was fully implemented. Moreover, mandating cross-platform solutions inevitably would remove incentives on the part of service providers to innovate and develop new technologies and methods for empowering parents, and deprive them the flexibility to do so.²⁶

In addition, mandates inevitably would be focused on attempting to solve the prevailing concern of the day, which as the relatively short history of the Internet has shown, can radically change over a short period of time. For example, as the Internet Safety Technical Task Force Report recently found, cyberbullying (which involves instances of youths intimidating or otherwise harassing other youths using the Internet or other forms of digital communications, and has grown in prevalence alongside the rise of social networking) appears to be the most far-reaching challenge that youths face on the Internet today. This issue, however, is relatively new when compared to the issue of accessing harmful or inappropriate content, and likely requires different responses and solutions than the ones used to deter children from accessing such content. In fact, cyberbullying is an excellent example of an issue where technology tools may allow parents become aware of circumstances that involve their children, but not (in and of themselves) to solve the problem or change the behavioral patterns of children. Cyberbullying thus illustrates why comprehensive, multi-faceted, multi-stakeholder, cooperative approaches ultimately are necessary.

²⁶ Enhancing Child Safety & Online Technologies at 35 (“endorsement of any one technological approach would stifle future progress in this area”).

In this regard, the history of the V-chip is instructive. In 1996, Congress required the incorporation of blocking technology in television sets.²⁷ In 1998, the Commission adopted rules requiring television sets with screens 13 inches or larger to be equipped with a V-chip.²⁸ A study by the Annenberg Public Policy Center shows that, a decade later, the V-chip is not widely used because parents either are unaware of it or find it difficult and confusing to use.²⁹ And, although parental controls for other devices and platforms have evolved, manufacturers have had no incentive to improve V-chip technology and make it easier to use because they are required to build devices to comply with the Commission’s mandatory V-chip standards. Thus, any government mandated standards would become (like the V-chip) a ceiling, rather than a floor, as providers sought simply to comply with regulatory requirements rather than seeking new and improved methods of protecting children and families.

III. Conclusion.

As children today spend an ever increasing amount of time interacting with each other and the world through a variety of electronic media – including the Internet, wireless devices, and television – parents, family advocates, and government officials rightly have become concerned about the many risks children face online. Internet service providers, phone companies, wireless providers, video service providers, online providers and others have responded to these concerns by deploying a broad array of parental control technologies to help parents keep children safe online and prevent them from accessing inappropriate content. The government can help encourage further development, deployment and use of such tools, *inter*

²⁷ 47 U.S.C. § 303(x).

²⁸ *Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings*, 13 FCC Rcd 11248 (1998).

²⁹ NOI at ¶ 15 (“The study showed that many parents are not aware that they have a V-chip and others find that ‘programming the V-chip is a multi-step and often confusing process.’”), citing The Annenberg Public Policy Center, *Parent’s Use of the V-Chip to Supervise Children’s Television Use*.

alia, by educating parents about Internet safety, pulling together all stakeholders to communicate and exchange information about advances in control technologies, and funding further research. It should not, however, seek to encourage or impose uniform standards or mandatory rules relating to parental control technologies and methods.

Respectfully submitted,

/s/ Christopher M. Heimann

Christopher M. Heimann
Gary L. Phillips
Paul K. Mancini

AT&T Inc.
1120 20th Street, NW
Washington, D.C. 20036
202-457-3058
Its Attorneys

April 16, 2009