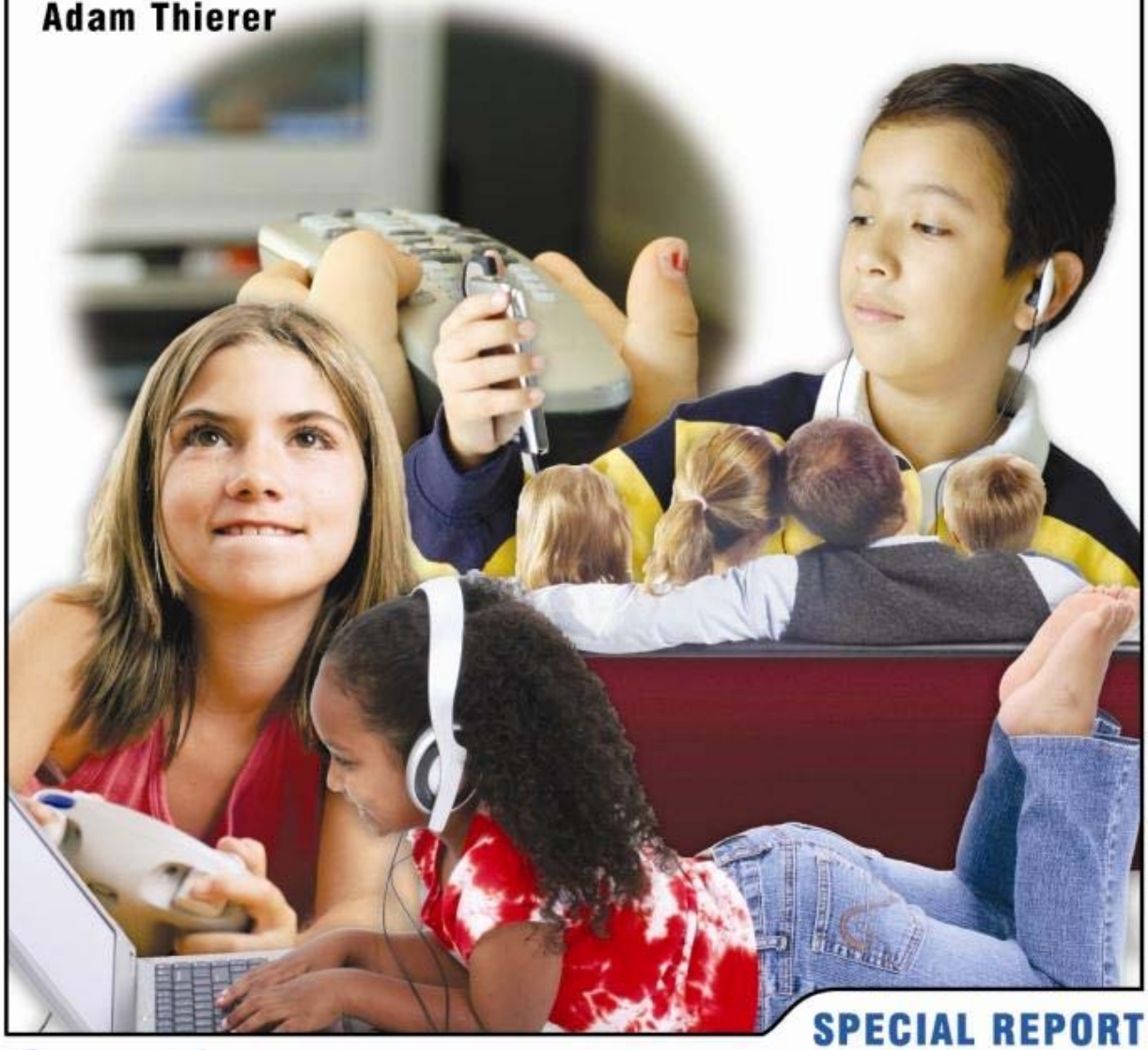
PARENTAL CONTROLS & ONLINE CHILD PROTECTION:

A Survey of Tools and Methods

Adam Thierer



SPECIAL REPORT

THE PROGRESS & FREEDOM FOUNDATION

Parental Controls and Online Child Protection:
A Survey of Tools and Methods

Version 2.2
July 2007

Adam Thierer
The Progress & Freedom Foundation
(www.PFF.org)
Washington, D.C.

PFF *Special Report*

Library of Congress Catalog Card Number: Pending
ISBN: Pending

TABLE OF CONTENTS

LIST OF EXHIBITS

— Author's Note —

In this report, I have attempted to provide a comprehensive survey of the wide variety of parental control and online child protection tools and methods that exist today. I have undoubtedly missed some things, however. I encourage readers to send me suggestions about what should be included in subsequent editions of this report. I hope to publish frequent updates (available online at www.pff.org/parentalcontrols) to ensure that I have painted the most thorough, up-to-date picture of the amazingly diverse universe of parental control tools and methods.

Second, there are many books and studies that deal with how best to raise your children and the role media and technology should (or shouldn't) play in their lives.[†] This report takes a different approach. Even though the report contains a variety of recommendations and helpful tips for parents, I have done my best to avoid a "preachy" tone because I believe that every family will bring different values and approaches to the challenging task of raising children and dealing with unwanted media exposure. My goal here is to provide parents with an exhaustive inventory of the tools and methods at their disposal that can assist them in that effort, however they choose to go about it.

— Adam Thierer[‡]

[†] Some of my personal favorites include: Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), www.pluggedinparent.com; Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), www.cskcst.com; Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), www.myspaceunraveled.com

[‡] Adam Thierer (athierer@pff.org) is a senior fellow with The Progress & Freedom Foundation and the director of its Center for Digital Media Freedom. The views expressed in this report are his own.

I. Introduction: Why Parental Controls Are Important

> *"Our government should not be in the business of choosing which programs are appropriate for our nation's children. By showing the public how to use available blocking mechanisms, we ensure those in the best position to make viewing decisions—parents—are able to do so."*
>
> — Senator Ted Stevens, vice chairman of the Senate Commerce Committee.[1]

What effect does media exposure have on our children? That question has generated heated debates from one generation to the next. From the waltz to rock and roll to rap music, from movies to comic books to video games, from radio and television to the Internet and social networking websites—every new media format or technology spawns a fresh debate about the potential negative effects it might have on kids.[2] Parents, educators, academics, social scientists, media pundits, and many others all offer their opinions, but rarely is any consensus reached.

Inevitably, these social and cultural debates become political debates. Indeed, each of the media technologies or outlets mentioned above was either regulated or threatened with regulation at some point in its history. And the cycle continues. For example, during the 109th session of Congress, several hearings were held and multiple bills introduced on a wide variety of content-related issues. These proposals dealt with broadcast television and radio programming, cable and satellite television content, video games, the Internet, social networking sites, and other types of online content.[3] Many of the policymakers

---

[1] Ted Stevens, "Guest Columnist: State of Decency in DC," *CableFax*, vol. 17, no. 69, April 10, 2006, http://stevens.senate.gov/public/index.cfm?FuseAction=Files.View&FileStore_id=d0450162-bbf2-4326-86da-a835636c43ad

[2] For examples, see Tom Standage, "Those Darn Kids and Their Darn New Technology," *Wired*, April 2006, pp. 114-5; James A. Monroe, *Hellfire Nation: The Politics of Sin in American History* (New Haven, CT: Yale University Press, 2003).

[3] For a discussion of some of these measures, see Adam Thierer, "Thinking Seriously about Cable and Satellite Censorship: An Informal Analysis of S. 616, The Rockefeller-Hutchison Bill," Progress & Freedom Foundation *Progress on Point* no. 12.5, April 2005, www.pff.org/issues-pubs/pops/pop12.6cablecensorship.pdf; Adam Thierer, "Moral and Philosophical Aspects of the Debate over A La Carte Regulation," Progress & Freedom Foundation *Progress Snapshot* 1.23, December 2005, www.pff.org/issues-pubs/ps/ps1.23alacarte.pdf; Adam Thierer, "Kid-Friendly" Tiering Mandates: More Government Nannyism for Cable TV," Progress & Freedom Foundation *Progress Snapshot* 1.2, May 2005, www.pff.org/issues-pubs/ps/ps1.2familyfriendlytiering.pdf; Adam Thierer, "A 'Voluntary' Charade: The 'Family-Friendly Tier' Case Study," Progress & Freedom Foundation *Blog*, December 13, 2005, http://blog.pff.org/archives/2005/12/a_voluntary_cha.html#more; Adam Thierer, "Fact and Fiction in the Debate over Video Game Regulation," Progress & Freedom Foundation *Progress Snapshot* 13.7, March 2006, www.pff.org/issues-pubs/pops/pop13.7videogames.pdf; Adam

and groups supporting these efforts argue that parents are essentially powerless to stop the flow of objectionable media content in their homes. Therefore, in the name of protecting children, they argue that government regulation is required.

Perhaps the most troubling aspect about these calls for increased content controls, however, is that they ignore the fact that parents have many constructive alternatives to government regulation at their disposal. This study documents the many tools and techniques that parents can use to better control media content before they call on government to do this job for them. The conclusion: 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 is acceptable in their homes and in the lives of their children.

A. A Broad View of Parental Controls

Parental controls will be defined broadly throughout this report to include *any tool or method that parents might use to restrict or tailor the media content their family consumes.* The "restrict *or tailor*" qualifier is important. Too often, parental controls are viewed as being merely restrictive in character. That is, they are used to block or filter media content. That is certainly one important use for parental controls; perhaps even the most important use for many families. But content *tailoring* is an equally important part of the parental controls mix.

Content tailoring refers to parents' use of any tool or method that *enables* their families to see, hear, or consume content they would regard as "better" (i.e., more educational, enriching, or ethical) for them. This is perhaps the most exciting part of the parental controls story today. Parental control tools and methods now exist that make it easier than ever before to tailor media content and consumption to a family's specific needs and desires. For example, as the Federal Communications Commission (FCC) noted in a recent report, "through the use of advanced set-top boxes and digital video recorders, and the introduction of new mobile video services, consumers are now able to maintain more control over what, when, and how they receive information."[4]

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 is acceptable in their homes and in the lives of their children.

Thierer, "Saving Online Free Speech: A Voluntary Code of Conduct for Internet Operators," Progress & Freedom Foundation *Progress Snapshot* 2.19, August 2006, www.pff.org/issues-pubs/ps/2006/ps_2.19_conduct_net_ops.pdf

[4] Federal Communications Commission, *Twelfth Annual Video Competition Report*, MB Docket No. 05-255, February 10, 2006, p. 4, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-11A1.pdf

Regardless of which approach parents prefer, Parts II and III of this study will document the many tools and methods at their disposal to restrict or tailor media content in their lives and their lives of their children. Part II highlights the various formal and informal household media rules that parents can use to restrict or tailor media to their preferences or values. Part III will then provide a sector-by-sector survey of the rating systems and technological tools available to parents if they wish to take advantage of more stringent controls.

This study will also discuss online child protection efforts, primarily in Part V. Many parental control technologies help parents shield their children from potentially objectionable media content, including Internet content. But the debate about online child protection has another, more serious, dimension because of concerns about child pornography or child predation. I refer to this problem as the "bad-people" problem, vis-à-vis the "bad-pictures" (objectionable, but legal media content) problem.

All too often, the bad-pictures and bad-people problems get conflated when, in fact, they are two very different issues that deserve different treatment and solutions. Much, if not all, of the bad-pictures problem can be dealt with by parents on their own without resorting to any government regulation. But, in addition to parental oversight and education, the bad-people problem demands a government role, primarily in the form of stepped up enforcement efforts and penalties to combat child predation. Importantly, in many cases, policymakers are currently misallocating resources by sometimes obsessing over regulatory solutions to the bad-pictures problem when they should be plowing almost all their time and resources into handling the far more serious bad-people problem. Part V of this report will discuss that problem in greater detail and call on lawmakers and law enforcement officials to redouble their efforts on this front.

The best answer to the problem of unwanted media exposure is for parents to rely on a mix of technological controls, informal household media rules, and, most importantly, education and media literacy efforts.

As Part IV will illustrate, education is also a vital part of parental controls and online child protection efforts. In fact, if there is one thing that this report will seek to impress upon the reader it is that, regardless of how robust they might be today, parental control tools and rating systems are no substitute for education—of both children and parents. Thus, the best answer to the problem of unwanted media exposure is for parents to rely on a mix of technological controls, informal household media rules, and, most importantly, education and media literacy efforts. And government can play an important role by helping educate and

empower parents and children to help prepare them for our new media environment.

That was the central finding of a blue-ribbon panel of experts convened in 2002 by the National Research Council of the National Academy of Sciences to study how best to protect children in the new interactive, "always-on" multimedia world. Under the leadership of former U.S. Attorney General Richard Thornburgh, the group produced a massive report that outlined a sweeping array of methods and technological controls for dealing with potentially objectionable media content or online dangers. Ultimately, however, the experts used a compelling metaphor to explain why education was the most important tool on which parents and policymakers should rely:

> Technology—in the form of fences around pools, pool alarms, and locks—can help protect children from drowning in swimming pools. However, teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning. Does this mean that parents should not buy fences, alarms, or locks? Of course not—because they do provide some benefit. But parents cannot rely exclusively on those devices to keep their children safe from drowning, and most parents recognize that a child who knows how to swim is less likely to be harmed than one who does not. Furthermore, teaching a child to swim and to exercise good judgment about bodies of water to avoid has applicability and relevance far beyond swimming pools—as any parent who takes a child to the beach can testify.[5]

Regrettably, we often fail to teach our children how to swim in the new media waters. Indeed, to extend the metaphor, it is as if we are generally adopting an approach that is more akin to just throwing kids in the deep end and waiting to see what happens. To rectify this situation, a serious media literacy agenda is needed in America. Media literacy programs teach children and adults alike to think critically about media to better analyze and understand the messages that media providers are communicating. Part IV of this report will argue that government should push media literacy efforts at every level of the education process. And those efforts should be accompanied by widespread public awareness campaigns to better inform parents about the parental control tools, rating systems, online safety tips, and other media control methods at their disposal.

This represents an *education and empowerment* approach that government(s) can adopt to help families deal with media content as opposed to the traditional regulatory approaches generally favored by lawmakers. This approach, which I also refer to as the "Tools, Rules, Schools, and Talk" strategy,

---

[5] Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 187.

has the added benefit of clearly falling within the boundaries of the Constitution, which is important for reasons discussed next.

B. Parental Controls and the Law

The current state of parental control tools and online child protection efforts is also important because it has a profound effect on the legal and regulatory status of many modern media providers or various types of speech and expression. Public policy discussions about content regulation have long been tied up with thorny debates about what constitutes the proper "community standard" for determining the appropriateness of certain types of speech or media content.

The current state of parental control tools and online child protection efforts is also important because it has a profound effect on the legal and regulatory status of many modern media providers or various types of speech and expression.

That's because, in the past, it was quite difficult for individual households to tailor media content—especially broadcast television and radio content—to their specific needs or values. In essence, the off button on TVs and radios was the only technical control at a parent's disposal. In that environment, many believed that government needed to act as surrogate for parents given the lack of control families had over their media decisions and encounters. In other words, because it was difficult for families to enforce their own "household standard," the government would step in and create a baseline—but quite amorphous and sometimes completely arbitrary—"community standard" for the entire nation. And that community standard would be enforced by law and treat all households as if they had the same tastes or values.

For example, in the context of broadcast television and radio programming, the Supreme Court famously held in the 1978 *Pacifica* case that FCC oversight and regulatory penalties (i.e., fines or license revocation) would help prevent "uninvited" programming from acting as an "intruder" into the home.[6] By a slim 5-4 margin, that logic became the law of the land for broadcasting and remains so today.

Similar arguments would be put forward by policymakers in the mid-1990s when they sought to impose restrictions on Internet and video game content. Courts have rejected these efforts, however. In striking down the Communications Decency Act's effort to regulate underage access to adult-oriented websites, the Supreme Court declared in *Reno v. ACLU* (1997) that a

[6] *FCC v. Pacifica Foundation*, 438 U.S. 726, 727-8 (1978).

law that places a "burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving" the same goal.[7] And several lower courts have rejected regulation of video game content on similar grounds.[8]

What is most interesting about these recent Internet and video game decisions is that the same logic could be applied to many other types of media outlets and content—including broadcasting. Indeed, this study reveals that many "less restrictive alternatives" are available to parents today to help them shield their children's eyes and ears from content they might find objectionable, regardless of what that content may be.

If it is the case that families now have the ability to effectively tailor media consumption to their own preferences—that is, to craft their own "household standard"—the regulatory equation should also change. Regulation can no longer be premised on the supposed helplessness of households to deal with content flows if families have been empowered and educated to make content determinations for themselves.

If it is the case that families now have the ability to effectively tailor media consumption to their own preferences—that is, to craft their own "household standard"—the regulatory equation should also change.

In fact, in another recent decision, the Supreme Court confirmed that this would be the new standard to which future government enactments would be held. In *United States v. Playboy Entertainment Group* (2000),[9] the Court struck down a law that required cable companies to "fully scramble" video signals transmitted over their networks if those signals included any sexually explicit content. Echoing its earlier holding in *Reno v. ACLU,* the Court found that less restrictive means were available to parents looking to block those signals in the home. Specifically, the Court argued that:

> [T]argeted blocking [by parents] enables the government to support parental authority without affecting the First Amendment interests of speakers and willing listeners—listeners for whom, if the speech is unpopular or indecent, the privacy of their own homes may be the optimal place of receipt. Simply put, targeted blocking is less restrictive than

[7] *Reno v. ACLU*, 521 U.S. 844 (1997).
[8] See Adam Thierer, "Fact and Fiction in the Debate over Video Game Regulation," Progress & Freedom Foundation *Progress Snapshot* 13.7, March 2006, www.pff.org/issues-pubs/pops/pop13.7videogames.pdf
[9] *United States v. Playboy Entertainment Group,* 529 U.S. 803 (2000).

> banning, and the Government cannot ban speech if targeted blocking is a feasible and effective means of furthering its compelling interests.[10]

More importantly, the Court held that:

> It is no response that voluntary blocking requires a consumer to take action, or may be inconvenient, or may not go perfectly every time. A court should not assume a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act.[11]

This is an extraordinarily high bar the Supreme Court has set for policymakers wishing to regulate modern media content. Not only is it clear that the Court is increasingly unlikely to allow the extension of broadcast-era content regulations to new media outlets and technologies, but it appears certain that judges will apply much stricter constitutional scrutiny to *all* efforts to regulate speech and media providers in the future, including broadcasting. As constitutional scholar Geoffrey R. Stone, professor of law at the University of Chicago School of Law, has noted:

> The bottom line, then, is that even in dealing with material that is "obscene for minors," the government cannot *directly* regulate such material... Rather, it must focus on empowering parents and other adults to block out such material at their own discretion, by ensuring that content-neutral means exist that enable individuals to exclude constitutionally protected material they *themselves* want to exclude. Any more direct regulation of such material would unnecessarily impair the First Amendment rights of adults.[12]

This is why parental control tools and methods are more important than ever before. The courts have largely foreclosed government censorship and placed responsibility over what enters the home squarely in the hands of parents.

C. Parental Controls, Personal Responsibility, and a Free Society

And that is how it should be. Decisions about acceptable media content are extraordinarily personal; no two people or families will have the same set of values, especially in a nation as diverse as ours. Consequently, it would be optimal if public policy decisions in this field took into account the extraordinary diversity of citizen and household tastes and left the ultimate decision about

[10] *Ibid.* at 815.
[11] *Ibid.* at 824.
[12] Geoffrey R. Stone, "The First Amendment Implications of Government Regulation of 'Violent' Programming on Cable Television," National Cable and Telecommunications Association, October 15, 2004, p. 10, www.ncta.com/ContentView.aspx?hidenavlink=true&type=lpubtp5&contentId=2881

acceptable content to them. That's especially the case in light of the fact that most U.S. households are made up entirely of adults. According to the Census Bureau, only one-third of U.S. households include children under the age of 18.[13]

Importantly, household-based controls need not be perfect to be preferable to government controls. That is particularly true because of the First Amendment values at stake here, as the Supreme Court noted in the *Playboy* decision. Absent removing all media devices from a home, it would be impossible to eliminate all unwanted or unexpected encounters from life.[14] Parental control tools and methods will not always provide perfect protection, but they can act as training wheels or speed bumps along the media paths that children seek to go down *without destroying those paths altogether as government censorship would do.*

Household-based controls need not be perfect to be preferable to government controls. That is particularly true because of the First Amendment values at stake

It's also worth noting that older media sectors (books, magazines, or newspapers, for example) offer far fewer parental controls but have generally received the maximum protection of the First Amendment. It only makes sense to accord similar First Amendment treatment to new digital media providers and content. As we move toward a fully converged media world, where the same content flows across multiple media platforms and devices,[15] it will be essential to apply a consistent set of First Amendment protections to ensure that all technologies and speakers are treated equally in the eyes of the law.[16]

So, Senator Stevens is right when he argues that "our government should not be in the business of choosing which programs are appropriate for our nation's children." The same goes for the music they listen to, the websites they surf, the games they play, the books they read, and so on. Public officials should not act *in loco parentis* when parents have the power to make media decisions

---

[13] U.S. Census Bureau, *2007 Statistical Abstract of the United States*, Table No. 57, p. 52, available at www.census.gov/prod/2006pubs/07statab/pop.pdf

[14] Of course, this is the case outside the home as well. Consider ball games, shopping malls, and even parks and playgrounds.

[15] Henry Jenkins, founder and director of the MIT Comparative Media Studies Program and author of *Convergence Culture: Where Old and New Media Collide*, defines convergence as "the flow of content across multiple media platforms, the cooperation between multiple media industries, and the migratory behavior of media audiences who will go almost anywhere in search of the kinds of entertainment experiences they want." Henry Jenkins, *Convergence Culture: Where Old and New Media Collide* (New York: New York University Press, 2006), p. 2.

[16] See Adam Thierer, "Why Regulate Broadcasting: Toward a Consistent First Amendment Standard for the Information Age," Catholic University Law School *CommLaw Conspectus*, vol. 15, pp. 431-482, Summer 2007; http://commlaw.cua.edu/articles/v15/15_2/Thierer.pdf

on their own; raising children, and determining what they watch, play, read, listen to, or download, is a quintessential parental responsibility.

Of course, it isn't easy. Parenting is tough work; probably the most challenging task we will ever undertake as adults. Luckily, as this report will hopefully prove, parents have more tools and methods at their disposal than ever before to help them carry out this difficult responsibility. But there isn't any one, silver bullet tool or method that will get the job done on its own. As Exhibit 1 illustrates, we will need to adopt a "layered" approach to parental controls and online child protection to do the job right. This four-layer strategy of "Tools, Rules, Schools, and Talk" is discussed throughout the rest of this report.

Exhibit 1:
A Layered Approach to Parental Controls and Child Protection

Strategy Name	Some Examples	Primarily Led By..	Section in Study
"Tools"	V-Chip, STB Controls, Ratings, Filters, Monitoring Tools, etc	Industry & Nonprofits	Part III
"Rules"	"Where, When, What & How Much" Rules	Parents	Part II
"Schools"	K-12 Media Literacy Programs & Online Safety Lessons	Schools, Nonprofits & Parents	Part IV
"Talk"	Ongoing Dialogue with Kids	Mostly Parents + Educators, Health officials, etc.	All

II. Household Media Rules and Informal Parental Control Methods

Before outlining the many media-specific parental control tools and technologies that are available today (summarized in Part III), it is important to realize that many household-level rules and informal parental control methods exist that are equally important elements of this story. In fact, in many ways, these household efforts represent the most important steps that most parents can take in dealing with potentially objectionable content or teaching their children how to be sensible, savvy media consumers. Indeed, to the extent that many households never take advantage of the many technical controls discussed in Part III, it is likely because they rely instead on the informal household media rules discussed here in Part II.

A. Household Media Consumption Rules

To begin, there are formal and informal household "media consumption rules." A 2003 Kaiser Family Foundation survey found that "Almost all parents say they have some type of rules about their children's use of media."[17] More recent Kaiser surveys have bolstered that finding. For example, a 2006 Kaiser survey of families with infants and preschoolers revealed that 85 percent of those parents who let their children watch TV at that age have rules about what their child can and cannot watch.[18] Of those parents, 63 percent say they always enforce those rules. About the same percentage of parents said they had similar rules for video game and computer usage. Likewise, a June 2007 Kaiser poll revealed that:[19]

- 65 percent of parents say they closely monitor their children's media use;
- 73 percent of parents say they know a lot about what their kids are doing online;
- 87 percent of parents check their children's instant messaging "buddy lists;"
- 82 percent of parents review their children's social networking sites; and,
- 76 percent of parents look to see what websites their children have visited.

Parents use a wide variety of household media consumption rules. Some can be quite formal in the sense that parents make the rules clear and enforce them routinely in the home over a long period. Other media consumption rules

[17] *Zero to Six: Electronic Media in the Lives of Infants, Toddlers and Preschoolers*, Kaiser Family Foundation, Fall 2003, p. 9, available at www.kff.org/entmedia/entmedia102803pkg.cfm

[18] *The Media Family: Electronic Media in the Lives of Infants, Toddlers, Preschoolers and Their Parents*, Kaiser Family Foundation, May 2006, p. 20, www.kff.org/entmedia/7500.cfm

[19] Victoria Rideout, *Parents, Children & Media*, Kaiser Family Foundation Survey, June 2007, http://www.kff.org/entmedia/entmedia061907pkg.cfm

can be fairly informal, however, and are enforced on a more selective basis. Regardless, these household media consumption rules can be grouped into three general categories: (1) "where" rules; (2) "when and how much" rules; and, (3) "under what conditions" rules.

(1) **"Where" Rules**: One of the most important steps that parents can take to better control their children's media usage is to establish firm rules regarding where their children can do so. "We don't have to say no to having TVs, video games, or computers in our homes," argues Dr. David Walsh, president and founder of the National Institute on Media and the Family, "but we should say no to where some of the screens go."[20]

For example, parents can assign a specific television or computer for most media usage and then take steps to ensure that those devices have screening or filtering controls installed and programmed. Additionally, parents can require that their children consume media (TV, Internet, video games, etc.) in a specific room or area of the house where they can keep an eye or ear on what their kids are doing.

To the extent that many households never take advantage of technical controls, it is likely because they rely instead on the informal household media rules.

At a minimum, parents can start by at least getting televisions, computers, and game consoles out of kids' bedrooms so they can monitor what is going on. According to a Kaiser survey, 68 percent of 8 to 18 year-olds have televisions in their bedrooms and 31 percent have computers.[21] Parents who let their kids lock themselves in their rooms with media devices have surrendered their first line of defense in protecting their children from potentially objectionable content.[22] Luckily, the reverse appears to be true for computers. A 2006 Pew Internet & American Life Project survey of teenage media usage revealed that 74 percent of

[20] David Walsh, PhD, *No: Why Kids—of All Ages—Need to Hear It and Ways Parents Can Say It* (New York: Free Press, 2007), p. 269.

[21] *Generation M: Media in the Lives of 8-18 Year-Olds*, Kaiser Family Foundation, March 2005, p. 10, www.kff.org/entmedia/entmedia030905pkg.cfm

[22] "One of the most beneficial Nos is to keep TVs, video games, or computers out of kids' bedrooms. Sending your kid to her room isn't a punishment when she can catch up on her favorite shows or 'whatever else is on.' Once her door is closed, you don't know where your child goes on the Internet, what she is watching, or for how long. Keeping media out of the bedroom increases school performance and decreases the risk of obesity. Say yes to screens in a common space in the house. This may be a bit noisy, but it will help you keep track of your kids' screen time and virtual activities." Walsh, *op. cit.,* pp. 269-270.

homes with teenagers have their computers in an "open family area."[23] That result was consistent with Pew surveys taken in 2004 and 2000.

(2) **"When and How Much" Rules**: Parents can also limit the overall number of hours that children can consume various types of media content, or when they can do so. (Several technological tools mentioned in Part III can help parents accomplish this.) For example, parents can impose restrictions on the times of the day that children can consume media with rules like, "No TV or video games after 8:00 PM," or, more stringently, "No TV or games on a school night." The Pew Internet & American Life Project survey mentioned above found that 58 percent of parents limit the amount of time their children can spend watching television; 59 percent limit how much time their kids can play video games; and 69 percent limit how much time their children can spend online.[24]

(3) **"Under What Condition" Rules**: "When and how much" rules represent a carrot-and-stick approach to media consumption / exposure. Parents can incentivize their children by requiring that other tasks or responsibilities be accomplished before media consumption is permitted. For example, many of us are familiar with this very common household media rule: "You have to finish your homework before you get to watch any TV." Similar rules can be used for video games and other types of media. My mother effectively used a conditional media rule with me as a child when she rewarded weekly achievement in school by letting me pick out a comic book at a local pharmacy. On the weeks I didn't do so well in school, I didn't get my *Batman* or *Spiderman* fix!

More creatively, parents can formulate a "media allowance" for their children (especially as they get older) to allow them to generally consume the media they want but only within certain boundaries. Again, incentives can be used with this approach. For example, better grades at school might be rewarded by adding one more hour of media time to their overall weekly media allowance.

B. The Importance of a Good (Media) Diet: A Media Food Pyramid

The efforts described above represent commonsense approaches parents can use to establish basic ground rules about how media are consumed in the home. But what about the substance of the media that are being consumed within these preestablished boundaries? This might constitute a fourth category—"what" rules—that could be added to the list of informal household media rules listed earlier.

For example, a poll conducted by the group TV Watch in June 2007 found that 73 percent of parents monitor what their children watch, including 87 percent

[23] Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 8, www.pewinternet.org/PPF/r/211/report_display.asp

[24] *Ibid.*, p. 9.

of parents whose children are ages 0-10.[25] Similarly, according to the Pew Internet & American Life Project, 77 percent of parents already have rules for which TV shows their kids can watch, 67 percent have rules for the kinds of video games they can play, and 85 percent have rules about which Internet websites they can and cannot visit.[26]

How can parents do more to encourage their kids to consume media that they feel are appropriate and enriching? Although every family will have a different set of values and preferences, when it comes to media consumption, parents need to think about what constitutes a sensible "media diet" for their own families.[27] Toward that end, parents should consider taking a "food pyramid" approach to media consumption: Teach kids the importance of a balanced media diet while also teaching them the types of things that you think they should probably avoid altogether.

The federal government has a recommended food pyramid for nutritional purposes, of course. But just as government doesn't enforce the food pyramid through regulation, neither should it enforce a media food pyramid through mandates or restrictions. In fact, we don't need the government to tell us what is in a "media food pyramid" at all. This is something that parents can do quite effectively on their own, especially in light of the differing values each household will bring to the job.

Although every family will have a different set of values and preferences, when it comes to media consumption, parents need to think about what constitutes a sensible "media diet" for their own families.

A family's media food pyramid might have specific time allotments and recommended "portions" of different types of content. The American Academy of Pediatrics recommends no more than one or two hours of "screen time" per day,[28] but families might vary that depending on their desires and their children's ages. Once parents decide roughly how much media they will allow their children to consume, they can determine what are the best portions to be served.

Consider how this might work for television. In their recent book *The Elephant in the Living Room: Making Television Work for Your Kids*, Dimitri Christakis and Frederick Zimmerman, directors of the Child Health Institute at the University of Washington, offer parents numerous suggestions for how to make

---

[25] *TV Watch Survey of Parents*, Hart Research, June 2007, www.televisionwatch.org/junepollresults.pdf

[26] *Ibid.,* p. 9.

[27] The author wishes to thank Rich Lappenbusch of the Microsoft Corporation for inspiring and helping to develop this concept during a series of ongoing conversations in 2006-2007.

[28] "Television: How it Affects Children," American Academy of Pediatrics, www.aap.org/pubed/ZZZGF8VOQ7C.htm?&sub_cat=1

television viewing a more positive experience for everyone in the family.[29] They group TV programs into several categories and then encourage parents to use a mix of shows in each category to achieve a balanced media diet. Exhibit 2 outlines some of the programs they recommend to satisfy desired skills or values that most parents would find important.

Exhibit 2: Sample "Media Diet" of Children's Television Programming

Desired Skills / Values	Sample Programs
Literacy skills	*Sesame Street, Arthur, Between the Lions*
Math skills	*Sesame Street, Cyberchase*
Problem-solving skills	*Blue's Clues, Dora the Explorer, Go Diego Go*
Music and dance / physical activity	*The Wiggles, The Backyardigans, Animal Jam*
Imagination / creativity	*Mister Rogers' Neighborhood, Barney & Friends*
Pro-social skills	*Higglytown Heroes, Dragon Tales, Clifford*
Geography skills	*It's a Big Big World, Postcards from Buster*
Cultural diversity	*Dora the Explorer, Go Diego Go, Sesame Street*

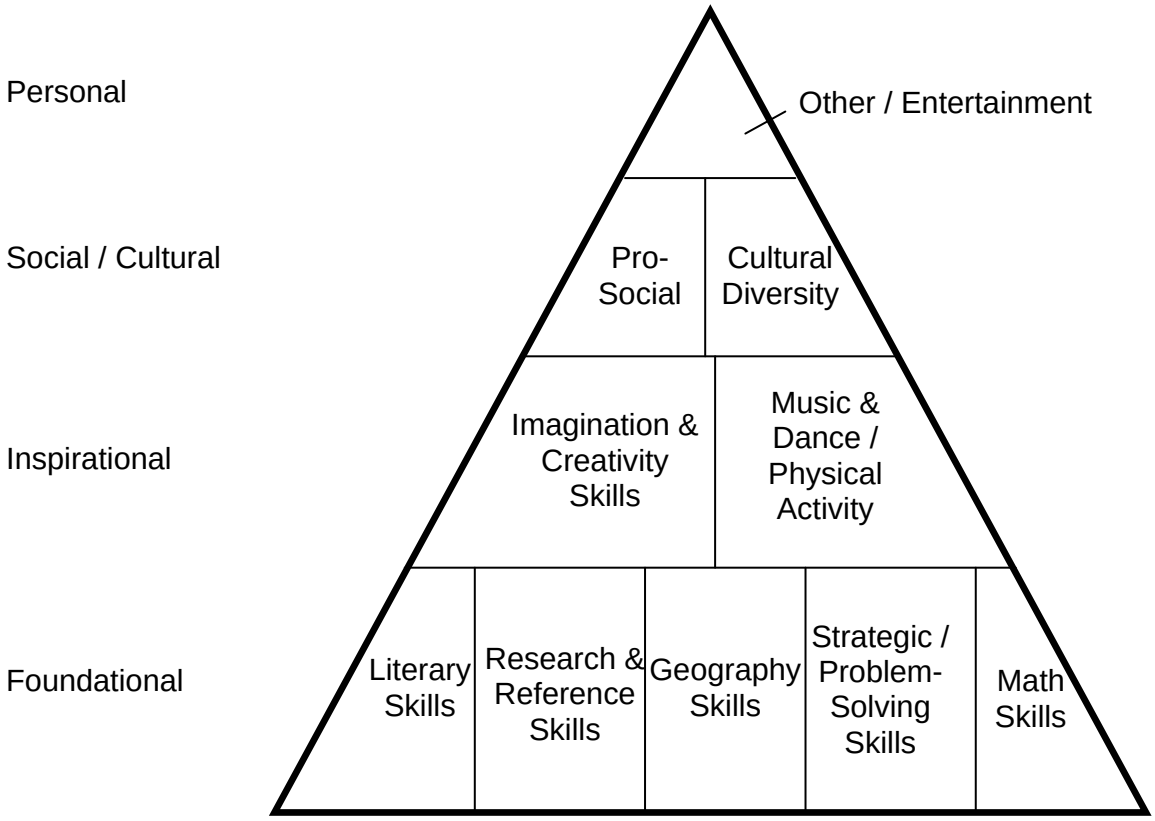
This approach works equally well for music, games, interactive software, websites and all types of media. They can be integrated into each family's media pyramid once parents decide the proper mix of skills and values. The resulting family food pyramid might look something like
Exhibit 3.

Again, every family will bring a different set of needs and values to this task. And the needs of children will vary by age. The proper media diet for a 5-year-old will be much different from that of 15-year-old. In other words, no two family media diets will be the same. Portion sizes from each category will likely differ. And the type of media content used in each category might be different for each family. For example, to instill geography skills in children, some families might rely heavily on interactive computer software, online encyclopedias, and various TV or DVD documentaries. On the other hand, some families might adopt the old-fashioned approach that my wife and I use in our home. We have a library filled with old maps, atlases, a globe, and a 40-year collection of *National Geographic* magazines that we use to teach geography to our kids.[30]

[29] Dimitri A. Christakis and Frederick J. Zimmerman, *The Elephant in the Living Room: Making Television Work for Your Kids* (New York: Rodale, 2006).

[30] We also have a map of United States glued to a piece of cardboard that we let our kids stick colored pins into it to highlight the cities they have visited.

Exhibit 3:
The Media Food Pyramid: The Importance of a Balanced (Media) Diet



The bottom line: While different families will always have different values and approaches, there is something to be said for a balanced diet when it comes to media consumption, just as is the case with child nutrition.

Finally, it should be stressed that not everything in a family's media diet must be completely educational in character. Sometimes parents and kids just want to relax and enjoy various types of entertainment, whatever they may be. A certain portion of every family's media diet, therefore, will be non-educational media content—and there's nothing wrong with that. For example, one can be thankful for the many lessons learned by watching *Sesame Street*, as I do, but still have fond memories of those old *Batman* or *Spiderman* cartoons and comic books that many boys like me enjoyed when we were growing up in the 1970s.

C. Teaching Good Etiquette in a Multimedia World

One of the most important parenting responsibilities involves teaching our children basic manners and rules of social etiquette. For example, we teach them proper dinner table manners, to cover their mouths when they cough or sneeze,

to hold doors open for others, or simply to say "thank you" when given something. When we become parents, no one from the government gives us a handbook instructing us to do all this. Rather, these are social conventions that come to us naturally, just as they did with our parents and the generations of parents that came before them.

These informal social rules of etiquette are essential to well-functioning civil society. And it is commonly understood that these are "rules" that families, communities, and other social groups or institutions are primarily responsible for instilling in children. Few would seriously argue that government should have a role in mandating proper etiquette in a free society.

Why should it be any different for media usage? It shouldn't. Proper online etiquette is a private responsibility, albeit one that is probably not taken as seriously as "offline" etiquette. Again, most parents repeatedly drill basic manners into their kids until it's clear that they "get it." Unfortunately, the same cannot be said for online manners. This might be the case because the Internet and digital communications technologies have taken the world by storm and caught the current generation of parents a bit off guard. Unaccustomed to using modern computing or communications devices, some parents may be neglecting their duties in terms of teaching good online etiquette. Of course, as the blue-ribbon panel of experts assembled by the National Academy of Sciences noted, "It may be that as today's children become parents themselves, their familiarity with rapid rates of technological change will reduce the knowledge gap between them and their children, and mitigate to some extent the consequences of the gap that remains."[31]

Unaccustomed to using modern computing or communications devices, some parents may be neglecting their duties in terms of teaching good online etiquette.

Nonetheless, here are a few lessons children need to be taught as they begin using interactive communications and computing technologies, including cell phones,[32] mobile media devices, interactive video games, instant messaging, social networking websites, blogs, and so on. To begin, kids need to be taught to assume that *everything* they do in the digital, online world could be archived *forever* and will be available to future employers, romantic interests,

[31] Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 49.

[32] The National Institute on Media and the Family produces an excellent guide for parents entitled "Cell Phones and Your Kids" that offers friendly pointers for parents looking to teach their children proper cell phone etiquette. See *A MediaWise Parent Guide—Cell Phones and Your Kids*, (Minneapolis, MN: National Institute on Media and the Family, 2006), www.mediafamily.org/network_pdf/cellphon_guide.pdf

their children and grandchildren, and so forth.[33] This admonition needs to be repeated frequently to remind minors that their online actions today could have profound consequences for them tomorrow. Beyond this warning, children need to be encouraged to follow some other sensible rules while using the Internet and other interactive technologies:

- ✓ **Treat others you meet online with the same respect that you would accord them in person;**
- ✓ **Do not cyber-bully or harass your peers;**
- ✓ **Do not post negative comments about your teachers or principals online;**
- ✓ **Do not post or share inappropriate pictures of yourself or others;**
- ✓ **Avoid talking to strangers online;**
- ✓ **Avoid using lewd or obscene language online or in communications;**
- ✓ **Do not share your personal information with unknown parties; and,**
- ✓ **Talk to parents and educators about serious online concerns and report dangerous situations or harassing communications to them.**

To better formalize such guidelines in the home, parents might want to ask their children to sign the "Family Netiquette Plan"[34] and the "Internet Respect Plan,"[35] documents that the National Institute on Media and the Family produces. The one-page "contracts" contain many of the listed guidelines and ask both parents and children to sign the formal household agreement pledging to abide by those rules. Parents can then devise penalties if their children break the rules. The National Institute on Media and the Family recommends the following punishment if the rules are violated: "If there are any violations to expected behaviors, there will be no Internet, TV, or video games for the following three days except for necessary school work."[36]

D. Third-Party Pressure, Ratings, and Advice

Parents can also work with others to influence media content before it comes into the home, or rely on other groups they trust to help them better understand what is in the media they are considering bringing into the home. Parents can pressure media providers and programmers directly through public

[33] "The biggest message that must be imparted to children and teens with respect to [their] privacy and the Internet is: *it's not private!!!* Anything and everything that is put into electronic form and sent or posted online is public or could easily be made public. Think before you post." Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), p. 92, [emphasis in original].

[34] www.mediafamily.org/pdf_files/Network_Family_Netiquette_Plan.pdf

[35] www.mediafamily.org/pdf_files/Network_Internet_Respect_Plan.pdf

[36] *Ibid.*

campaigns, or indirectly through advertisers.[37] Groups like the Parents Television Council, Morality in Media, Common Sense Media, and the National Institute on Media and the Family can play a constructive role in influencing content decisions through the pressure they can collectively bring to bear on media providers in the marketplace.

For example, Morality in Media's website outlines several strategies parents can use to influence advertisers, programming executives, and cable operators before resorting to calls for censorship. To allow parents to pressure advertisers, the group publishes a book listing the top 100 national advertisers, with addresses, phone and fax numbers, names of key executives, and their products, along with a products list cross-referenced to the manufacturer. The group produces a similar book that lists the names and addresses of the CEOs of the leading broadcast and cable companies in America so that viewers or listeners can complain directly to them.[38] Similarly, the Parents Television Council (PTC) awards its "seal of approval" to advertisers who only support programs that the PTC classifies as family-friendly.[39] PTC also encourages parents to send letters and e-mails to advertisers who support programming they find objectionable and encourage those advertisers to end their support of those shows.

Parents can also work with others to influence media content before it comes into the home, or rely on other groups they trust to help them better understand what is in the media they are considering bringing into the home.

Such efforts have been effective at changing corporate behavior in other contexts. For example, in late 2006 after years of pressure from various health groups and average parents, 10 major food and beverage companies announced new, self-imposed restrictions on advertising to children. These 10 companies, which included McDonald's, Coca-Cola, Pepsi, Kraft Foods, and Hershey, account for more than two-thirds of all food and beverage advertising aimed at children.[40] Among their commitments, they agreed to not advertise products in schools; devote half their advertising to promoting healthier lifestyles and foods; limit the use of popular third-party characters (such as cartoon characters) in

[37] "There is every reason to believe that the marketplace, speaking through advertisers, critics, and self-selection by viewers, provides an adequate substitute for Commission involvement in protecting children and adults from television's 'captive' quality." Mark S. Fowler and Daniel L. Brenner, "A Marketplace Approach to Broadcast Regulation," *Texas Law Review*, vol. 60, no. 2, February 1982, p. 229.

[38] Robert Peters, "The Importance of Making Complaints," Morality in Media website, available at www.moralityinmedia.org

[39] www.parentstv.org/PTC/awards/main.asp

[40] Betsy McKay and Janet Adamy, "Food Companies Vow to Tighten Limits on Kids' Ads," *Wall Street Journal*, November 15, 2006, p. B3.

their ads; and limit ads seen in interactive video games or promote healthy alternatives in those ads. The initiative will be monitored by the Council of Better Business Bureaus, which helped craft the agreement.

If public pressure can help change corporate attitudes and outputs when it comes to food and beverage advertising, there's every reason to believe that it can also change other types of media behavior. For example, in late 2006, intense public pressure forced News Corp. to abandon the publication of a controversial book by O.J. Simpson in which he described how he might have killed his ex-wife and her friend.[41] *Washington Post* columnist Shankar Vedantam argued that this episode "showed that shame remains a powerful tool in America."[42] Likewise, in April 2007, radio talk show host Don Imus had his CBS Radio show and MSNBC television program canceled after making offensive remarks about the Rutgers University women's basketball team.[43] Public outcry was so intense that almost all his largest advertisers pulled their support for his show less than a week after the incident occurred.[44]

Parents and other organizations might also be able to work together to pressure content providers or distributors to self-regulate materials that cannot be blocked with parental control technologies. For example, some parents feel that the in-flight movies shown on drop-down screens in airplanes contain sexual or violent themes unfit for some younger viewers. And there is no way for them to block the screen or turn off those videos. KidSafeFilms.org is a new group that pressures airline operators to take steps to further restrict or edit what is shown in the open cabin space since parents have no control over it.[45] Of course, eventually most airlines will have individual screens for each seat and parents will be able to control what is being viewed by their children. But the efforts of KidsSafeFilms.org might help speed up those efforts and get airlines to be more selective about the content they show on drop-down screens in the meantime. A similar effort might be useful in terms of discouraging advertising for potentially offensive content on television, or at least encouraging programmers to air such ads during later hours of the day.

Most parents, however, will not likely feel the need to pressure media producers directly but instead simply want better information about the media they bring into the home. Or they might feel comfortable getting independent

---

[41] Tim Harper, "O.J. Book, Fox Show Cancelled," *Toronto Star,* November 21, 2006.

[42] Shankar Vedantam, "Abandoned O.J. Project Shows Shame Still Packs a Punishing Punch," *Washington Post*, November 27, 2006, p. A2.

[43] Bill Carter and Jaques Steinberg, "CBS Drops Imus Radio Show over Racial Remark," *New York Times*, April 12, 2007, www.nytimes.com/2007/04/12/business/media/12cnd-imus.html?ex=1180756800&en=15850df43f6b8c51&ei=5070; Matthew Robinson, "U.S. Radio Host Imus Hints Career May Be Ending," *The Guardian*, April 12, 2007, http://sport.guardian.co.uk/breakingnews/feedstory/0,,-6552506,00.html

[44] Kenneth Li, "Here's Why MSNBC Dropped Imus," *Reuters*, April 11, 2007, http://blogs.reuters.com/2007/04/11/heres-why-msnbc-dropped-imus

[45] www.kidsafefilms.org

advice or third-party ratings about various types of media content. Help is out there. (Exhibit 4). For example:

- **Common Sense Media's** comprehensive website[46] allows both parents and children to rate a diverse assortment of media content and then sort it all by age group to find what is appropriate for their families.[47] The site also offers parental tips such as its "Managing Media: Downloads, Internet TV, and More" checklist, which helps parents manage their children's media consumption.[48]
- The National Institute on Media and the Family's **MediaWise** website offers occasional columns and newsletters for parents that include information they can use to make more informed judgments about the content their children consume.[49] In particular, the institute's website offers a free "KidsScore" system[50] that rates thousands of movies, TV shows, video games. All content is alphabetized and easy to search.
- Focus on the Family's *Plugged In* magazine and **Plugged In Online** website[51] are independent rating resources "designed to help equip parents, youth leaders, ministers and teens with the essential tools that will enable them to understand, navigate and impact the culture in which they live."[52] Because of the group's religious focus, its movie, television, and music reviews also probe the spiritual content found in some media titles.
- The **Parent Previews** website[53] reviews new movies, DVDs and video games on an easy-to-understand A-F grading systems. Four primary categories are graded (violence, sexual content, language and drug or alcohol use) to determine the title's overall grade.

Other creative, independent rating systems are on the market or being developed. For example, in March 2006, TiVo announced a partnership with the Parents Television Council, the Parents Choice Foundation and Common Sense Media to jointly develop TiVo KidZone. Using ratings and information created by those groups, KidZone will allow parents to filter and record only the content that parents deem appropriate for their children.[54] All these private, voluntary

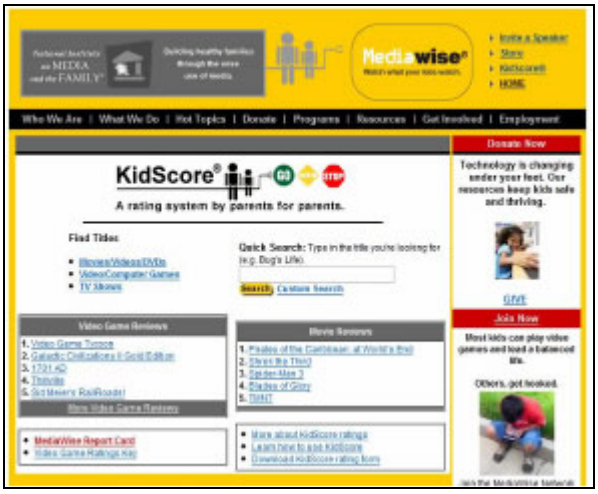
[46] www.commonsensemedia.org
[47] Joe Garofoli, "Media Guide Offers Reviews for Parents—But No Soapbox," *San Francisco Chronicle*, December 8, 2006, http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2006/12/08/MNG75MS23C1.DTL
[48] www.commonsensemedia.org/parent_tips/commonsense_view/index.php?id=232
[49] www.mediafamily.org
[50] www.mediafamily.org/kidscore
[51] www.pluggedinonline.com
[52] www.pluggedinonline.com/aboutUs/index.cfm
[53] http://movies.go.com/parentpreviews
[54] Saul Hansell, "TiVo to Offer Tighter Rein on Children's Viewing," *New York Times*, March 2, 2006, www.nytimes.com/2006/03/02/technology/02tivo.html?_r=1&oref=slogin

education and rating methods are preferable to the type of pressure that some groups bring to bear in the *political* marketplace when they encourage policymakers to regulate media content.[55]

Exhibit 4:
Independent Media Reviews and Rating Systems

Common Sense Media

Media Wise "KidScore"



Plugged In Online

Parents Preview

[55] See generally Adam Thierer, "Examining the FCC's Complaint-Driven Broadcast Indecency Enforcement Process," Progress & Freedom Foundation *Progress on Point* 12.22, November 2005, www.pff.org/issues-pubs/pops/pop12.22indecencyenforcement.pdf

Finally, there are several other excellent websites supported by media enterprises that offer parents excellent advice on media ratings and parental controls, such as: TV Watch,[56] The TV Boss.org,[57] Pause-Parent-Play,[58] Control Your TV.org,[59] Project Online Safety,[60] and Take Parental Control.org.[61] These efforts are discussed further in Parts III and IV, and some of them are highlighted in Exhibit 5.

Exhibit 5:
Industry Supported Efforts that Highlight Parental Controls

The TV Boss

Pause Parent Play

Project Online Safety

Take Parental Control

[56] www.televisionwatch.org
[57] www.thetvboss.org
[58] www.pauseparentplay.org
[59] www.controlyourtv.org
[60] www.projectonlinesafety.com
[61] http://takeparentalcontrol.org

E. The Ultimate Parental Control: The Power of the Purse

Finally, it is important that we not forget what, at times, constitutes the ultimate parental control tool: the "power of the purse." In most cases, when kids want to consume a certain type of media—or even consume something they see advertised in the media—they need money to do so. Televisions, movies, video games, cell phones, computers, and so on, do not just drop from high-tech heaven into our kids' laps![62] When kids want those things—or want things that are advertised on those media platforms—they must go to their parents and ask them for money. And, although at times it may be difficult, we all have the power to say "No."[63]

Parents can, and do, establish media budgets to better control what their kids see, hear, or play.[64] Many of the technologies discussed in Part III can facilitate this. Many new parental control tools incorporate sophisticated bill monitoring and spending control tools. For example, some TV set-top boxes, video game consoles, and most cell phones have tools that can limit media spending or at least give parents a clear report on how much money has been spent under their account. These tools can help parents enforce whatever media budget they establish for their children.

[62] Indeed, many of these technologies and types of media are out of the financial reach of most kids. Video games can cost $40-$60 per title. DVDs run between $10-$25. Cable subscriptions run at least $50 per month. While most websites are free, the computers and Internet connections needed to access them are not. Finally, most kids can't afford cell phones and monthly subscriptions, and they are not old enough to sign up for service anyway. So parents must be involved in all these media decisions.

[63] See David Walsh, PhD, *No: Why Kids—of All Ages—Need to Hear It and Ways Parents Can Say It* (New York: Free Press, 2007).

[64] See Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), pp. 8-9.

Informal Household Media Rules and Tips for Parents:

- ✓ *Always* be willing to sit down and talk to your kids about controversial and provocative media programming. Teach them the difference between fantasy and reality. Explain what is right or wrong from your perspective. And do it all in an open, understanding, and loving fashion.
- ✓ Strongly consider removing televisions, game consoles, computers, and other media devices from kids' bedrooms. Parents who allow their kids to lock themselves in their rooms with media technologies have surrendered their first line of defense.
- ✓ Establish household rules governing when and where children can watch TV, play video games, surf the Internet, and so on.
- ✓ Use third-party ratings or advice to help construct a balanced "media diet."
- ✓ Create carrot-and-stick incentives to encourage your kids to complete other important tasks before allowing media usage.
- ✓ Establish a media budget that limits how much kids are allowed to spend overall or on certain types of content, software, or devices.
- ✓ Teach children basic etiquette as they start to use more interactive media and technologies, such as cell phones, instant messaging, blogs, and social networking websites.
- ✓ Finally, remember that you were a kid once too! Teach your children what you've learned and teach them how to be smart media viewers and consumers. With a little guidance and common sense, they'll become savvy and discriminating media consumers just like you.

III. Ratings Systems and Technological Controls for Various Media

Part III of this report will explore the ratings, labeling systems, and technological controls that can help parents manage various media devices or different types of content. Although there is some overlap in the discussions about the various ratings and controls discussed, each major type of media content or platform—television, movies, music, wireless, video games, and Internet / computing—will be discussed separately.

But first a word of caution is in order. As mentioned at the outset, no rating system is perfect and no parental control tool is foolproof. Many critics are fond of pointing to supposed deficiencies in certain rating systems or technological controls and then attempt to use them to indict all voluntary ratings or private controls. But ratings and parental control tools need not be perfect to be preferable to government regulation.

Media rating and content-labeling efforts are not an exact science; they are fundamentally subjective exercises. Ratings are based on value judgments made by humans who all have somewhat different values.

Let's consider ratings first. What critics consistently forget—or perhaps intentionally ignore—is that media rating and content-labeling efforts are not an exact science; they are fundamentally subjective exercises. Ratings are based on value judgments made by humans who all have somewhat different values. Those doing the rating are being asked to evaluate artistic expression and assign labels to it that provide the rest of us with some rough proxies about what is in that particular piece of art, or what age group should (or should not) be consuming it. In a sense, therefore, all rating systems will be inherently "flawed" since humans have different perspectives and values that they will use to label or classify content.

Likewise, technological controls will always be hindered by certain inherent limitations. Technologies, markets, and artistic expression all evolve, and they do so at an increasingly rapid pace in our modern Information Age. Moreover, controls can be cracked or circumvented. There's always someone out there—including, all too often, our own children—who are looking to evade technological controls.[65]

[65] See Tom A. Peter, "Internet Filters Block Porn, But Not Savvy Kids," *Christian Science Monitor,* April 11, 2007, www.csmonitor.com/2007/0411/p13s02-lihc.htm

For these reasons, there will always be some critics who will argue that someone—presumably themselves or the government—can devise better ratings or controls. But, even setting aside the clear First Amendment concerns it would raise, there is no reason to believe that the government could actually do a better job.

There will always be some critics who will argue that someone—presumably themselves or the government—can devise better ratings or controls. But, even setting aside the clear First Amendment concerns it would raise, there is no reason to believe that the government could actually do a better job.

If the government were responsible for assigning content ratings or labels, for example, five unelected bureaucrats at the Federal Communications Commission or some other regulatory agency would simply substitute their own values for those of the voluntary rating boards or other labeling organizations in existence today. And the argument that government would provide more objective ratings or effective controls is also undermined by the grim reality of special-interest politics. Government officials would be more susceptible to various interest group pressures as they were repeatedly lobbied to change ratings or restrict content based on widely varying objectives and values. Inevitably, as has been the case with the broadcast indecency complaint process in recent years, a handful of particularly vociferous groups could gain undue influence over content decisions.[66] That possible outcome raises what the Supreme Court has referred to as the "heckler's veto" problem since a vocal minority's preferences could trump those of the public at large.[67]

With private, independent rating and labeling systems, by contrast, those assigning ratings or labels are intentionally isolated from lobbying or other interest group pressures. This it what makes the argument for "transparency" in rating systems so disingenuous, or even somewhat dangerous. If transparency means forcing raters to be exposed to endless special-interest lobbying or other pressures, one wonders if that would really produce a better system. It would likely produce a system that bowed to those pressures. For example, if those assigning video game ratings weren't anonymous, they might be harassed by both game developers (who want to make them more lax) and game critics (who want to make them more stringent).[68] This does not mean the raters ignore

[66] Adam Thierer, "Examining the FCC's Complaint-Driven Broadcast Indecency Enforcement Process," Progress & Freedom Foundation *Progress on Point* 12.22, November 2005, www.pff.org/issues-pubs/pops/pop12.22indecencyenforcement.pdf

[67] *Reno v. ACLU*, 521 U.S. 844, 880 (1997).

[68] Adam Thierer, "Can Government Improve Video Game Ratings?" Progress & Freedom Foundation *Blog*, October 26, 2006, http://blog.pff.org/archives/2006/10/can_government.html

public input. To the contrary, private rating boards and labeling bodies poll the public and monitor what critics are saying to adjust their ratings accordingly. But if the government forced their ratings systems to be open to all who cared to provide input (including the public policymakers themselves), it would result in a circus-like atmosphere and little content would get rated in a timely manner.

Similarly, there is no reason to believe that the government could construct more rigorous parental controls or screening technologies. Consider Internet filters, for example. Starting with the passage of the Communications Decency Act of 1996, there have been endless political debates about the efficacy of private filters relative to government content controls. Policymakers typically argue that regulation is needed because filters are not 100 percent effective in blocking pornography or other types of objectionable online content.

Instead of thinking of ratings and technological controls as absolute controls, it makes more sense to think of them as training wheels and speed bumps.

No doubt this point is true, but what of it? During a recent trial about the merits of the Child Online Protection Act (COPA) of 1998, the Department of Justice (DOJ) introduced evidence showing that major filters blocked sexually explicit content 87.4 to 98.6 percent of the time.[69] The DOJ seemed to suggest that this was not good enough, but would government regulation really produce a better track record than that? It's doubtful, especially because the government is largely powerless to control offshore activity. Private filters, by contrast, can capture objectionable offshore material. Private filters can also use industry standard identification systems to allow legitimate rated commercial content to be seen while screening out unknown or unrated content. And new methods are being developed and deployed to monitor and identify content, such as image-recognition technologies, which can further facilitate screening and filtering.

Moreover, it is reasonable to assume that a market of commercial filters and other technological controls will flourish if governments promote industry experimentation rather than impose a "one-size-fits-all" regulatory model. A marketplace of controls and filters can then develop that is more closely tailored to the diverse values of the citizenry. Government controls, by contrast, essentially treat all households as having the same core needs and values, which we know is not the case. Even though not all private filters will be equally effective, failure will be detected more rapidly and the better systems will gradually win out as all legitimate content is tagged and rated.

[69] *American Civil Liberties Union v. Gonzales*, No. 98-5591 (E.D. Pa. Mar. 22, 2007). For a breakdown of how successful various filters were, see http://www.aclu.org/freespeech/internet/27490res20061120.html

Again, as mentioned at the outset, instead of thinking of ratings and technological controls as absolute controls, it makes more sense to think of them as training wheels and speed bumps. If we want to make our kids slow down and be more cautious on today's "information highways," we can add more speed bumps and affix better training wheels on their bikes. But even with training wheels, kids will still fall off their bikes sometimes. And long after they learn how to ride without training wheels and have given up their bikes for cars, speed bumps can only slow them down so much; they won't stop them from speeding entirely.[70]

What do we do about it as parents and a society? We promote better industry-wide safety designs, we add layers of protection, and we try to educate our children about the dangers they face. When they're young and still riding bikes, we make them wear helmets, warn them of the dangers of traffic, and tell them to slow down. And when they become teenagers and get their first car, we make them wear their seat belts and avoid aggressive driving, and we still keep telling them to slow down! In sum, *we use the protections and safeguards at our disposal while educating them about safe and responsible use*.

This is the same mindset we need to adopt when it comes to parental controls and online child safety. The following sections illustrate how we can do so for every major media sector and technology.

A. Television

Television programming remains the focus of more public policy debates than any other type of media content. That is not surprising given the continued centrality of television as a mass medium and cultural phenomenon in our society. Even as consumption of other types of content increases, television still reigns as the king of the media hill. Luckily, numerous tools and methods exist to restrict potentially objectionable television programming from entering the home and help parents tailor the video programming their children see on their media devices.

The V-Chip and TV Ratings

As a standard feature in all televisions 13 inches and larger built after January 2000, the V-Chip gives households the ability to screen televised content by ratings that are affixed to almost all programs.[71] The V-Chip can be accessed through the setup menus on televisions, or is often just one click away using a designated button on the TV's remote. Households can then use

[70] Nancy E. Williard, author of Cyber-Safe Kids, Cyber-Savvy Teens, argues that "Placing significant reliance on parental controls may end up backfiring, because such reliance often leads to false security. … The biggest problem with the promotion of protection technologies is that these technologies will never be totally effective." Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), p. 31, 33-4.

password-protected blocking to filter programs by rating. The rating system, available online at www.tvguidelines.org/ratings.asp, offers seven age-based designations:

Exhibit 6: TV Ratings

TV Y	**All Children**
TV Y7	**Directed to Children Age 7 and Older**
TV Y7 FV	**Directed to Older Children Due to Fantasy Violence**
TV G	**General Audience**
TV PG	**Parental Guidance Suggested**
TV 14	**Parents Strongly Cautioned**
TV MA	**Mature Audience Only**

The TV rating system also uses several content descriptors to better inform parents and all viewers of the nature of the content they will be experiencing. (Exhibit 7)

[71] It is important to realize that most video consumed on televisions today is not from traditional broadcast stations. New video distribution sources such as cable, satellite, DVD, HD-DVD, Blu-Ray, and IPTV all inherit a social norm and cultural responsibility to allow parents controls that are easy to set once and enforce everywhere.

Exhibit 7: TV Content Descriptors[72]

D	Suggestive Dialogue
L	Coarse Language
S	Sexual Situations
V	Violence
FV	Fantasy Violence

These age-based ratings and content descriptors appear in the upper left hand corner of the screen at the start of each television program. If the program is more than one hour, the icon will reappear at the beginning of the second hour. (For some programs, the ratings appear during every commercial break). The ratings and descriptors also appear on the TV's on-screen menus and interactive guides, on the TV networks' websites, and in local newspaper or *TV Guide* listings. This information is also encoded and embedded into each TV program so that the V-Chip or other devices can screen and filter by ratings.

The Federal Communications Commission also hosts a website that provides detailed instruction on how to use the V-Chip.[73] "TV Watch," a coalition of media experts and media organizations, provides a website with tutorials and tool kits to help parents program the V-Chip and find other tools to control television in the home.[74] And a new industry sponsored campaign entitled "The TV Boss" (www.thetvboss.org) offers easy-to-understand tutorials explaining how to program the V-Chip or cable and satellite set-top box controls. (Exhibit 8). As part of the effort, several public service announcements (PSAs) and other advertisements have aired or been published reminding parents that these capabilities are at their disposal.

[72] The meaning of the content descriptors varies depending on the age-based rating to which they are attached. For example, "L" means "infrequent coarse language" when attached to a TV-PG rating and "strong, coarse language" when attached to a TV-14 rating. See www.tvguidelines.org/ratings.asp

[73] www.fcc.gov/vchip

[74] www.televisionwatch.org

Exhibit 8:
"TheTVBoss.org" Website

Importantly, the relatively low V-Chip usage rates among U.S. households should not be used as an excuse for government regulation of television programming. Some polls or surveys of V-Chip and parental control usage unfairly include *all* households in the sample group, which means they are including in their results the millions of households without children in them, and thus have no incentive to use the V-Chip or any parental control technologies.[75] Again, according to the U.S. Census Bureau, almost 68 percent of American homes do *not* have any children under 18 years of age in residence.[76] Therefore, it doesn't make sense to survey all homes about V-Chip or parental control usage because adult-only homes almost certainly would not be using any parental controls to block programming. That would be like polling all Americans, including homes made up of only adults, about whether they used baby locks on their kitchen cabinets!

It is also important to keep in mind that even those homes with children in residence will not all need to use parental control technologies before a certain age (4-5) or after a certain age (15-16). That is because many parents do not let their kids watch much TV before they reach a certain age and then later, after

[75] Adam Thierer, "Distorting Numbers in the Debate over Parental Controls," Progress & Freedom Foundation *Blog*, March 26, 2007, http://blog.pff.org/archives/2007/03/distorting_numb.html

[76] U.S. Census Bureau, *2007 Statistical Abstract of the United States*, Table No. 57, p. 52, available at www.census.gov/prod/2006pubs/07statab/pop.pdf

they reach a certain age, the parents just trust their kids or talk to them about objectionable fare.

Moreover, as discussed below, the vast majority of American homes now rely on many alternative technologies and methods to filter or block unwanted programming. Many families will forgo V-Chip capabilities in light of the alternative technological controls at their disposal, or even the informal household rules that they have established in their homes, as was outlined in Part II. A November 2005 survey by the polling firm Russell Research revealed that twice as many parents frequently use the parental controls that offered by their cable and satellite providers as use the V-Chip controls built into their television sets.[77] In other words, the V-Chip is just one of many tools or strategies that households can use to control television programming in their homes.

Cable and Satellite TV Controls

With roughly 86 percent of U.S. households subscribing to cable or satellite television systems,[78] the tools that multichannel video providers (cable, satellite and telephone companies) offer to subscribers are a vital part of the parental controls mix today. Parental controls are usually just one button-click away on most cable and satellite remote controls and boxes.

It doesn't make sense to survey all homes about V-Chip or parental control usage because adult-only homes almost certainly would not be using any parental controls to block programming.

Both analog and digital boxes allow parents to block individual channels and lock them with passwords so that children can't access them. Newer, digital boxes offer more extensive filtering capabilities that allow programs to be blocked by rating, channel, or title. Some systems even allow users to block the program descriptions on the interactive guide (for adult pay-per-view programming, for example) if families don't want them to be visible.

Those cable subscribers without digital set-top boxes can request that cable companies take steps to block specific channels for them. A comprehensive survey of the content controls that cable television providers make available to their subscribers can be found on the National Cable and

[77] "Survey: Parents Combine Old-Fashioned TV Rules and Latest Blocking Technologies to Manage Kids' TV," TV Watch *Press Release*, November 28, 2005, www.televisionwatch.org/NewsPolls/PressReleases/PR008.html

[78] Federal Communications Commission, *Twelfth Annual Video Competition Report*, February 10, 2006, p. 118, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-06-11A1.pdf

Telecommunications Association's (NCTA) "Control Your TV" website.[79] (Exhibit 9).

Exhibit 9:
NCTA's "ControlYourTV.org" Website

Aftermarket solutions are also available that allow parents to block channels. The "TV Channel Blocker" gives households the ability to block any analog cable channel between channels 2 and 86, including broadcast stations carried by the cable operator.[80] Homeowners themselves can install the unit on the wall where the cable line enters the home. It can then block specific channels on any television in the home. The unit sells online for $99.99.

Satellite providers DirecTV[81] and EchoStar's Dish Network[82] also offer extensive parental control tools via their set-top boxes. And telephone companies

[79] http://controlyourtv.org
[80] www.tvchannelblocker.com
[81] www.directv.com/DTVAPP/global/contentPage.jsp?assetId=900007 and www.directv.com/DTVAPP/equipment/demoInfo.jsp?assetId=1100093
[82] www.dishnetworkproducts.com/products/parental_controls.php

such as AT&T and Verizon are also getting into the video distribution business and offering similar tools. Many of the same set-top boxes deployed by the cable industry are used by these telco providers. Therefore, the parental control capabilities are quite similar. (Incidentally, as the blending of the Internet and television continues with the rise of Internet protocol-based television delivery, there will be increased pressure for industry to rally around clear international standards for content identification and independent ratings. This should ensure that still more content gets rated / labeled.)

Some multichannel operators also offer subscribers the option of buying a bundle of "family-friendly" channels. For example, Dish Network offers a "Family Pak"[83] and DirecTV offers a "Family Choice" bundle of channels.[84] Many cable operators offer similar bundles, but parents must consult their local provider to get details since packages vary by zip code or county.[85] Major cable operators such as Comcast,[86] Time Warner,[87] Cox,[88] Insight Communications,[89] Mid-Continent,[90] and Bright House[91] all offer family packages. Also, a unique satellite service called Sky Angel offers 33 channels of what it describes as "Christ-centered and family-friendly choice(s)" that households can subscribe to if they want only religious programming available in their homes.[92]

Other Video Devices and Technological Control Measures

One of the most important developments on the parental controls front in recent years has been the rapid rise and diffusion of VCRs, DVD players, personal video recorders (PVRs) and home computers. These technologies give parents the ability to accumulate libraries of preferred programming for their children and determine exactly when it will be viewed. This can help parents tailor programming to their specific needs and values.[93] If certain parents believed that their children should only be raised solely on reruns of *The Lone Ranger* and *Leave it to Beaver*, then these new media technologies can make it happen!

To use a personal example: My wife and I have developed a strategy of designating a specific television in our home for most of our children's media consumption and then using a PVR to amass a large library of programming we

---

[83] www.dishnetworkproducts.com/packages.php
[84] www.directv.com/DTVAPP/packProg/channelChart1.jsp?assetId=1000005
[85] A good example from my home county of Fairfax, Virginia, is the Family Package that Cox Communications offers. See www.cox.com/fairfax/cable/familyservice.asp
[86] www.comcast.com/customers/faq/FaqCategory.ashx?CatId=356
[87] www.timewarnercable.com/corporate/programming/familychoice.html
[88] www.cox.com/fairfax/cable/familyservice.asp
[89] www.insight-com.com/documents/Insight_01172006.pdf
[90] www.midcocomm.com/ResidentialServices/DigitalCable/DigitalFamilyTier/
[91] http://cfl.mybrighthouse.com/products_and_pricing/digital_cable/familypack.aspx
[92] www.skyangel.com
[93] "[PVRs] are quickly revolutionizing the way families watch television, with easy-to-use-systems and a convinence that every family can appreciate." Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), p. 172.

believe is educational, enriching and appropriate for them. Dozens of programs can be cataloged and archived in this fashion and then supplemented with VHS tapes, DVDs and computer software. As a result, when we allow our children some TV time, we always know that the episodes of *Dora the Explorer, Go Diego Go, Blue's Clues* and *The Wiggles* that we approve of for our kids will be available. Needless to say, such content tailoring was not an option for families in the past.

Incidentally, to find such family-friendly fare, parents can search for it using set-top box controls or retrieve information about such shows from various Internet web services such as TV Guide.com's "Family TV Hot List."[94] The TV Guide.com site allows parents to search an online guide of all the programming televised by their local broadcasters or multichannel video providers, where they can examine program ratings and information. This too can help parents tailor programming in the home to their exact needs and values.

One of the most exciting things about the modern parental controls market-place is that families have the ability to better tailor media programming to their particular needs or values.

But for those families that want to block out televised programming aired during certain hours of the day or limit how much TV can be viewed at all, technological tools exist that can make that possible. The Family Safe Media website sells a half dozen "TV time management" tools that allow parents to restrict the time of day or aggregate number of hours that children watch programming.[95] Most of these devices, such as the Bob TV Timer by Hopscotch Technology[96] and the TV Allowance television time manager,[97] feature PIN-activated security methods and tamper-proof lock boxes that make it impossible for children to unplug or reset the device. Parents can use these devices to establish a daily or weekly "allowance" of TV or game screen time and then let children determine how to allocate it. Prices for these devices range from $39.95 to $110.95. Similarly, "credit-based" devices such as the Play Limit box require children to place time tokens in a metallic lockbox to determine how much TV or game time is allowed.[98] Parents can provide a certain allowance of tokens to restrict the overall amount of screen time.

[94] www.tvguide.com/Find-Shows-Movies/TV/Family/HotList
[95] www.familysafemedia.com/tv_time_management_tools_-_par.html
[96] www.hopscotchtechnology.com
[97] www.tvallowance.com
[98] www.playlimit.com

Exhibit 10: The "Weemote"

Another innovative technology to restrict children's viewing options by children is the appropriately named the Weemote. It is a remote control made for children that has only a handful of large buttons. Parents can program each button to call up only those preset channels that they approve of for their children. No other channels can be accessed using the remote. The product has a suggested retail price of $24.95.[99]

For those families looking to take more direct steps to specifically curb potentially offensive language heard on some televised programs, solutions are available. For example, over seven million Americans currently use TVGuardian systems, which bill themselves as "The Foul Language Filter." TVGuardian's set-top boxes filter out profanity by monitoring the closed-caption signal embedded in the video signal and comparing each word against a dictionary of more than 150 offensive words and phrases. If the device finds a profanity in this broadcast, it temporarily mutes the audio signal and displays a less controversial rewording of the dialog in a closed-captioned box at the bottom of the screen.[100] The device can also be tailored to individual family preferences to edit out references that some might consider religiously offensive.

TV for Kids / Content-Tailoring Options

As stressed from the outset, one of the most exciting things about the modern parental controls marketplace is that families have the ability to better tailor media programming to their particular needs or values. Instead of merely focusing on restricting content, more families are now focusing on encouraging their children to watch enriching programming. Although it just scratches the surface of what is available, Exhibit 11 highlights some of the child- and family-friendly television options for parents today. And this list does not include the many excellent instructional or educational videos available on VHS or DVD that parents can use to supplement or even supplant regular television viewing.

[99] www.weemote.com
[100] www.tvguardian.com

Exhibit 11: Educational / Entertainment Viewing Options for Children

- **ABC Family Channel** (http://abcfamily.go.com)
- **Animal Planet** (http://animal.discovery.com)
- **Discovery Channel** (www.discovery.com)
- **Discovery Kids** (http://kids.discovery.com)
- **Disney Channel** (www.disney.go.com/disneychannel)
- **Familyland Television Network** (www.familyland.org/content/Content.aspx?CategoryID=51)
- **Hallmark Channel** (www.hallmarkchannel.com)
- **Hallmark Movie Channel** (www.hallmarkmoviechannel.com)
- **HBO Family** (www.hbofamily.com)
- **History Channel** (www.history.com)
- **Learning Channel** (http://tlc.discovery.com)
- **National Geographic Channel** (http://channel.nationalgeographic.com/channel)
- **Nickelodeon** (www.nick.com)
- **Noggin** (www.noggin.com)
- **N Channel** (www.the-n.com)
- **PBS** (www.pbs.org)
- **PBS Kids** (http://pbskids.org/go)
- **Science Channel** (http://science.discovery.com)
- **Showtime Family Zone**
- **Sprout** (www.sproutonline.com)
- **Starz! Kids and Family** (http://www.starz.com/appmanager/seg/s?_nfpb=true&_pageLabel=starz_kids_family)
- **Toon Disney** (http://psc.disney.go.com/abcnetworks/toondisney)
- **Varsity World** (www.varsityworld.com)

Independent Television Rating Organizations

Finally, if parents wish to independently verify official TV ratings, or just get more information about the content of specific shows, many services are available:

- **Common Sense Media's** user-friendly website offers detailed TV reviews as well as user-generated reviews submitted by both parents and kids themselves.[101] The site offers extremely detailed descriptions of almost every possible type of content that one might find in a given show.

- **Plugged In Online's** website, a project of the religious group Focus on the Family, reviews many TV shows and as part of its review process considers the following elements: positive elements, spiritual content, sexual content, violent content, crude or profane language, drug and alcohol content, and other negative components.[102]

[101] www.commonsensemedia.org/tv-reviews
[102] www.pluggedinonline.com/tv/index.cfm

- The **Parents Television Council's** ParentsTV website offers a searchable "Family Guide to Prime Time Television"[103] and awards a seal of approval to shows that it deems suitable for families.[104]

***Television Tips for Parents**:*

- ✓ Program the V-Chip in your televisions or the parental controls embedded in your cable or satellite set-top boxes to block potentially objectionable programming.
- ✓ Use VCRs, DVD players, and personal video recorders (PVRs) to better control your family's viewing habits.
- ✓ Familiarize yourself with TV ratings (www.tvguidelines.org/ratings.asp) and also consult Common Sense Media (www.commonsensemedia.org) and other independent review sites to learn what others think about various TV programs.
- ✓ Instead of placing televisions in bedrooms and allowing your children to watch shows unsupervised, consider placing the sets in a common area of the home so that you can keep can keep an eye (and ear) on the programming they are viewing.
- ✓ Consider establishing household rules limiting the aggregate amount of time (on a daily or weekly basis) that children can spend watching television. Also, provide carrot-and-stick incentives for kids to use media sensibly.

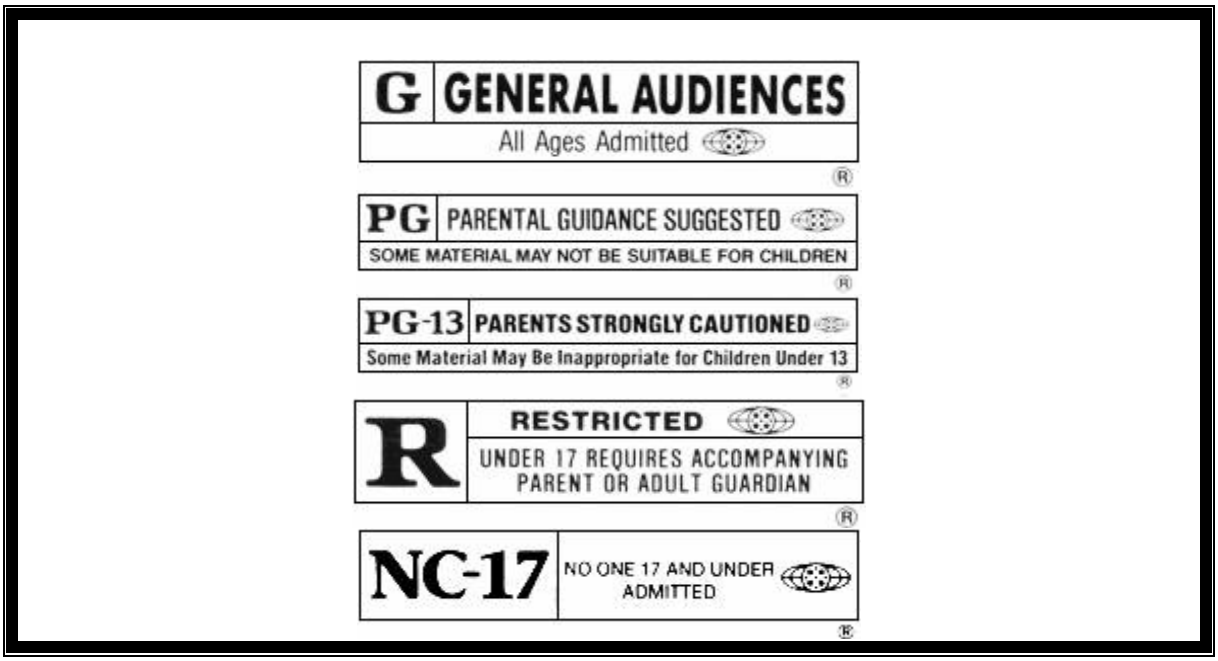
B. Movies

The MPAA Movie Rating System

The motion picture industry has the longest-running and most widely recognized rating system in America. Established by the Motion Picture Association of America (MPAA) and theater operators in 1968, the MPAA's familiar rating system includes the age-based designations shown in Exhibit 12.

[103] www.parentstv.org/PTC/familyguide/main.asp
[104] www.parentstv.org/PTC/awards/main.asp

Exhibit 12: The MPAA Movie Rating System

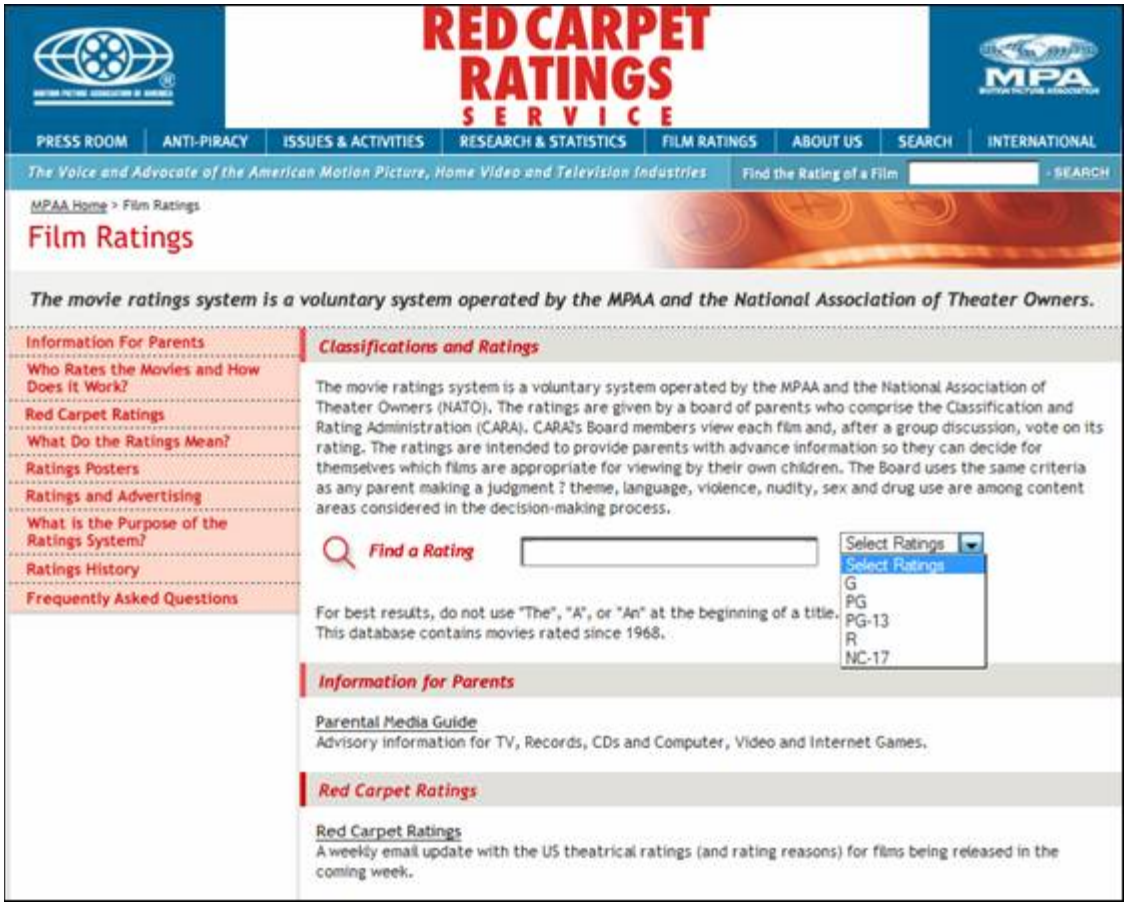


These ratings are accompanied by additional content descriptors explaining what viewers can expect to see in the movie. Both the ratings and content descriptors appear at the beginning of all movies—whether seen at a cinema or on VHS or DVD. When movies are sold on DVDs, the MPAA rating information is embedded on the discs in the form of machine-readable "metadata." DVD players, gaming consoles, and other devices that can play DVDs can then read the ratings via the embedded metadata. That allows parents to block movies of a certain rating from playing on those devices.

The MPAA also requires that the ratings appear on all promotional advertising (posters, TV ads, etc.). Finally, the MPAA's website also features a search engine that allows the public to look for any movie it has rated since 1968 and find its rating and a description of the content.[105] The MPAA also recently introduced the "Red Carpet Ratings Service," which allows parents to sign up to receive a weekly report of the ratings of recently premiered movies.[106] (Exhibit 13). In addition, the MPAA has also been involved in a variety of cross-industry educational efforts that will be summarized in Part IV.

[105] www.mpaa.org/FilmRatings.asp or www.filmratings.com
[106] www.mpaa.org/FlmRat_RedCarpet.asp

Exhibit 13:
MPAA's "Red Carpet Ratings" Service



Independent Movie-Rating Organizations

As was the case with TV programs, if parents wish to verify MPAA movie ratings independently, or just get more information about the content of specific movies, there are many services to which they can turn:

- **Common Sense Media's** user-friendly website offers detailed movie reviews as well as user-generated reviews submitted by both parents and kids themselves.[107] The site offers extremely detailed descriptions of almost every possible type of content that one might find in a given title.

- The **Parent Previews** website reviews new theatrical releases and DVDs according to an easy-to-understand A-F grading system.[108] Four primary categories are graded (violence, sexual content, language, and drug or alcohol use) to determine the movie's overall grade.

[107] www.commonsensemedia.org/movie-reviews
[108] http://movies.go.com/parentpreviews

- **Kids-in-Mind** is another online rating service that assigns films three distinct, category-specific ratings: one for sex and nudity, one for violence and gore, and another for profanity. Each review provides highly detailed listings of instances of those categories within a film. Each movie's rating is on a scale of 0 to 10, depending on the quantity and context of what is shown. The site's reviews also cover other themes that parents might want to discuss with their children, such as substance abuse, divorce, or the occult.[109]

- **ScreenIt.com** is an online subscription-based movie review service ($24.95 per year) for parents looking for extremely detailed summaries of the content found in movies.[110] It evaluates each movie title using 15 different criteria.

- **Plugged In Online's** website, a project of the religious group Focus on the Family, reviews many movies and DVDs and as part of its review process considers the following elements: positive elements, spiritual content, sexual content, violent content, crude or profane language, drug and alcohol content, and other negative components.[111]

- The **Parents Television Council's** ParentsTV website offers recent movie reviews[112] and awards a seal of approval to movies that its deems suitable for families.[113]

- **Yahoo.com's Movie Mom** movie page includes reviews by Nell Minnow, author of *The Movie Mom's Guide to Family Movies*. [114]

- The **Coalition for Quality Children's Media** is a national, not-for-profit organization founded in 1991 that seeks to teach children critical viewing skills and increase the visibility and availability of what it regards at quality children's programming. On its KidsFirst website, it offers critical reviews of movies and other forms of children's entertainment and provides a searchable database of recommended titles by age group.[115] It also sponsors a film and video festival dedicated to "promoting excellence in children's films and engaging children as film critics, curators and filmmakers."[116]

---

[109] www.kids-in-mind.com
[110] www.screenit.com
[111] www.pluggedinonline.com
[112] www.parentstv.org/PTC/publications/moviereviews/main.asp
[113] www.parentstv.org/PTC/awards/main.asp
[114] www.movies.yahoo.com/mv/moviemom
[115] www.kidsfirst.org/kidsfirst
[116] www.kidsfirst.org/kidsfirst/fabout.htm

- Finally, some of the best information about what parents can expect to see and hear in movies comes from other parents who review them on sites like **Amazon.com**,[117] **Netflix.com**,[118] **Metacritic.com**,[119] and the **Internet Movie Database**.[120] Indeed, most movies listed on these sites contain hundreds of user-generated reviews that typically make it very clear what the movie contains and at what approximate age it is appropriate for viewing. Unofficial sources such as The Internet Movie Database also lists major ratings that each movie has received by ratings organizations worldwide.

Independent Movie Screening Tools

ClearPlay produces a unique DVD player that eliminates profanity, violence and nudity from certain movies.[121] ClearPlay doesn't produce preedited DVDs, rather, the company "create[s] filtering information on a movie by movie basis, and then put[s] those 'filters' into the DVD player. By doing so the DVD player knows when to skip or mute while the movie is playing."[122] Therefore, consumers don't have to purchase special DVDs; they just need to purchase a ClearPlay DVD player and download the codes for their movies to activate the filtering controls. The company's current MaxPlay DVD player retails for $99.00 and comes loaded with the filters for about 1,000 popular movies. A monthly membership fee of $7.95 is required to access new movie filtering codes.

ClearPlay's technology raised some copyright concerns and was opposed by many movie directors and studios. But in 2005, Congress passed and President George W. Bush signed the Family Movie Act, which exempted services like ClearPlay from any copyright liability.[123] However, other types of preedited DVD software service—"scrubbed" DVDs—were ruled copyright violations by a U.S. district court judge in 2006 and are no longer available.[124]

***Movie Tips for Parents**:*

✓ For movies seen within the home, follow the same guidelines outlined earlier for general television viewing. Program the V-Chip, cable or satellite set-top boxes, and PC and video game console parental controls to block potentially objectionable movies from being seen (especially pay-per-view titles).

[117] www.amazon.com
[118] www.netflix.com
[119] www.metacritic.com
[120] www.imdb.com
[121] www.clearplay.com
[122] www.clearplay.com/about.aspx
[123] The Family Movie Act was part of the Family Entertainment and Copyright Act of 2005. President Bush signed the measure into law on April 27, 2005.
[124] Keith Regan, "Court Says Editing DVDs for Content Is Illegal," *E-Commerce News*, July 10, 2006, www.ecommercetimes.com/story/51667.html

✓	Use VCRs, DVD players and personal video recorders to ensure that your children see only the movies you think are appropriate for them at a certain age. Build a library of your favorite material.
✓	Familiarize yourself with MPAA ratings (www.mpaa.org/FilmRatings.asp) and also consult the many independent websites listed earlier to learn what other groups or parents think of the movies your kids want to see.
✓	Again, keep TVs and other movie-playing devices out of kids' bedrooms and in a common area of the home so that you can keep an eye on what they are viewing.

C. Music and Radio

Album Ratings

Since the mid-1980s, the music industry (working with retailers) has administered a voluntary parental advisory labeling program to give parents fair warning that a particular album might contain explicit lyrics about sex, violence, or drug use. The Recording Industry Association of America (RIAA) runs the program on behalf of record companies and producers who, working with their artists, decide which of their songs and products receive the explicit label.[125] If they determine that a warning is appropriate, the industry's widely recognized black-and-white "Parental Advisory – Explicit Content" label is affixed prominently to the outside of the permanent packaging and embedded in the digitally delivered files. (Exhibit 14). They also have an option to release a "non-explicit" version of the same song or product with the appropriate modifications.

Exhibit 14:
The RIAA's Explicit Content Parental Advisory Label

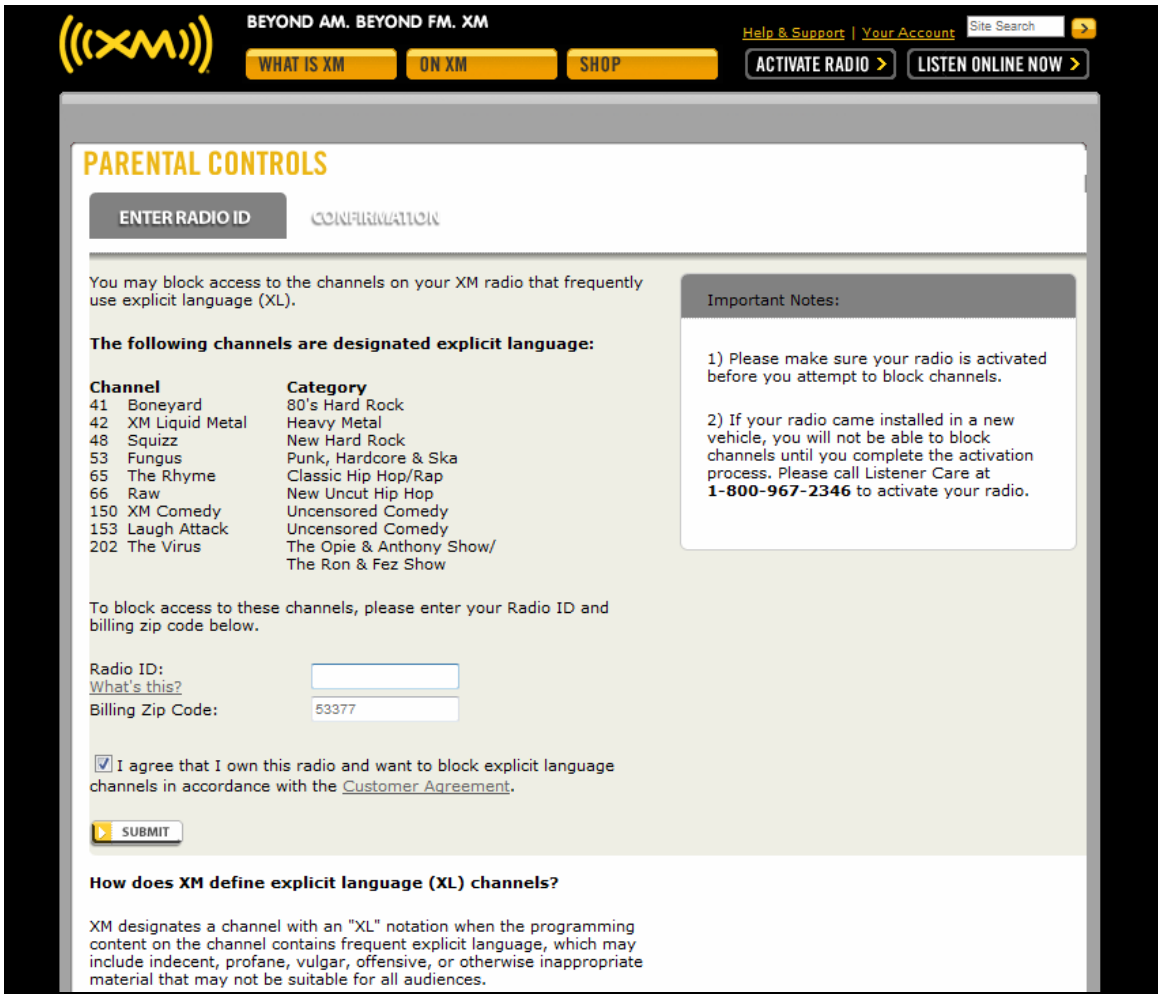
Retailers also prominently display the warnings regardless of how they choose to offer the products for sale; retail or digital. Many retailers have long-established procurement guidelines and refuse to sell "Explicit" labeled products to those younger than 18. Other retailers, such as Wal-Mart, refuse to carry such albums at all.

[125] www.riaa.com/issues/parents/advisory.asp

Satellite Radio Controls

Satellite radio operators XM and SIRIUS offer some blocking tools for their music services. XM labels eight of its channels with an "XL" tag to designate that some shows or music on those channels might contain explicit lyrics. When subscribers scroll through the stations on their player, the "XL" label will be visible next to those stations. Subscribers can then program their XM receivers to block those channels automatically. (Exhibit 15). According to the XM website: "XM designates a channel with an 'XL' notation when the programming content on the channel contains frequent explicit language, which may include indecent, profane, vulgar, offensive, or otherwise inappropriate material that may not be suitable for all audiences."[126]

Exhibit 15:
XM Satellite Radio Parental Controls



[126] www.xmradio.com/parentalcontrols/index.jsp?refsrc=hp_ex

Although SIRIUS does not label its stations in the same fashion, SIRIUS radio receivers have the capability to lock, password-protect, and hide channels that subscribers do not want to access or have their children stumble upon.[127]

Apple iPod and Microsoft Zune Parental Controls

Not every portable music player on the market today offers embedded parental control capabilities, but two major competitors in this space—Apple and Microsoft—do offer some controls and have standing commitments to improve these capabilities over time by working together with the music industry in standards-settings organizations.

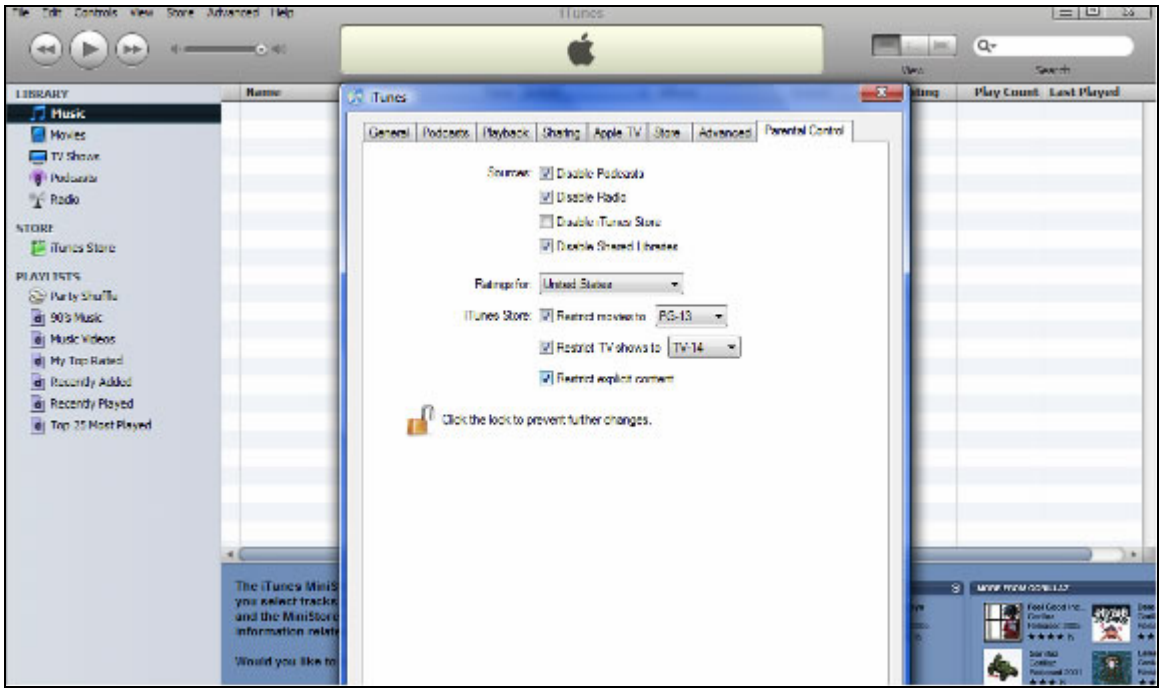
Apple's wildly successful iPod is by far the most popular portable music player on the market today. Once users purchase an iPod, they also download iTunes software onto computers to transfer music onto their player or buy material online at Apple's iTunes Store.[128] At the iTunes Store, users can purchase songs and videos or download free online radio stations or podcasts. Music singles containing explicit lyrics have a bold red "EXPLICIT" label next to song title. Movies are clearly labeled with MPAA movie ratings and other content descriptors making it clear what type of content can be found in the title.

Parents can find parental controls in the iTunes software on the main menu under "Edit / Preferences / Parental Controls." (Exhibit 16) Once there, they can disable all podcasts, online radio and music sharing, or they can just disable access to the iTunes Store altogether. Less drastically, if they want to make the iTunes Store accessible but limit what can be downloaded, they can designate the level of movie and TV ratings that are appropriate for their children and nothing rated above that level will be accessible. And parents can restrict the downloading of any music that contains the "EXPLICIT" label on the site. Once appropriate settings are determined, parents can lock the software to prevent further changes.

[127] http://buy.sirius.com/resources/faq.html#programming. Also see http://siriuscanada.ca/_ProductLocking-e.htm

[128] www.apple.com/itunes/store

Exhibit 16:
Apple iTunes Parental Controls



Microsoft's Zune portable media player also offers family settings that allow parents to control what their children can download from the Zune Marketplace website. According to the Zune website, before a child can create an online Zune account he or she must have parental consent:

> When your child first signs up online for Zune, they enter (or you enter for them) their own Windows Live ID and account information, and then Zune asks for parental permission to continue creating the account. You give parental permission by using or creating a master Windows Live ID and entering some credit card information to verify that you are an adult. (The credit card is not charged.)[129]

Parents can also establish their own family settings when creating an account for their children. Specifically, parents determine whether to allow their kids to purchase premium content or explicit content on the Zune Marketplace website. Like the iTunes Store, Microsoft's Zune Marketplace contains some material marked as "explicit" and allows parents to block such material from being downloaded by their children. Parents can alter the settings at any time by going to the main menu and clicking "Account Management / Family Settings."

Importantly, new music industry product identification solutions are developing that will facilitate parental control technologies in the future. For

[129] www.zune.net/en-us/support/howto/marketplace/familysettings.htm

example, the Global Release Identifier (GRID) is the recording industry's new product identification system that encourages those in the industry to embed product metadata in their digital music files.[130] And the Digital Data Exchange (DDEX) is the music industry's system for reporting and tracking these new digital music IDs.[131]

GRID and DDEX are primarily used by music companies, device manufacturers, service providers, and technology implementers to track sales, gauge royalties, and monitor piracy. But embedded metadata can also include digital content labels and rating information that can facilitate screening capabilities. For example, on its Zune webpage, Microsoft outlines the type of metadata labels that content creators can include in their digital files that can then be read by the Zune.[132] Parental ratings—for music, movies, and television—are among the metadata labels that Microsoft recommends. As these metadata labeling efforts expand, other consumer electronic device makers will also be able to include parental controls in their products that can read media labels and ratings. This will make it easier for parents to restrict potentially objectionable or age-inappropriate content on music players or other mobile media devices.

Independent Rating Organizations

Once again, as is the case with TV, movies, and video games, parents who want more information about the music their kids might want can use independent websites for their research. The **Common Sense Media**[133] website provides detailed music reviews and details what parents can expect their kids to hear in the music they buy. Similarly, **Plugged In Online**[134] focuses on the "pro-social content" versus "objectionable content" found on each album it reviews. And user-generated reviews on sites like **Amazon.com**[135] and **Metacritic.com**[136] feature excellent product summaries that can help parents decide if various music titles are right for their kids. Finally, if parents want to examine the lyrics of the songs their children are listening to, they can find them at sites such as **Lyrics.com**[137] and **LyricsMania.com**.[138]

---

130 www.ifpi.org/content/section_resources/grid.html
131 www.ddex.net/index.htm
132 www.zune.net/en-us/support/howto/start/providecontent.htm#section7
133 www.commonsensemedia.org/music-reviews
134 www.pluggedinonline.com/music
135 www.amazon.com
136 www.metacritic.com
137 www.lyrics.com
138 www.lyricsmania.com

***Music Tips for Parents**:*

- ✓ Look for "Explicit Lyrics" labels on music and determine the best course of action for such music purchases. Consider "Clean Lyrics" versions for younger children.
- ✓ Use parental controls embedded in digital music services to block music downloads with objectionable lyrics.
- ✓ Consult independent rating websites (such as Common Sense Media.org and Plugged In Online.com) to learn what other parents think about music that you are considering buying for your kids or that your children are already listening to.
- ✓ Check out the lyrics in the songs your kids are listening to by visiting websites such as Lyrics.com or LyricsMania.com.

D. Video Games

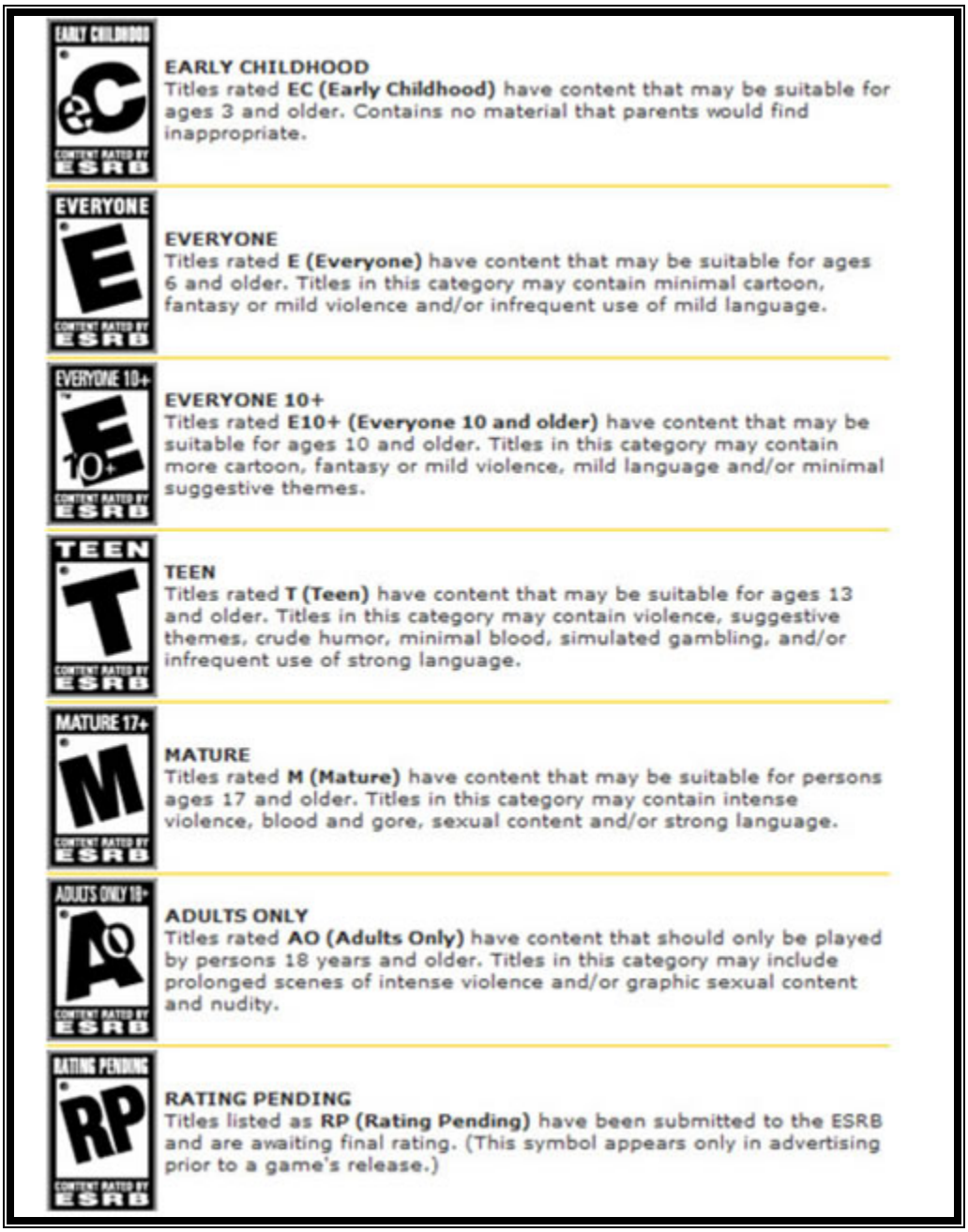
The ESRB Rating System

Although it is the newest of all industry content rating and labeling schemes, the video game industry's system is in many ways the most sophisticated, descriptive, and effective ratings system ever devised by any major media sector in America. Established by the video game industry in 1994, the Entertainment Software Rating Board (ESRB) is a self-regulatory rating and labeling body.

The ESRB rating scheme is remarkably comprehensive. According to the ESRB, it rates over 1,000 games per year. Virtually every title produced by major game developers for retail sale today carries an ESRB rating and content descriptors. Generally speaking, the only games without ESRB ratings today are those developed by web amateurs that are freely traded or downloaded via the Internet. The ESRB applies seven different rating symbols to the games it rates. Exhibit 17 describes these ratings.

In addition to designating these ratings, the ESRB has over 30 different content "descriptors" (Exhibit 18) that it uses to give consumers highly detailed information about games. Thus, by simply glancing at the back of each game container, parents can quickly gauge the appropriateness of the title for their children. If parents want to do additional research in advance of a purchase, the ESRB's website allows them to enter the name of any game and retrieve its rating and various content descriptors.

Exhibit 17: ESRB Video Game Ratings System[139]



EARLY CHILDHOOD
Titles rated **EC (Early Childhood)** have content that may be suitable for ages 3 and older. Contains no material that parents would find inappropriate.

EVERYONE
Titles rated **E (Everyone)** have content that may be suitable for ages 6 and older. Titles in this category may contain minimal cartoon, fantasy or mild violence and/or infrequent use of mild language.

EVERYONE 10+
Titles rated **E10+ (Everyone 10 and older)** have content that may be suitable for ages 10 and older. Titles in this category may contain more cartoon, fantasy or mild violence, mild language and/or minimal suggestive themes.

TEEN
Titles rated **T (Teen)** have content that may be suitable for ages 13 and older. Titles in this category may contain violence, suggestive themes, crude humor, minimal blood, simulated gambling, and/or infrequent use of strong language.

MATURE
Titles rated **M (Mature)** have content that may be suitable for persons ages 17 and older. Titles in this category may contain intense violence, blood and gore, sexual content and/or strong language.

ADULTS ONLY
Titles rated **AO (Adults Only)** have content that should only be played by persons 18 years and older. Titles in this category may include prolonged scenes of intense violence and/or graphic sexual content and nudity.

RATING PENDING
Titles listed as **RP (Rating Pending)** have been submitted to the ESRB and are awaiting final rating. (This symbol appears only in advertising prior to a game's release.)

[139] www.esrb.org/ratings/ratings_guide.jsp

Exhibit 18: ESRB Content Descriptors

- **Alcohol Reference** - Reference to and/or images of alcoholic beverages
- **Animated Blood** - Discolored and/or unrealistic depictions of blood
- **Blood** - Depictions of blood
- **Blood and Gore** - Depictions of blood or the mutilation of body parts
- **Cartoon Violence** - Violent actions involving cartoon-like situations and characters. May include violence where a character is unharmed after the action has been inflicted
- **Comic Mischief** - Depictions or dialogue involving slapstick or suggestive humor
- **Crude Humor** - Depictions or dialogue involving vulgar antics, including “bathroom” humor
- **Drug Reference** - Reference to and/or images of illegal drugs
- **Edutainment** - Content of product provides user with specific skills development or reinforcement learning within an entertainment setting. Skill development is an integral part of product
- **Fantasy Violence** - Violent actions of a fantasy nature, involving human or non-human characters in situations easily distinguishable from real life
- **Informational** - Overall content of product contains data, facts, resource information, reference materials or instructional text
- **Intense Violence** - Graphic and realistic-looking depictions of physical conflict. May involve extreme and/or realistic blood, gore, weapons, and depictions of human injury and death
- **Language** - Mild to moderate use of profanity
- **Lyrics** - Mild references to profanity, sexuality, violence, alcohol, or drug use in music
- **Mature Humor** - Depictions or dialogue involving "adult" humor, including sexual references
- **Mild Violence** - Mild scenes depicting characters in unsafe and/or violent situations
- **Nudity** - Graphic or prolonged depictions of nudity
- **Partial Nudity** - Brief and/or mild depictions of nudity
- **Real Gambling** - Player can gamble, including betting or wagering real cash or currency
- **Sexual Themes** - Mild to moderate sexual references and/or depictions. May include partial nudity
- **Sexual Violence** - Depictions of rape or other violent sexual acts
- **Simulated Gambling** - Player can gamble without betting or wagering real cash or currency
- **Some Adult Assistance May Be Needed** - Intended for very young ages
- **Strong Language** - Explicit and/or frequent use of profanity
- **Strong Lyrics** - Explicit and/or frequent references to profanity, sex, violence, alcohol, or drug use in music
- **Strong Sexual Content** - Graphic references to and/or depictions of sexual behavior, possibly including nudity
- **Suggestive Themes** - Mild provocative references or materials
- **Tobacco Reference** - Reference to and/or images of tobacco products
- **Use of Drugs** - The consumption or use of illegal drugs
- **Use of Alcohol** - The consumption of alcoholic beverages
- **Use of Tobacco** - The consumption of tobacco products
- **Violence** - Scenes involving aggressive conflict

Source: Entertainment Software Rating Board

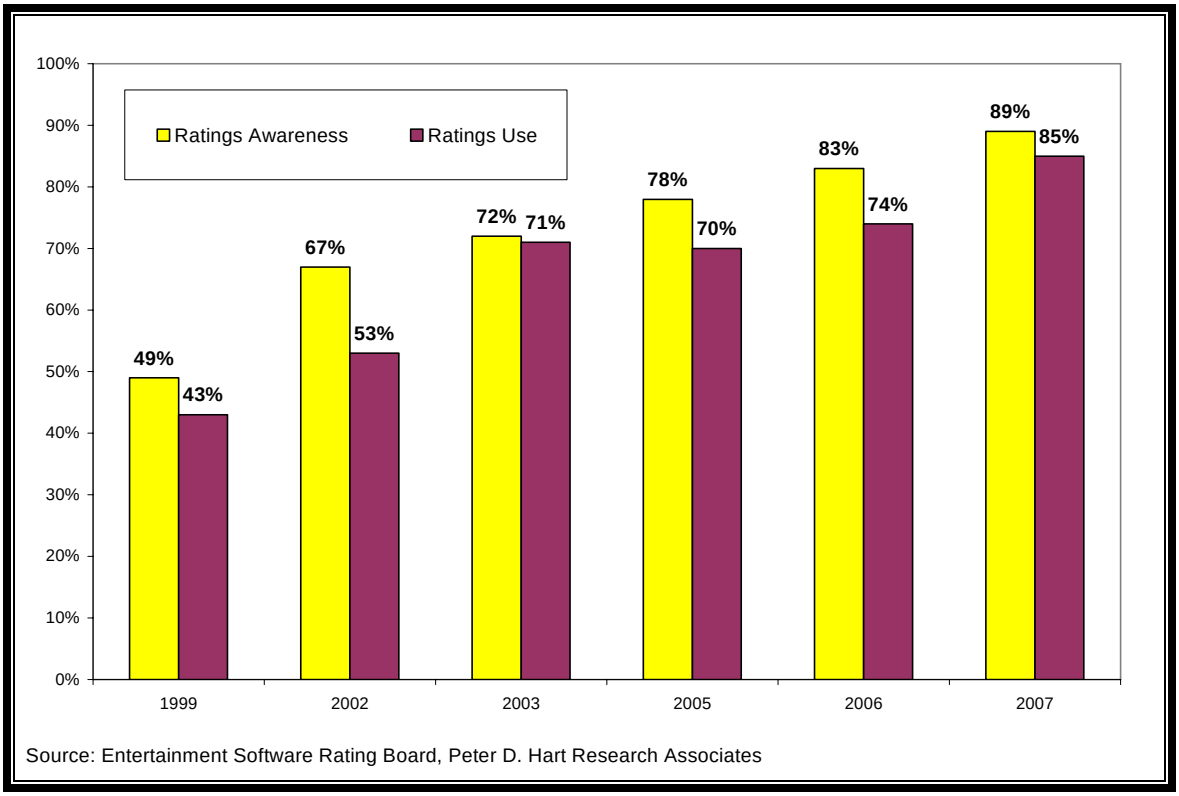
To ensure that its system is enforced properly under all cross-platform scenarios, the console manufacturers require that the rating is digitally available in the metadata or product description so the console or PC can identify and screen the content in advance.

Surveys have shown that most parents find the ratings and labels very helpful. Studies by Peter D. Hart Research Associates reveal that:[140]

- 89% of American parents of children who play video games are aware of the ESRB ratings;
- 85% consult the ratings regularly when buying games for their families; and,
- 90% say the ratings are very to somewhat helpful in buying or renting games for their kids.

As Exhibit 19 illustrates, these results have been increasing steadily since Hart Research Associates began conducting these surveys for the ESRB in 1999.

Exhibit 19: ESRB Ratings: Parental Awareness & Use



Source: Entertainment Software Rating Board, Peter D. Hart Research Associates

[140] "Parents Increasingly Using ESRB Ratings to Restrict the Video Games Their Children Play," Entertainment Software Rating Board *Press Release,* May 4, 2007, www.esrb.org/about/news/downloads/ESRB_AwarenessUsePR_5.4.07.pdf

Importantly, surveys have also shown a high level of parental involvement when games are purchased or rented. According to other Hart Research surveys, the average age of a video game purchaser is 40, and 89 percent of the time parents are present when games are purchased or rented.[141] Of parents surveyed, 80 percent also say that they play video games with their children.[142]

Exhibit 20:
ESRB Ratings Ads and Brochures

The ESRB also operates the Advertising Review Council (ARC) that promotes and monitors advertising and marketing practices in the gaming industry. The ARC monitors compliance with ESRB guidelines and places restrictions on how game developers may market ESRB-rated games through its "Principles for Responsible Advertising" and "Advertising Code of Conduct."

As part of its "OK to Play?" education campaign, the ESRB provides a variety of materials to retailers. The materials include an ESRB employee training

[141] *Essential Facts about the Computer and Video Game Industry: 2006 Sales, Demographics and Usage Data,* Entertainment Software Association, 2005, p. 3, 6, www.theesa.com/archives/files/Essential%20Facts%202006.pdf
[142] *Ibid.,* p. 7.

manual and quiz about the rating system. According to the ESRB, the "OK to Play?" signage is displayed at 17 top national retailers who account for approximately 90 percent of all game sales. Prominent retailers involved in the effort include Wal-Mart, Best Buy, Target, Toys-R-Us, and EB Games among others. These retailers, which are responsible for a significant portion of all video game sales, have enormous reputational incentives to abide by the ESRB rating system. Importantly, the in-store signage used by these and other game retailers is also reproduced as consumer advertising in various magazines, newspapers, websites, and so on. (Exhibit 20).

The video game industry's system is in many ways the most sophisticated, descriptive, and effective ratings system ever devised by any major media sector in America.

Finally, as will be noted in a subsequent section on education efforts, in November 2006 the ESRB announced an educational partnership with the Parent-Teacher Association (PTA) to "encourage and enable state and local PTAs to educate their community's parents about the [ESRB] ratings."[143] As part of this new education campaign, 1.3 million brochures will be distributed to 26,000 PTAs nationwide in both English and Spanish. Additional online support and education is offered on both the ESRB and PTA websites. The ESRB has also cosponsored several TV PSAs that were supported by legislators such as Senators Hillary Clinton and Joe Lieberman,[144] and state attorneys general Mark Shurtleff of Utah and Thurbert Baker of Georgia. In these TV spots, public officials encourage parents to use the video game ratings when buying games for their children.

Console Blocking Controls

Parents have another line of defense once video games are brought into their homes. Major game console developers (Microsoft,[145] Sony,[146] and Nintendo[147]) all recognize the digitally embedded ratings and offer blocking tools in their new gaming systems.[148] For example, the Microsoft Xbox 360 (Exhibit 21) and the Nintendo Wii consoles allow parents to enter the ESRB rating level that they believe is acceptable for their children. Once they do so, no game rated

[143] "PTA and ESRB Launch Nationwide Video Game Ratings Educational Partnership," Parent Teacher Association *Press Release*, November 15, 2006, www.pta.org/ne_press_release_detail_1163547309281.html

[144] "Senators Hillary Rodham Clinton and Joe Lieberman Join ESRB to Launch Nationwide Video Game Ratings TV PSA Campaign," Entertainment Software Rating Board *Press Release,* December 7, 2006, www.esrb.org/about/news/12072006.jsp

[145] www.xbox.com/en-US/support/familysettings/xbox360/familysettings-intro.htm

[146] Instructions for how to do so on the PlayStation3 can be found under the "Parental Controls" tab at: www.us.playstation.com/content/sites/176/info/frame_hardware.html

[147] www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

[148] See generally Mike Musgrove, "A Computer Game's Quiet Little Extra: Parental Control Software," *Washington Post*, December 23, 2006, p. D1, www.washingtonpost.com/wp-dyn/content/article/2006/12/22/AR2006122201278.html

above that level can be played on the console. All ESRB-rated games contain embedded metadata "flags," or a string of code in the software, that allow the consoles to automatically recognize the game's rating. (Personal computers using the new Microsoft Windows Vista operating platform have the same screening capabilities as these stand-alone gaming consoles.)[149]

Exhibit 21:
Microsoft Xbox Parental Control Set-Up Menus

Thus, parents could set the rating threshold on their child's video game console or personal computer to T for Teen and then no games rated Mature (M) or Adults Only (AO) could be played on the console unless the parent first enters

[149] This system works cross-platform because the game industry has reached a consensus on how to embed ratings information in a standard way. Film, music, and television industries are considering similar methods for their commercial products.

a password. (These controls can also be used to block movie playback according to the MPAA ratings.)

Sony's PlayStation 3 console and PlayStation Portable (PSP) handheld gaming system work a little differently. Both Sony gaming products let parents use a 1-11 scale to determine the level of game and DVD content they will allow their kids to play. The lower the level, the tighter the restriction.

A Word about Online, Multiplayer Gaming

Online gaming and what are referred to as "massively multiplayer online games" or "MMOG" are the hottest thing in the gaming world today. A user must have an Internet connection—usually a high-speed broadband connection—to interact in these online environments. Once they are connected, players can interact with countless other gamers, some of whom will be friends, but many will be strangers.

This fact will obviously raise some concern for some parents. While the ESRB can rate game content for traditional, individual game play, it cannot rate or perfectly describe how the gaming experience might change while online since game play is spontaneously shaped by multiple participants. This is why many online games sold today include an additional warning to parents that reads, "Game Experience May Change During Online Play." This makes it clear that user-generated content or online social interaction cannot be rated by the ESRB.

Parents have a couple of options at their disposal. First, they can disable online gaming capabilities altogether by either (a) not connecting the gaming console to an Internet connection or (b) using the controls embedded in new gaming consoles to disable or limit online connections. This approach is particularly sensible if parents allow their children to start gaming at a young age.

Second, parents can allow limited online gaming but demand that their children play with only known, trusted acquaintances. This process can be automated in the new Microsoft Xbox,[150] (Exhibit 22) Sony PS3[151] and Nintendo Wii[152] gaming consoles by restricting access to the child's friends list or gamer profile. In other words, parents can build the equivalent of a "buddies list" for their kids and allow them to play with only those other children. Alternatively, the systems enable parents to allow online gaming but restrict the chat capabilities so others cannot talk to their children. Incidentally, parents can also view a list of whom their children have been playing by examining the list of other gamers with whom they have interacted during online sessions. And parents can also limit

[150] Instructions for how to do so on the Xbox 360 can be found at: www.xbox.com/en-US/support/familysettings/console/xbox360/consolefamilysettings.htm

[151] Instructions for how to do so on the PlayStation3 can be found under "Creating an Account" and "Going Through the Registration Process" at: www.us.playstation.com/content/sites/176/info/frame_network.html

[152] www.nintendo.com/consumer/systems/wii/en_na/settingsParentalControls.jsp

how much children can spend in online "marketplaces" and set the limit to zero if they do not want their kids buying any online content. Integrated Internet browser capabilities can also be turned off entirely.

Exhibit 22:
Microsoft Xbox Communications Blocking Controls

Third, as their children get older and are allowed more interactive gaming, parents should ask them to report any suspicious communications from strangers in these games. Parents can report such behavior to online gaming operators who will take appropriate steps if undesirable activities are detected.

Independent Video Game Rating Organizations

As was the case with TV, movie and music ratings, if parents wish to verify ESRB game ratings independently, or just want more information about what their kids might see or hear in the games they buy them, several services are at their disposal. The **Common Sense Media**,[153] **Parent Previews**,[154] **Family Media Guide**,[155] and **MediaWise "KidScore"**[156] websites provide extremely

[153] www.commonsensemedia.org/game-reviews. In May 2007, electronic retailing giant Best Buy announced that, in addition to ESRB ratings, it would begin using Common Sense Media's ratings in its stores and online to provide parents with more information about the games their kids desire. See: Carissa Wyant, "Best Buy Launches Video Game Rating System for Parents," *Minneapolis / St. Paul Business Journal,* May 16, 2007, http://twincities.bizjournals.com/twincities/stories/2007/05/14/daily19.html

[154] www.parentpreviews.com/html/games.shtml

[155] www.familymediaguide.com/media/videogames.html

detailed video game reviews and information about the specific types of content that kids will see or hear in a game. And user-generated reviews on sites like **Amazon.com**[157] and **Metacritic.com**[158] feature excellent product summaries, often written by other parents, which can help parents decide if games are right for their kids.

Video Game Tips for Parents:

- ✓ When purchasing video games for your children, carefully review the ratings and content descriptors on the back of each box to determine if the game is acceptable for your family.
- ✓ If games are purchased online, first consult the ESRB website (www.esrb.org) to learn more about those games.
- ✓ Consult the independent ratings websites listed earlier to learn what other parents think about video games that you are considering buying for your kids.
- ✓ As soon as a new gaming console is brought into the home and unpacked, program the parental controls to designate the level of game (and movie) ratings that is acceptable within your household.
- ✓ Instead of placing gaming consoles in bedrooms and allowing your children to play unsupervised, consider placing the consoles in a common area of the home so that you can keep can keep an eye (and ear) on the content of the games that your kids are playing.
- ✓ When you see or hear objectionable content in certain games, talk to your kids about it.

E. Wireless and Mobile Media

Cell phones and other handheld mobile media devices have taken the world by storm. According to CTIA, the wireless industry's trade association, there were almost 240 million cellular telephone subscribers in America by the summer of 2007.[159] This is an astonishing number considering that few of us carried mobile devices in our pockets just 10 years ago. Today, however, even young children have their own cell phones.

[156] www.mediafamily.org/kidscore/chart.asp?MediaType=games&place=0. MediaWise also produces an annual report card about the video game industry and video game ratings: www.mediafamily.org/research/vgrc_index.shtml
[157] www.amazon.com
[158] www.metacritic.com
[159] www.ctia.org

Importantly, cell phones are becoming much more than just communication devices; they are now full-fledged multimedia platforms capable of delivering video, data, games, instant messages, and more.[160] Subscribers can use these devices to access news, information and entertainment from almost anywhere. Of course, this otherwise wonderful development has some downsides for parents who are concerned about the types of inappropriate content their children might be able to access on mobile devices.

Wireless Carrier Guidelines

The wireless industry is responding to this concern in a preemptive fashion. In November 2005, CTIA unveiled new "Wireless Content Guidelines" that industry members would follow "to proactively provide tools and controls to manage wireless content offered by the carriers or available via Internet-enabled wireless devices."[161] Under the guidelines, wireless carriers pledged not to offer any adult-oriented content until they have created controls to allow parents to restrict access.[162]

Cell phones are now full-fledged multimedia platforms capable of delivering video, data, games, instant messages, and more.

The guidelines propose the creation of a Content Classification Standard, which will divide mobile content into two categories: (a) "Generally Accessible Carrier Content" and (b) "Restricted Carrier Content." Ratings will then be developed using familiar categories and criteria employed by existing movie, television, music and games rating systems; and then tools will be developed to "ensure carrier-offered content either excludes or requires parent or guardian permission to access any material inappropriate for subscribers under 18."[163] Under the second phase of the plan, wireless carriers will implement Internet Content Access Control technologies to let consumers block access to the Internet entirely or block access to specific websites that they might find inappropriate.[164]

---

[160] "[T]he devices we call 'mobile phones' are, in fact, PCs. They're just another computer form factor. Some PCs are desktops. Some are laptops. And some are handhelds." Sascha Segan, "Think of Cell Phones Like Miniature PCs," *PC Magazine*, June 26, 2007, p. 80, www.pcmag.com/article2/0,1895,2139510,00.asp .

[161] "Wireless Carriers Announce 'Wireless Content Guidelines,'" CTIA *Press Release,* November 8, 2005, www.ctia.org/news_media/press/body.cfm?record_id=1565

[162] See Amol Sharma, "Wireless Carriers Set Strict Decency Standards for Content," *Wall Street Journal,* April 27, 2006, p. B1.

[163] Ibid.

[164] The complete guidelines can be found at http://www.ctia.org/consumer_info/service/index.cfm/AID/10394 and the classification criteria for "Restricted Carrier Content" can be found at http://www.ctia.org/content/index.cfm/AID/10395

Many major carriers have already announced their plans or policies regarding such content or developed family tools to help parents protect their children.[165] Market leaders AT&T ("Media Net"),[166] Verizon Wireless: ("Chaperone Service"),[167] and Sprint[168] already have excellent parental control services and websites up and running.

CTIA has also developed an awareness campaign called "Get Wise about Wireless," which "helps educate students about cell phone use and the responsible behaviors associated with using cell phones."[169] The program includes a variety of materials such as a teacher's guide and a family take-home pamphlet about safe and courteous cell phone use.[170] As part of this effort, CTIA also runs a student essay contest about sensible wireless use.[171]

Devices Geared toward Younger Users

In addition to the parental controls and screening services offered by carriers, wireless handsets geared specifically for younger children are now on the market.[172] These systems give parents considerable control over what their kids can access on their phones, as well as several other useful monitoring features.[173] For example:

- **Firefly Mobile** sells a tiny, voice-only phone for kids with just five buttons on it.[174] Two of the buttons have small icons symbolizing Mom and Dad, allowing the child to call them directly via pre-programmed numbers. It comes in several colors and contains a variety of accessories geared toward kids.

- Another such phone called the **TicTalk**[175] is marketed by wireless company Enfora and the educational toy maker LeapFrog Enterprises. The TicTalk lets parents enter phone numbers that can be called anytime and also restrict numbers that can be called only during certain times of

---

[165] See Tom Spring, "Web-Enabled Handsets Deliver a Squeaky-Clean Internet," *PC World*, June 20, 2006, http://pcworld.about.com/news/Jun202006id126147.htm

[166] www.wireless.att.com/learn/articles-resources/parental-controls.jsp

[167] www.verizonwireless.com/b2c/splash/chaperone/splash.jsp

[168] www1.sprintpcs.com/explore/ueContent.jsp?scTopic=parentalControl

[169] www.wirelessfoundation.org/GetWise/index.cfm

[170] See www.wirelessfoundation.org/GetWise/teachers_guide2007.pdf and www.wirelessfoundation.org/GetWise/family_takehome2007.pdf

[171] www.wirelessfoundation.org/GetWise/contest.cfm

[172] Many of these phones are discussed and sold at www.kidswireless.com

[173] For more information, see Dan Costa, "Yes, I Spy on My Kid," *PC Magazine,* July 17, 2007, p. 58, www.pcmag.com/article2/0,1895,2145504,00.asp; Yuki Noguchi, "Connecting with Kids, Wirelessly," *Washington Post*, July 7, 2005, p. A1; Fern Shen, "Only a Few Can Hear You Now: Limited-Use Phones Geared to Kids," *Washington Post*, July 18, 2005, p. C14; David Pogue, "Cellphones That Track Kids," *New York Times*, December 21, 2006, www.nytimes.com/2006/12/21/technology/21pogue.html?ex=1167973200&en=898b8ec6c58ef344&ei=5070;

[174] www.fireflymobile.com

[175] www.mytictalk.com/LeapFrog

the day. Parents can also determine what times during the day the phone can even ring.[176]

- In the summer of 2006, The Walt Disney Co. and Sprint Corp. announced a new wireless phone service tailored to youngsters.[177] The **Disney Mobile** cell phone lets parents set talking and spending limits and also limit text messaging and photographs.[178] The Disney phone includes global positioning system (GPS) technology that allows parents to locate their children and monitor their whereabouts via an Internet website or another Disney phone. And parents can send out "family alerts" to instantly communicate with several family members at once. The service also offers a great deal of Disney programming that kids can download.

- The **Wherify "Wherifone"** offers robust GPS location tracking via the Internet. Phone numbers can be programmed by parents and the phone contains an SOS panic button for emergencies. The Wherifone also restricts the downloading of games, as well as text messages.[179]

- **Guardian Angel Technology** also produces a GPS phone for children that lets parents monitor their kids via the Internet.[180] Guardian phones let parents keep a record of their child's movements for a 30-day period. And when the child is traveling in a car, the phone can monitor how fast the car is going and the direction in which it is heading.

- **Verizon Wireless's "Migo"** is similar to the Firefly Mobile phone in that has a limited number of buttons for parents to program with approved and emergency-related numbers.[181] Kids can decorate the colorful phone with stickers and other accessories. Using Verizon's Chaperone service, parents can enable GPS tracking of their kids. Verizon also offers a feature called Child Zone which notifies parents via a text message if their child strays beyond pre-approved boundaries.[182]

A Word about Wireless Geo-location Services and Social Mapping

Many of the phones and services described above include geo-location technologies that parents can use to monitor the movement of their children. Those same geo-location services can be used for other purposes. Geo-location

---

[176] Kim-Mai Cutler, "A Phone of Their Own," *Wall Street Journal*, August 4, 2005,p. D1.
[177] http://disneymobile.go.com
[178] Also see Merissa Marr, "Ring the Parents: Disney Is Set to Unveil Cellphones for Kids," *Wall Street Journal*, April 5, 2006, p. B3; Walter S. Mossberg and Katherine Boehret, "Cellphones Let Parents Set Limits," *Wall Street Journal*, August 16, 2006, p. D3.
[179] www.wherify.com/wherifone
[180] www.guardianangeltech.com
[181] http://estore.vzwshop.com/search/devices/lg_migo.html
[182] www.kidswireless.com/articles/verizon-wireless-chaperone

technologies are now being married to social networking utilities to create an entirely new service and industry: social mapping.[183]

Social mapping allows subscribers to find their friends on a digital map and then instantly network with them. Companies such as Loopt[184] and Helio[185] have already rolled out commercial social mapping services. It is likely many other rivals will join them in coming months and years. This new service presents exciting opportunities for users to network with friends and family, but it might also raise some privacy concerns. For example, are random strangers or bad guys monitoring my daughter's whereabouts? Or, is her former boyfriend using such a service to track and stalk her?

Industry is responding to these concerns preemptively. As part of their effort to create and refine their "Wireless Content Guidelines," the CTIA has worked with some of these companies to create privacy and safety guidelines for this emerging technology and industry sector. Loopt and Helio have already taken steps to protect user privacy by establishing a variety of safeguards to ensure that information is not shared inappropriately.[186]

These tools and best practices will be refined and extended, but they are no substitute for parents talking to their kids about proper use of this new technology. Children need to be educated about how these new technologies work and taught to use the tools built into the services to safeguard their personal information. If parents decide to give cell phones to their pre-teen children, they need to configure those phones for them to ensure that these services are disabled or only accessible by trusted family members and acquaintances.

***Wireless / Mobile Media Tips for Parents**:*

- ✓ Teach your children basic etiquette as they start to use more interactive mobile media devices and services, such as cell phones and instant messaging. (See Section IIC for details).
- ✓ For a child's first phone, consider a model that restricts calling options to parents, schools, or emergency contacts. Also consider a model with embedded GPS tracking capabilities to monitor your child's whereabouts.
- ✓ Consider limitations of online and interactive functions until your child is older. Once he or she is given online access through mobile devices, use

[183] "Social networking is just the beginning. Eventually all forms of communication will converge on one pocket-size gizmo that lets you access virtually any information anywhere, at any time. Other people can likewise use their gizmo to find you—as will anyone interested in selling you location-based services. Or you can simply turn off and eat a sub—provided you can resist the urge to broadcast that info to the world." Dan Tynan, "Is That a Social Network in Your Pocket?" *PC World*, August 2007, p. 49.

[184] https://loopt.com

[185] www.helio.com

[186] For Loopt's safety and privacy tips see: https://loopt.com/loopt/beSafe.aspx

parental controls that are embedded within the phone to screen objectionable content or limit access to certain sites.

- ✓ Review your children's phone records to determine if they are communicating with strangers or accessing any objectionable sites or material.
- ✓ Consider calling plans that cap usage time (for both calls and online access) to ensure children do not abuse the privilege. Develop a "calling allowance" to place boundaries on overall monthly usage.

F. Internet, Computing and Social Networking

The Internet is massive, and the sheer scope and volume of online activities make parental control efforts quite challenging. That's especially the case because, as the Pew Internet & American Life Project notes, "American teens are more wired now than ever before."[187] According to a Pew survey taken in late 2006, 93 percent of all Americans between 12 and 17 years old use the Internet. In 2004, by contrast, 87 percent were Internet users, and in 2000, 73 percent of teens were online.[188]

Luckily, many companies and private organizations have already established systems and software to deal with objectionable online content. Parents need to adopt a "layered" approach to online child protection that involves many of the tools and strategies outlined in this section. Of course, it goes without saying that these methods should not be considered substitutes for talking to your children about what they might see or hear while online. Even though the tools and strategies that follow can help parents control the vast majority of objectionable content that their kids might stumble upon while online, no system is perfect. In the end, education and ongoing communication are vital. That being said, these tools and strategies are an important part of the "training wheels and speed bumps" approach discussed at the beginning of Part III.

Finding Help from Online Safety Metasites

There is so much good information on the Internet about online child safety that parents would be wise to rely on some of the "metasites" that aggregate helpful tips, tools, and other information all in one place. The best of these sites include:

[187] Amanda Lenhart and Mary Madden, *Teens, Privacy, and Online Social Networks*, Pew Internet & American Life Project, April 18, 2007, p. 3, www.pewinternet.org/PPF/r/211/report_display.asp

[188] *Ibid*.

- **GetNetWise.org** (www.getnetwise.org) is a public service website operated by the nonprofit Internet Education Foundation[189] and supported by a wide array of Internet and computer companies, as well as a host of public interest organizations and child and family activists.[190] GetNetWise's website offers a comprehensive "Online Safety Guide" and lengthy inventory of "Tools for Families" that can be custom-tailored to the needs and values of individual families.[191]

- **Internet Keep Safe Coalition** (www.iKeepSafe.org) is a coalition of 49 state governors and first spouses, law enforcement officials, the American Medical Association, the American Academy of Pediatrics, and many other corporations[192] and private associations (including many of the groups and sites listed below) that are dedicated to helping parents, educators, and caregivers by providing tools and guidelines to teach children the safe and healthy use of technology. iKeepSafe uses an animated mascot named Faux Paw the Techno Cat to teach children the importance of protecting personal information and avoiding inappropriate places on the Internet. The organization's website offers a downloadable "10 Common Questions about Internet Safety" pamphlet[193] and several video tutorials to help parents set up various filters or controls.[194]

- **i-SAFE Inc.** (www.iSafe.org) is a nonprofit foundation whose mission is "to educate students on how to avoid dangerous, inappropriate, or unlawful online behavior. i-SAFE accomplishes this through dynamic K-12 curriculum and community outreach programs to parents, law enforcement, and community leaders. It is the only Internet safety foundation to combine these elements," its website claims.[195] i-SAFE receives federal grants to support its efforts. The organization produces several monthly newsletters, including one for parents ("i-PARENT Times") and one for educators ("i-EDUCATOR Times"), and it sells a wide variety of printed materials on online safety issues for classroom use.

---

[189] www.neted.org

[190] Major corporate supporters include Google, Microsoft, Verizon, Amazon.com, Yahoo!, AOL, AT&T, Comcast, Dell, Earthlink, Visa, Wells Fargo, and the Recording Industry Association of America. Key public interest organizations include the Center for Democracy and Technology, the American Library Association, The Children's Partnership, People for the American Way Foundation, National Consumers League, and many others.

[191] See http://kids.getnetwise.org/safetyguide and http://kids.getnetwise.org/tools

[192] Corporate sponsors include AOL, Dell, Disney, Intel, Oracle, Siebel Systems, Symantec, and Yahoo! among others.

[193] www.ikeepsafe.org/iksc_partners/symantec/10_questions/Assets/TenCommonQuestions.pdf

[194] www.ikeepsafe.org/PRC/videotutorials/index.php

[195] www.isafe.org/channels/?ch=ai

Exhibit 23:
Various Online Safety "Metasites"

Get Net Wise

iKeepSafe

iSafe

NetSmartz

Project Online Safety

StaySafe.org

- **Net Smartz Workshop** (www.NetSmartz.org) is produced by the National Center for Missing and Exploited Children and the Boys and Girls Clubs of America. This comprehensive website contains web safety tips and educational materials for parents, preteens, teens, educators, and law enforcement officials. They also sponsor a site devoted to younger children (www.netsmartzkids.org) that features interactive online safety games and videos, as well as the NetSmartz Internet Safety Helpdesk (www.netsmartz411.org), which is sponsored by the Qwest Foundation.
- **Project Online Safety** (www.projectonlinesafety.com) is a collaborative online portal that offers a directory of online safety tools and educational materials developed by technology companies, media organizations and nonprofits. Coalition members include: AT&T, BlogSafety.com, Cable in the Classroom, Charter, Comcast, Cox, Facebook, Fox Interactive Media (owner of MySpace.com), Internet Education Foundation, National Cable and Telecommunications Association, Network Solutions, Qwest, Time Warner Cable, and the National Center for Missing and Exploited Children. Each organization provides an overview of its online safety efforts and links to various resources that parents can use to keep their kids safe online or to educate them about online dangers.
- **StaySafe.org** (www.staysafe.org) is an educational website sponsored by the Microsoft Corporation "intended to help consumers understand both the positive aspects of the Internet as well as how to manage a variety of safety and security issues that exist online."[196] The site contains specific sections for teenagers, parents, senior citizens, and educators with tips and tools tailored to each group.
- **WebWiseKids** (www.wiredwithwisdom.org) is a nonprofit organization "committed to teaching children and their caregivers strategies for safe Internet use, including methods of detecting and deterring online predators."[197] It specializes in interactive software and games that teach kids how to spot online threats and to deal with them promptly.
- **Wired Safety** (www.wiredsafety.org) bills itself as "the largest online safety, education and help group in the world. We are a cyber-neighborhood watch and operate worldwide in cyberspace through our more than 9,000 volunteers worldwide."[198] The site offers educational services and online assistance and reviews family-friendly websites, filtering software, and other Internet services. Wired Safety also operates or works with several other affiliated online safety sites, such as:
    - **Wired Cops** (www.wiredcops.org or www.cyberlaw-enforcement.org) are "specially-trained volunteers [who] patrol the

[196] www.staysafe.org/about.html
[197] www.wiredwithwisdom.org/who_we_are.asp
[198] www.wiredsafety.org/information/about_us.html

Internet looking for child pornography, child molesters and cyberstalkers."

- **Wired Kids** (www.wiredkids.org) is geared toward youngsters and teens to help them understand online threats and know how to deal with them.
- **Teen Angels** (www.teenangels.org) "is a group of 13 to 18 year-old volunteers that have been specially trained by the local law enforcement, and many other leading safety experts in all aspects of online safety, privacy, and security. After training for six sessions, the Teenangels run unique programs in schools to spread the word about responsible and safe surfing to other teens and younger kids, parents, and teachers."
- **Net Bullies** (www.NetBullies.com) aims to protect kids from cyber-bullying.

Many other excellent websites offer parents and kids outstanding advice about how to stay safe online, including: Net Family News,[199] ProtectKids.com,[200] SafeKids.com,[201] SafeTeens.com,[202] BlogSafety.com,[203] ChatDanger.com,[204] StopCyberbullying.org,[205] Cyberbully.org,[206] and StopTextBully.com.[207] CNet.com also offers a very user-friendly portal for families.[208] Finally, excellent examples of how other countries are addressing the same issues can be found at BeWebAware.ca (Canada),[209] BeSafeOnline.org (Europe),[210] and NetAlert.net (Australia).[211]

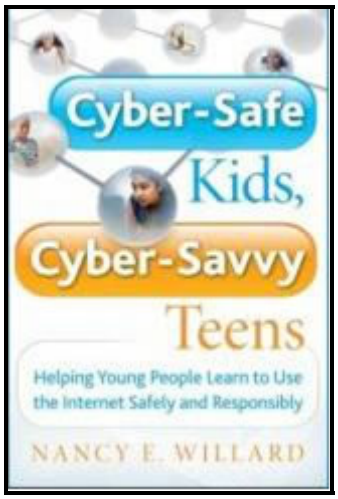
Several good books are also available that can help parents get a better feel for how to deal with online concerns in general. The best of these books include Nancy Willard's *Cyber-Safe Kids, Cyber-Savvy Teens*;[212] Sharon Miller Cindrich's *e-Parenting: Keeping Up with Your Tech-Savvy Kids*;[213] and, Larry

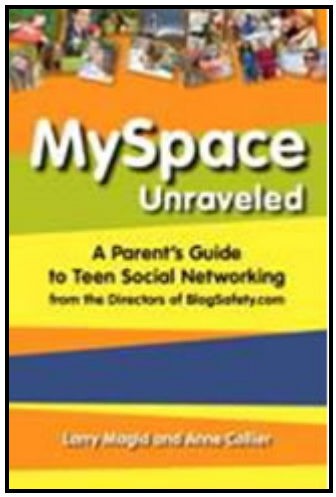
---

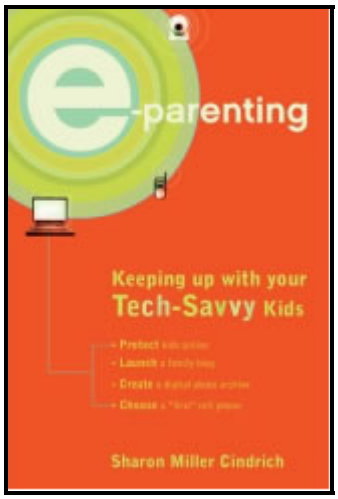
[199] http://netfamilynews.org/index.shtml
[200] http://protectkids.com
[201] www.safekids.com
[202] www.safeteens.com
[203] www.blogsafety.com
[204] www.chatdanger.com
[205] www.stopcyberbullying.org
[206] www.cyberbully.org
[207] www.stoptextbully.com
[208] www.cnet.com/2001-13384_1-0.html
[209] www.bewebaware.ca
[210] www.besafeonline.org
[211] www.netalert.net.au
[212] Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), www.cskcst.com
[213] Sharon Miller Cindrich, *e-Parenting: Keeping Up with Your Tech-Savvy Kids* (New York: Random House Reference, 2007), www.pluggedinparent.com

Magid and Anne Collier's *MySpace Unraveled: A Parent's Guide to Teen Social Networking*.[214]:

Exhibit 24: Books about Online Safety and Sensible Media Use







Filters and Monitoring Software

One of the first things that most of these sites and books recommend is that parents install filtering or monitoring software on the computers their children use. Parents can either use "stand-alone" filtering and monitoring tools or rely on the parental control tools provided by their Internet service provider. A discussion of both types of tools follows.

(1) Independent / "Client-Based" Filters and Monitoring Tools: Most parents are familiar with Internet filtering software and use filters to control their children's online surfing activities. At a minimum, these software tools let parents block access to adult websites and impose time management constraints on their children's computer and Internet usage.

Increasingly, however, these software packages also include far more robust monitoring tools that let parents see each website their children visit, view every e-mail or instant message that they send and receive, or even record every word that they type into their word processors.[215] Many of these monitoring tools can then send parents a periodic report summarizing their child's Internet usage and communications. More robust software programs even allow parents to capture screen shots of sites their kids have visited. Finally, these tools allow parents to do all this in a surreptitious fashion since, once the software is installed on a child's computer, it is entirely invisible to the user.

[214] Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), www.myspaceunraveled.com

[215] See Jessica E. Vascellaro and Anjali Athavaley, "Foley Scandal Turns Parents Into Web Sleuths," *Wall Street Journal*, October 18, 2006, p. D1.

Exhibit 25: Internet Filtering and Monitoring Software

- **Activity Logger** (www.softactivity.com)
- **BeNetSafe** (www.benetsafe.com)
- **Bsafe Online** (http://bsafeonline.com)
- **Children's Internet** (www.thechildrensinternet.com)
- **Clean Internet.com** (http://cleaninternet.com)
- **Content Cleaner** (www.contentpurity.com)
- **Content Protect** (www.contentwatch.com)
- **CyberPatrol** (www.cyberpatrol.com)
- **Cyber Sentinel** (www.cybersentinel.com)
- **CyberSitter** (www.cybersitter.com)
- **eBlaster** (www.spectorsoft.com)
- **FamiLink** (www.familink.com)
- **Family Cyber Alert** (www.itcompany.com)
- **FilterGate** (http://filtergate.com)
- **FilterPak** (www.surfguardian.net/products.shtml)
- **Guardian Monitor** (www.guardiansoftware.com)
- **IamBigBrother** (www.iambigbrother.com)
- **IM Safer** (www.imsafer.com)
- **Internet4Families** (www.i4f.com)
- **iShield** (www.guardwareinc.com)
- **K9 Web Protection** (www.k9webprotection.com)
- **KidsNet** (www.sti.net/s-kidsnet.html)
- **McAfee Internet Security Suite** (http://us.mcafee.com)
- **Microsoft Live One Care** (www.windowsonecare.com)
- **NetIntelligence** (www.netintelligence.com)
- **Netsweeper** (www.netsweeper.com)
- **NetMop** (www.netmop.com)
- **NetNanny** (www.netnanny.com)
- **Norton Internet Security** (www.symantec.com/home_homeoffice/products)
- **Online Safety Shield** (www.onlinesafetyshield.com)
- **Optenet PC** (www.optenetpc.com)
- **Parental Control Bar** (www.wraac.org)
- **PC Tattletale** (www.pctattletale.com)
- **Razzul** (www.kidinnovation.com)
- **SafeEyes** (www.safeeyes.com)
- **Sentry At Home** (www.sentryparentalcontrols.com)
- **Sentry Remote** (www.sentryparentalcontrols.com)
- **Snoop Stick** (www.snoopstick.com)
- **Spector Pro** (www.spectorsoft.com)
- **Spy Agent** (www.spytech-web.com/software.shtml)
- **Surf On the Safe Side** (www.surfonthesafeside.com)
- **SurfPass** (www.cogilab.com/us/homeedition)
- **Webroot Child Safe** (www.webroot.com)
- **WebWatcher** (www.awarenesstech.com/parents/index.html)

Similarly, "IM Safer" offers a free downloadable tool that can help parents monitor instant messenger conversations and notify them when their child is engaged in a potentially dangerous conversation on IM.[216] Importantly, the IM Safer tool respects a child's privacy since not parents are not allowed to read the full transcripts of online communications. Instead, the application only monitors IM conversations for content that is considered dangerous. Importantly, however, this includes the trading of phone numbers or other personal information.

Some parents might flinch at this level of child surveillance, but other will find it entirely appropriate, especially for very young children just getting online.[217] Regardless, a wide variety of such filtering and monitoring tools is available and they can be calibrated to meet parents' specific needs and values. A comprehensive list of these software tools can be found at the GetNetWise.org website ,[218] but some of the most popular filtering and monitoring tools are listed in Exhibit 25.

Parents need to adopt a "layered" approach to online child protection that involves many tools and strategies.

Of course, not all filtering and monitoring tools are equal, and features vary by product. Moreover, tools come and go, and many change over time in terms of functions and capabilities. Parents trying to determine which tool or service is best for them can find helpful reviews at the sites shown in Exhibit 26.

(2) ISP-Integrated Parental Controls and Filtering Tools: Stand-alone or "client-based" filtering solutions, such as those described above, dominated the online parental controls marketplace in the late 1990s. The market has changed significantly since then, however. Today, Internet service providers (ISPs)—which include major broadband service providers (BSPs)—offer parental control services as part of an integrated suite of security tools, which typically also usually includes anti-virus, anti-spyware, and anti-Spam tools. These security options are often offered free of charge, or for a small additional fee, when subscribers sign up for monthly Internet service. And most of these integrated tools offer automatic updates such that consumers need not manually download upgrades to stay current.

That means that millions of parents now have free or quite inexpensive Internet parental control tools at their disposal as soon as they sign up for

[216] www.imsafer.com

[217] As the National Research Council report concluded of monitoring software: "[A]ctive supervision of children is often appropriate—not because they are criminals but because it is the responsibility of adults to teach them how to internalize the appropriate values and to become better at avoiding inappropriate behavior as they mature." Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 315.

[218] See www.getnetwise.org

Internet access through an ISP. Of course, parents can also add on other tools or independent filtering and monitoring solutions such as those outlined earlier.

Exhibit 27 lists the Internet security websites for major ISPs and broadband operators. And Exhibit 28 provides screen shots of some of their websites.

Exhibit 26: Filter and Monitoring Software Review Sites

- www.child-internet-safety.com
- www.monitoringsoftwarereviews.org
- http://internet-filter-review.toptenreviews.com
- www.filterreview.com
- www.download.com/sort/3150-2162_4-0-1-3.html
- www.consumersearch.com/www/software/parental-control-software/index.html
- www.pcmag.com/category2/0,1874,1639158,00.asp
- www.consumerreports.org/cro/electronics-computers/internet-filtering-software-605/overview/index.htm

Exhibit 27:
Internet Security and Parental Control Websites
for Major ISPs and Broadband Operators

- **AOL** (http://daol.aol.com/parentscentral)
- **AT&T** (www.att.com/safety)
- **Cablevision** (www.powertolearn.com/internet_smarts/index.shtml)
- **Charter** (www.charter.com/Visitors/NonProducts.aspx?NonProductItem=65)
- **Comcast** (www.comcast.net/security)
- **Cox** (www.cox.com/takecharge/internet_controls.asp)
- **Earthlink** (www.earthlink.net/software/free/parentalcontrols)
- **Insight BB** (www.insightbb.com/pcsecurity/default.aspx)
- **Microsoft** (www.microsoft.com/protect)
- **NetZero** (www.netzero.net/support/security/tools/parental-controls.html)
- **Qwest** (www.incredibleinternet.com)
- **Time Warner** (www.timewarnercable.com/centralny/products/internet/parentalcontrols.html)
- **Verizon** (http://netservices.verizon.net/portal/link/main/safety)

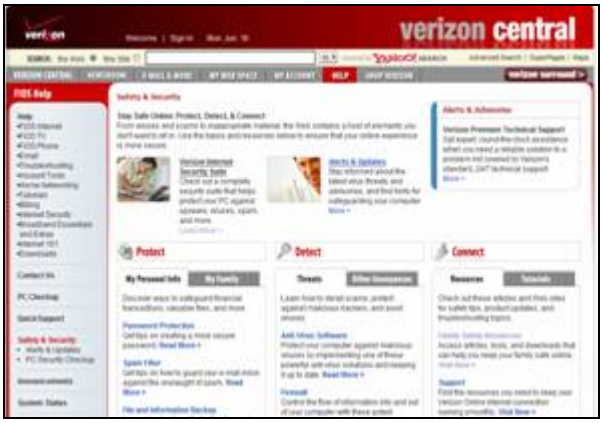
Exhibit 28:
Major ISP Online Safety Sites

AT&T's "Smart Limits"

Qwest's "Incredible Internet"

NCTA's "Point Smart. Click Safe"

Verizon's "Verizon Central"



Operating Systems and Web Browser Controls

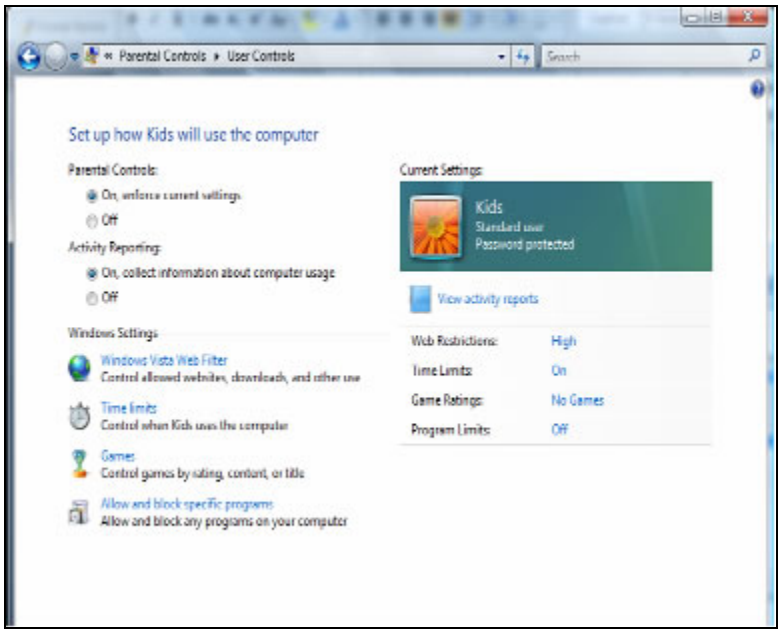
Increasingly, companies like Microsoft and Apple are integrating parental controls into PC operating systems and web browsers. As Walter Mossberg of *The Wall Street Journal* notes, these are "powerful tools to help parents get a handle on their children's computing and online activities."[219]

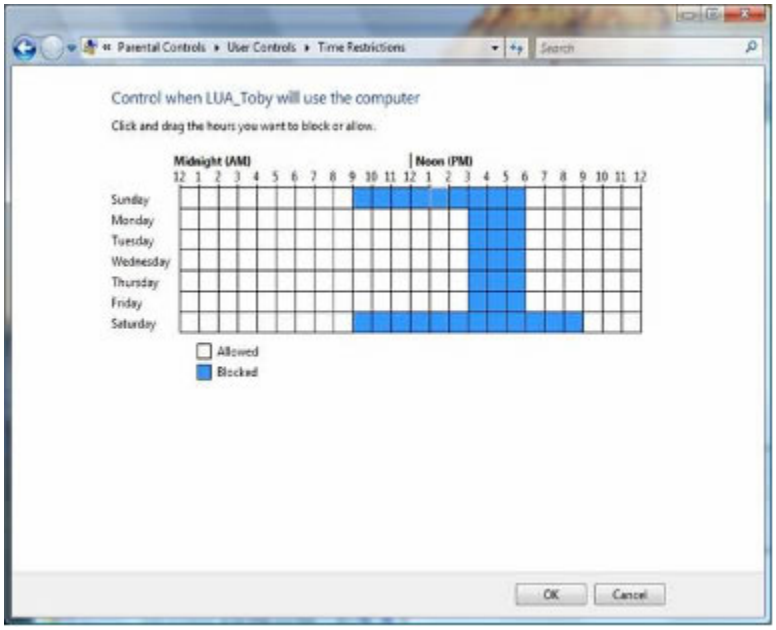
(1) Microsoft's "Vista" OS and Internet Explorer: The new Windows Vista operating system is Microsoft's first version of Windows that incorporates embedded family safety tools. As Seth Schiesel of *The New York Times* reports, "With Vista, Microsoft has for the first time built a robust set of parental controls

[219] Walter S. Mossberg, "You Have Weapons in Your Computer to Monitor Your Kids," *Wall Street Journal*, June 14, 2007, p. B1.

directly into the operating system, not just for gaming but also for Web browsing, file downloading and instant messaging."[220]

Exhibit 29:
Vista Operating System Parental Controls





[220] Seth Schiesel, "For Parents, New Ways to Control the Action," *New York Times*, January 8, 2007, www.nytimes.com/2007/01/08/arts/08vist.html?ex=1325912400&en=3bb7bc1b6a470a23&ei=5090&partner=rssuserland&emc=rss

Vista lets parents establish "administrator" accounts and then oversee the individual users—namely, their own children—who are using the PCs. Parents can then configure the Vista sub-accounts to enable various parental control features and monitoring tools. They can turn on web filters that will block specific types of potentially objectionable website content or downloads. Time limits can also be established for the PC that restrict when or how long the child may use the computer. (Exhibit 29).

Also, much like new video game consoles, Vista will also let parents restrict video game play by rating or title, and games with no ratings can be blocked entirely if the parents want. Parents can also see an "activity list" of the sites their child has visited, or attempted to visit, as well as files and applications that have been downloaded. Applications or software that the parents find objectionable can then be blocked from that same screen.[221] Importantly, once these parental controls have been enabled within Vista, there is no need for parents to configure additional controls within Internet Explorer. Vista controls all Internet Explorer web-browsing activities.

Finally, Microsoft has opened up "application programming interfaces" (APIs) to third-party software developers so that they can build additional parental control tools on top of Vista. One of these developers is IM Safer, which was discussed earlier. A number of other add-ons for Internet Explorer also let parents add more layers of controls. Microsoft has created a webpage featuring all these parental control add-ons.[222]

(2) Apple's Tiger OS X and Safari: Apple's parental controls aren't quite as sophisticated as Microsoft's Vista-based controls. Apple's Safari web browser adopts a white-listing approach to parental controls. Parents can establish which website children can visit by bookmarking them for their kids. All other sites will be blacklisted.[223] Apple's Tiger operating system also allows parents to establish accounts for their children and control some of their online activities. In addition, parents can also build a restricted "buddies list" for their children and then disallow instant messaging to anyone else. The system can also hide the child's online status so that only those pre-approved buddies can see that they are online at any time.[224]

(3) Firefox: Firefox is an independent web browser that is managed by the Mozilla Foundation. Although Mozilla does not offer parental controls directly for the Firefox browser, third parties are free to devise and offer parental control tools as "add-ons" to the browser. "Glubble" is one such example.[225] (Exhibit 30).

---

[221] www.microsoft.com/windowsvista/features/forhome/safety.mspx#more
[222] www.windowsmarketplace.com/category.aspx?bcatid=837&tabid=1
[223] www.apple.com/macosx/features/safari
[224] www.apple.com/macosx/features/family
[225] http://glubbleworld.com

Once the program is loaded onto a user's computer, it locks the Firefox browser such that a password is required before a user can access the Internet. Parents can then establish a user account for their children that only allows them to access to a set of pre-screened, kid-friendly websites.

Exhibit 30:
"Glubble" for the Firefox Web Browser

The Importance of Website Labeling and Metadata Tagging

Many of the parental control tools mentioned throughout this study rely on labeling schemes and metadata tagging. As was explained in previous sections, metadata are machine-readable digital data that describe audiovisual media content. For example, MPAA movie ratings and ESRB video game ratings are digitally embedded within DVDs and video games so that other parental control tools (i.e., DVD players, computers, video game consoles, etc.) can then be used to screen out unwanted content.

This same approach can work for Internet websites. Machine-readable content descriptors can be embedded within websites or online content to "tag" the sites or material. Once tagged, the sites or content can be automatically screened by other devices (i.e., filters, operating systems, etc.) regardless of how that content is accessed.

The Internet Content Rating Association (ICRA),[226] which is part of the Family Online Safety Institute (FOSI),[227] is helping to develop improved Internet

[226] www.fosi.org/icra
[227] www.fosi.org

filtering systems through comprehensive website labeling and metadata tagging. ICRA has created a wide variety of content descriptors that website operators can use to self-label their sites. ICRA does not rate Internet websites or the content itself. It leaves it to the content providers to do that using the ICRA labeling system.[228] ICRA's website provides additional detail about how the system works:

> The centerpiece of the organization is the descriptive vocabulary, often referred to as "the ICRA questionnaire." Content providers check which of the elements in the questionnaire are present or absent from their websites. This then generates a small file containing the labels that is then linked to the content on one or more domains.…
>
> The descriptive vocabulary was drawn up by an international panel and designed to be as neutral and objective as possible. It was revised in 2005 to enable easier application to a wide range of digital content, not just websites. Most of the items in the questionnaire allow the content provider to declare simply that a particular type of content is present or absent. The subjective decision about whether to allow access to that content is then made by the parent.[229]

Once these metadata labels have been embedded within websites, parents can freely download the ICRAplus filter from ICRA's website and customize it to their specific needs / tastes.[230] Or they can use unaffiliated filters or computer operating system controls to screen content by ICRA labels.

Many of the parental control tools mentioned throughout this study rely on labeling schemes and metadata tagging. This same approach can work for Internet websites.

Other metadata labeling initiatives exist. The Association of Sites Advocating Child Protection (ASACP), a nonprofit organization founded in 1996 by the adult entertainment industry to eliminate child pornography from the Internet.[231] ASCAP also works to help parents prevent children from viewing age-inappropriate material online through its "Restricted to Adults" (RTA) website metadata labeling initiative.[232] The RTA label is a general descriptor that all adult entertainment website operators are encouraged to use to help parents who wish to block all such content. Incidentally, websites using

[228] For a description of the ICRA labels and the labeling process, see www.icra.org/label/generator
[229] See "About ICRA," www.fosi.org/icra
[230] www.icra.org/icraplus
[231] www.asacp.org
[232] www.rtalabel.org

the RTA metadata tag can use it in conjunction with more descriptive ICRA metadata labels.

Microsoft also has an "Essential Metadata Initiative" that works in conjunction with a wide variety of organizations to develop digital metadata tags for media content.[233] Specifically, Microsoft works closely with the Geneva, Switzerland-based International Standard Audiovisual Number International Agency (ISAN-IA), which operates the International Standard Audiovisual Number (ISAN). ISAN is a widely recognized, global content labeling system for digital audiovisual material.[234]

Although it is generally known as a system to help content creators manage their intellectual property rights, ISAN tags can also be useful in identifying many other attributes of the underlying content in question. Specifically, content rating and labeling information can be embedded within the ISAN tag. Microsoft products such as Vista and Internet Explorer can read ISAN metadata tags and then filter accordingly.[235] And the motion picture industry is using ISAN tags to better identify its content, and rating information from various countries is included in those tags.[236] According to Patrick Attallah, ISAN Managing Director, as of April 2007, the ISAN identification and metadata system supported over 90 different content-specific tags and more than 50 worldwide rating systems in over 35 languages.[237]

Search Engine Filters and Portals for Kids

Parents can also use tools embedded in search engines to block a great deal of potentially objectionable content that children might inadvertently stumble upon during searches.

For example, Google offers a SafeSearch feature that allows users to filter unwanted content. Users can customize their SafeSearch settings by clicking on the "Preferences" link to the right of the search box on the Google.com home page.[238] Users can choose "moderate filtering," which "excludes most explicit images from Google Image Search results but doesn't filter ordinary web search results," or "strict filtering," which applies the SafeSearch filtering controls to all search engine results.

---

[233] "International Organization Licenses Microsoft's New Multicolor Bar Code Technology for Identifying Audiovisual Works," Microsoft Corporation, *Press Release*, April 16, 2007, www.microsoft.com/Presspass/press/2007/apr07/04-16MSBarCodePR.mspx

[234] www.isan.org

[235] Kevin J. Comerford and Michael A. Dolan, "ISAN Implementation in Windows Media Technologies," Microsoft Corporation, May 2006, www.isan.org/docs/ISAN%20Implementation%20in%20WindowsMedia%20May%202006.pdf

[236] "Audiovisual Works Identification for the Motion Picture Studio: Conceptual, Operational, and Technical," Motion Picture Association of America, 2007, www.secpath.com/pdf/Audiovisual_ID_Practices%202007-03-20_r2.pdf

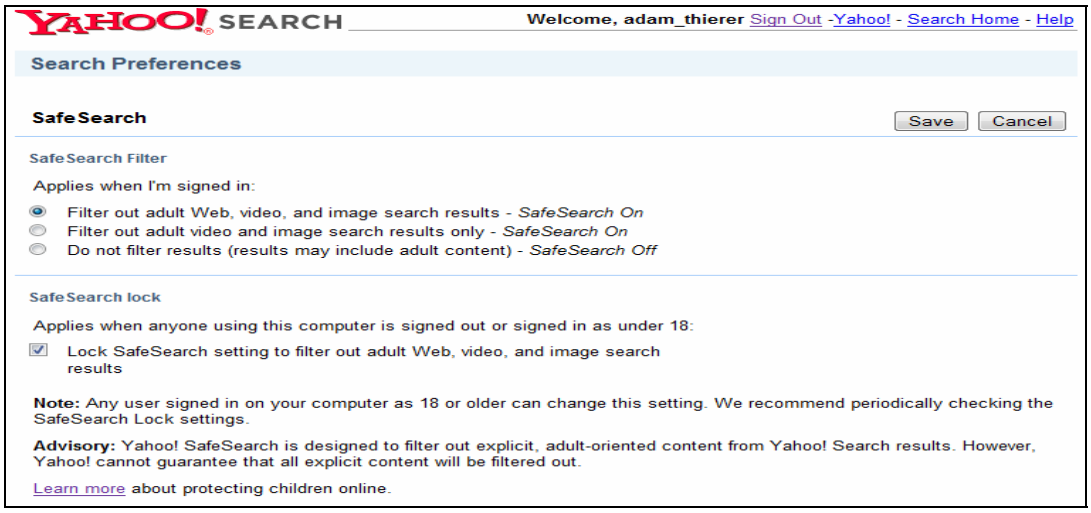
[237] E-mail conversation on April 17, 2007, on record with author.

[238] www.google.com/intl/en/help/customize.html#safe

Exhibit 31:
"Safe Search" Filtering Tools

Google

Yahoo



Microsoft

Similarly, Yahoo! also has a SafeSearch tool that can be found under the "Preferences" link on the "My Web" tab.[239] Like Google, Yahoo! allows strict or moderate filtering. Microsoft's Live Search works largely the same way.[240] Other search engine providers such as AltaVista,[241] AskJeeves,[242] HotBot,[243] Lycos,[244] and AllTheWeb,[245] also provide filtering tools. Working in conjunction with other filters, these search engine tools are quite effective in blocking a significant amount of potentially objectionable content.

Exhibit 32: Kid-Friendly Internet Search Engines and Portals

- **ALA's Great Web Sites for Kids** (www.ala.org/greatsites)
- **AOL for Kids (U.S.)** (http://kids.aol.com)
- **AOL for Kids (Canada)** (http://canada.aol.com/aolforkids)
- **Ask Jeeves for Kids** (www.askforkids.com)
- **Awesome Library for Kids** (www.awesomelibrary.org)
- **Diddabdoo** (www.dibdabdoo.com)
- **Education World** (www.education-world.com)
- **Fact Monster** (www.factmonster.com)
- **Family Source** (www.family-source.com)
- **FirstGov for Kids** (www.kids.gov)
- **KidsClick** (www.kidsclick.org)
- **NetTrekker** (www.nettrekker.com)
- **SearchEdu.com** (www.searchedu.com)
- **Surfing the Net with Kids** (www.surfnetkids.com)
- **Surf Safely.com** (www.surfsafely.com)
- **TekMom's Search Tools for Students** (www.tekmom.com/search)
- **ThinkQuest Library** (www.thinkquest.org/library)
- **Yahoo! Kids** (http://kids.yahoo.com)

A better approach to use with younger children is to direct them to search engines or web portals geared toward younger audiences. Several excellent websites, such as those listed in Exhibit 32, let kids search numerous sites without stumbling upon adult-oriented material.[246] Better yet, they direct children to sites and information that are educational and enriching. In essence, these

[239] http://myweb.yahoo.com
[240] http://search.msn.com/settings.aspx
[241] www.altavista.com/web/ffset?ref=/
[242] www.ask.com/webprefs
[243] www.hotbot.com/prefs_filters.asp
[244] http://search.lycos.com/adv.php?query=&adf=
[245] www.alltheweb.com/customize?backurl=Lw&withjs=1
[246] This lists builds on the excellent compendium of sites listed at the Search Engine Watch website: http://searchenginewatch.com/showPage.html?page=2156191

search portals are massive white lists of acceptable sites and content that have been pre-screened to ensure that they are appropriate for very young web surfers. The only downside of using such services is that a lot of wonderful material available on the World Wide Web might be missed. But many parents will be willing to make that trade-off since they desire greater protection of their children from potentially objectionable content.

Exhibit 33: Child- and Teen-Oriented Websites

- **Clever Island** (www.cleverisland.com)
- **Disney Playhouse** (http://disney.go.com/playhouse/today/index.html)
- **Disney's Club Blast** (http://disney.go.com/blast)
- **Disney's Toon Disney Games** (http://psc.disney.go.com/abcnetworks/toondisney/games)
- **Disney Toontown Online** (http://play.toontown.com)
- **Habbo** (www.habbo.com)
- **HBO Family Games** (www.hbofamily.com/games)
- **JuniorNet** (www.juniornet.com)
- **Kaboose Family Network** (www.kaboose.com)
- **Kaboose FunSchool** (http://funschool.kaboose.com)
- **KidsClick** (www.kidsclick.org)
- **KidsFirst** (www.kidsfirst.org)
- **Microsoft At School** (www.microsoft.com/education/atschool.mspx)
- **Net Smartz Kids** (www.netsmartzkids.org)
- **Nickelodeon Games** (www.nick.com/games)
- **Nick Jr. Games** (www.nickjr.com)
- **Nicktropolis** (www.nicktropolis.com)
- **Noggin Games** (www.noggin.com/games)
- **PBS Kids** (http://pbskids.org/go)
- **Safe Sites for Children (U.K.)** (www.ssfchildren.co.uk)
- **Surfing the Net with Kids** (www.surfnetkids.com)
- **Surf USA** (www.surfonthenet.com)
- **Yahoo! Kids** (http://kids.yahoo.com)
- **YoKidsYo** (www.yokidsyo.com)
- **Zeeks** (www.zeeks.com)

More Online Content-Tailoring Options and Kid-Friendly Websites

The child-friendly web portals discussed above generally direct children to informational and educational sites and resources. But there exist many other ways to tailor the web-surfing experience to a family's specific needs and values. The Internet is full of wonderful sites dedicated to kids and teens. Many have an educational focus, whereas others offer enjoyable games and activities for children. Exhibit 33 highlights some of the best of these websites, but this list just

scratches the surface. If parents wanted, they could configure their web browsers to access only sites such as these and then block access to all other webpages.

A Word about Social Networking Sites

Social networking websites have become wildly popular with teenagers in recent years. Sites such as MySpace, Facebook, Xanga, Bebo, Hi5, Friendster, Tagged, Imbee, LiveJournal, Yahoo! 360°, and Windows Live Spaces attract millions of users and represent just a few of the hundreds of social networking sites online today.[247] These sites offer their users the space and tools to build the equivalent of an online journal and then to network with others more easily. New sites are seemingly surfacing every week, and they are growing more personalized in an attempt to appeal to specific niches.[248]

But concerns about how youngsters use these services quickly prompted lawmakers to introduce legislation to ban access to such sites in schools and libraries.[249] Others, including several state attorneys general, want such sites to age-verify all users to exclude those over or under a certain age.[250] Proposals to impose age verification schemes on social networking websites are discussed in more detail in Part V.[251]

What parents need to understand about social networking websites is that, unlike other "professional" websites, they feature a great deal of "amateur" user-generated content. This makes it more difficult for filters or other parental control tools to screen out potentially undesirable material. Luckily, most mainstream social networking sites take steps to pre-screen many of the images that are uploaded to their sites and block objectionable material. But it will be impossible for these website operators to control everything that is said or posted on these sites in light of the sheer volume of material and human communication taking place.

---

[247] For a list of notable social networking sites, see: http://en.wikipedia.org/wiki/List_of_social_networking_websites

[248] See Robert D. Hof, "There's Not Enough 'Me' in MySpace," *Business Week*, December 4, 2006, p. 40.

[249] In the 109th Congress, former Rep. Michael Fitzpatrick (R-PA) introduced the Deleting Online Predators Act (DOPA), which proposed a ban on social networking sites in public schools and libraries. DOPA passed the House of Representatives shortly thereafter by a lopsided 410-15 vote, but failed to pass the Senate. The measure was reintroduced just a few weeks into the 110th Congress by Senator Ted Stevens (R-AK), the ranking minority member and former chairman of the Senate Commerce Committee. It is section 2 of a new bill that Sen. Stevens has sponsored and that is titled the "Protecting Children in the 21st Century Act" (S. 49). See Declan McCullagh, "Chat Rooms Could Face Expulsion," *CNet News.com,* July 28, 2006, http://news.com.com/2100-1028_3-6099414.html?part=rss&tag=6099414&subj=news; Anne Broache, "Congress Off to Slow Start with Tech," *ZDNet News*, January 9, 2007, http://news.zdnet.com/2100-9588_22-6148312.html

[250] Susan Haigh, "Conn. Bill Would Force MySpace Age Check ," *Yahoo News.com*, March 7, 2007, www.msnbc.msn.com/id/17502005

[251] Also see Adam Thierer, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," Progress & Freedom Foundation *Progress on Point* 14.5, March 21, 2007. www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

Thus, parents will need to consider additional solutions. Monitoring software could certainly be part of the answer. Many monitoring tools, discussed earlier, give parents a clear idea of how much time their kids spend online, the specific sites they are visiting, and with whom they are conversing. MySpace.com recently announced that it would soon make sophisticated monitoring software available to parents that will allow them to keep better tabs on their kids' online interactions. The software, dubbed Zephyr, will let parents see the name, age, and location that children are listing on their MySpace accounts. It will update parents if their children change that information for any reason. For privacy reasons, however, the software will not let parents read their child's personal e-mail.[252] Parents can also tap tools such as IM Safer, which was described earlier, to monitor potentially inappropriate release of information by their children.

Finally, parents of pre-teens should be careful about letting them go on social networking sites unattended. But there are some smaller social networking sites such as ZoeysRoom.com,[253] Imbee.com,[254] ClubPenguin.com,[255] and Tweenland.com that have extremely strict enlistment policies, primarily because they target or allow younger users. These sites are discussed in more detail in the section on age verification in Part V.

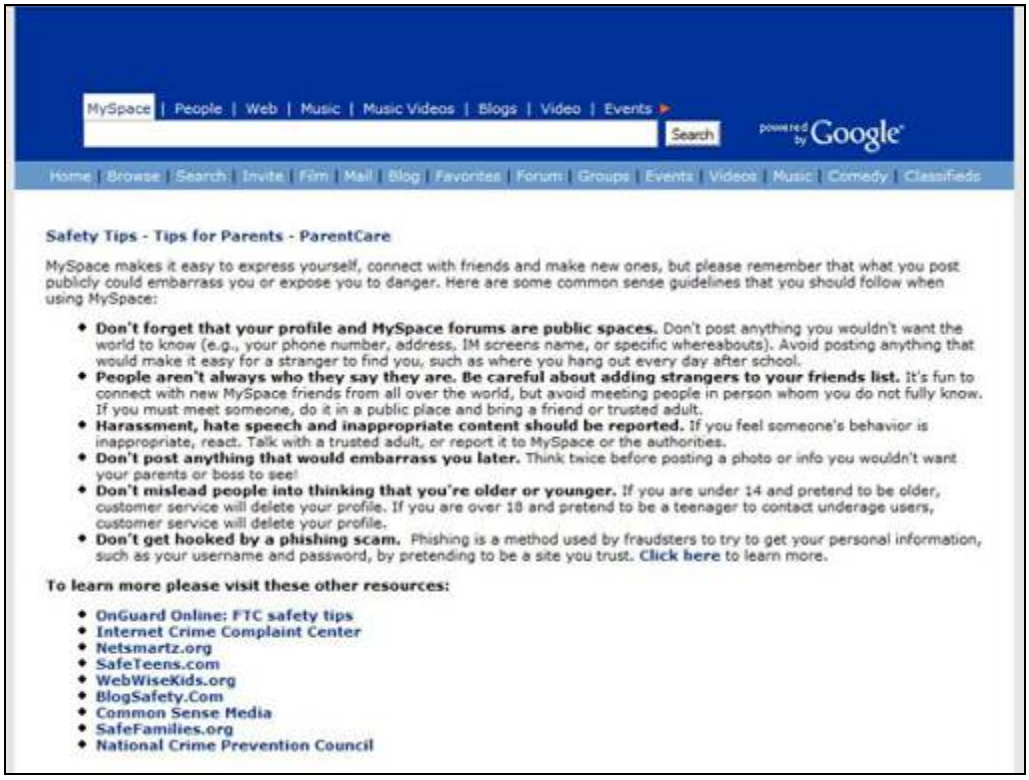
Additional tips for parents about social networking sites can be found in a very accessible booklet, *MySpace Unraveled: A Parent's Guide to Teen Social Networking,* by Larry Magid and Anne Collier.[256] Also, the Federal Trade Commission's OnGuardOnline.gov website offers "Social Networking Safety Tips for Tweens and Teens" as well as "A Parent's Guide" to social networking sites.[257] And the Federal Bureau of Investigation offers "A Parent's Guide to Internet Safety" on its website offering similar advice.[258] MySpace.com also offers safety tips for kids and parents on its site.[259] (Exhibit 34)

Finally, as was outlined in Part II, parents should discuss proper online etiquette with their children before they allow them to get online or visit social networking sites. The websites and books mentioned above can greatly assist parents in this regard.

---

[252] "MySpace Moves to Give Parents More Information," *Wall Street Journal,* January 17, 2007, p. B1.
[253] www.zoeysroom.com
[254] www.imbee.com
[255] www.clubpenguin.com
[256] Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), p. 2.
[257] http://onguardonline.gov/socialnetworking_youth.html and http://onguardonline.gov/socialnetworking.html
[258] www.fbi.gov/publications/pguide/pguidee.htm
[259] www.myspace.com/Modules/Common/Pages/SafetyTips.aspx

Exhibit 34:
MySpace.com's Safety Tips website



MySpace | People | Web | Music | Music Videos | Blogs | Video | Events

Search

powered by Google

Home | Browse | Search | Invite | Film | Mail | Blog | Favorites | Forum | Groups | Events | Videos | Music | Comedy | Classifieds

Safety Tips - Tips for Parents - ParentCare

MySpace makes it easy to express yourself, connect with friends and make new ones, but please remember that what you post publicly could embarrass you or expose you to danger. Here are some common sense guidelines that you should follow when using MySpace:

- **Don't forget that your profile and MySpace forums are public spaces.** Don't post anything you wouldn't want the world to know (e.g., your phone number, address, IM screens name, or specific whereabouts). Avoid posting anything that would make it easy for a stranger to find you, such as where you hang out every day after school.
- **People aren't always who they say they are. Be careful about adding strangers to your friends list.** It's fun to connect with new MySpace friends from all over the world, but avoid meeting people in person whom you do not fully know. If you must meet someone, do it in a public place and bring a friend or trusted adult.
- **Harassment, hate speech and inappropriate content should be reported.** If you feel someone's behavior is inappropriate, react. Talk with a trusted adult, or report it to MySpace or the authorities.
- **Don't post anything that would embarrass you later.** Think twice before posting a photo or info you wouldn't want your parents or boss to see!
- **Don't mislead people into thinking that you're older or younger.** If you are under 14 and pretend to be older, customer service will delete your profile. If you are over 18 and pretend to be a teenager to contact underage users, customer service will delete your profile.
- **Don't get hooked by a phishing scam.** Phishing is a method used by fraudsters to try to get your personal information, such as your username and password, by pretending to be a site you trust. **Click here** to learn more.

To learn more please visit these other resources:

- **OnGuard Online: FTC safety tips**
- **Internet Crime Complaint Center**
- **Netsmartz.org**
- **SafeTeens.com**
- **WebWiseKids.org**
- **BlogSafety.Com**
- **Common Sense Media**
- **SafeFamilies.org**
- **National Crime Prevention Council**

Internet and Computing Tips for Parents

- ✓ Place computers in an area of the home where you can keep an eye on what your kids are doing.
- ✓ Teach your children basic etiquette as they start to use more interactive and online services, such as e-mail, blogs, and instant messaging. (See Part IIC above for details).
- ✓ Do not allow pre-teens to go into chat rooms or on social networking sites unsupervised, if at all. Talk to teenagers about safe online interactions and proper behavior.
- ✓ Use a "layered" approach to online child protection that involves ISP-integrated filters or independent filtering software, monitoring and time management tools, "safe search" search engine controls, and other tools included in your computer's operating system or web browser. Contact your ISP or software vendor for assistance in installing Internet controls and make sure they are set to update automatically.
- ✓ Begin your search for these tools, and collect more helpful tips about online monitoring, by visiting helpful sites such as iKeepSafe.org, GetNetWise.org, StaySafe.org, NetSmartz.org, WiredSafety.org, and the many others listed in this chapter.
- ✓ Enable Internet controls in other media devices (such as gaming consoles or cell phones) if those devices allow online access.

IV. The Importance of Media Literacy and Consumer Education

A. Why Media Literacy Is Important

Everyone understands what is meant by literacy. It's about being able to read and write, of course. But more importantly, it is about comprehension and critical thinking skills. To be "media literate," therefore, is to apply such skills when consuming media. It means we can effectively analyze, comprehend and critique the media we consume.

"To be a functioning adult in a mediated society," notes a report from the Center for Media Literacy, "one needs to be able to distinguish between different media forms and know how to ask basic questions about everything we watch, read or hear."[260] Those questions include:

- What message or values are they trying to convey here?
- How was this made? Who was behind it?
- Is this fact or fiction? Fantasy or reality?
- Is there another perspective I should seek out on this issue?
- Could the story have been told or reported differently?
- What facts or values were left out?
- Where can I find the missing information or perspectives?
- How would others feel about this?
- Are they trying to sell me something? Is it really right for me?
- Is there something better I could be doing with my time?

Some of these critical thinking skills come to us naturally. Some are instilled by parents, but perhaps not regularly enough. "Simple questions about the media can start even at the toddler stage," argue Center for Media Literacy scholars. This brings us back the excellent advice of the National Research Council blue-ribbon panel: "teaching a child to swim—and when to avoid pools—is a far safer approach than relying on locks, fences, and alarms to prevent him or her from drowning."[261]

[260] Elizabeth Thoman and Tessa Jolls, "Literacy for the 21st Century: An Overview and Orientation Guide to Media Literacy Education," Center for Media Literacy, 2005, p. 10, www.medialit.org/reading_room/article540.html

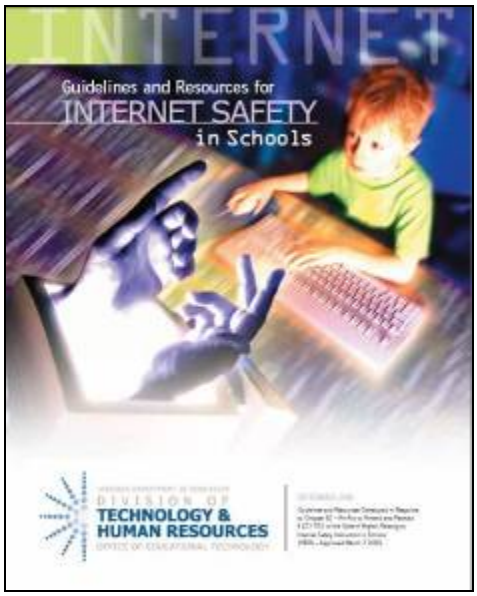
[261] National Research Council, *Youth, Pornography, and the Internet* (Washington, DC: National Academy Press, 2002), p. 187.

B. Promoting Media Literacy and Consumer Education

(1) **In the Classroom**: Unfortunately, it is clear that not nearly enough media literacy instruction is being done within America's educational process at any level. For the most part, media literacy is not routinely integrated into the curricula at elementary school, secondary school, high school, or college.

This situation must be reversed. And it wouldn't take much to make it happen. After all, these are simple principles. These lessons could be drilled into children from a young age as part of other routine studies. And beyond basic media literacy, extensive Internet safety training should also be part of the mix. In September 2006, the Commonwealth of Virginia produced an outstanding report entitled "Guidelines and Resources for Internet Safety in Schools" that can serve as model legislation for other states in this regard.[262] (Exhibit 35). The text of the enabling legislation is found in Exhibit 36. [263]

Exhibit 35:
Virginia's "Guidelines and Resources for Internet Safety in Schools"



[262] www.doe.virginia.gov/VDOE/Technology/OET/internet-safety-guidelines-resources.pdf
[263] http://leg1.state.va.us/cgi-bin/legp504.exe?061+ful+HB58ER

Exhibit 36: Virginia's Model Bill for Internet Safety Instruction

VIRGINIA ACTS OF ASSEMBLY

An Act to amend and reenact § 22.1-70.2 of the Code of Virginia, relating to Internet safety instruction in schools. [H 58] Approved. Be it enacted by the General Assembly of Virginia:

1. That § 22.1-70.2 of the Code of Virginia is amended and reenacted as follows:
§ 22.1-70.2 Acceptable Internet use policies for public and private schools.

A. Every two years, each division superintendent shall file with the Superintendent of Public Instruction an acceptable use policy, approved by the local school board, for the international network of computer systems commonly known as the Internet. At a minimum, the policy shall contain provisions that:

(i) are designed to prohibit use by division employees and students of the division's computer equipment and communications services for sending, receiving, viewing, or downloading illegal material via the Internet;

(ii) seek to prevent access by students to material that the school division deems to be harmful to juveniles as defined in § 18.2-390;

(iii) select a technology for the division's computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372; and

(iv) establish appropriate measures to be taken against persons who violate the policy; and

(v) include a component on Internet safety for students that is integrated in a division's instructional program. The policy may include such other terms, conditions, and requirements as deemed appropriate, such as requiring written parental authorization for Internet use by juveniles or differentiating acceptable uses among elementary, middle, and high school students.

B. The superintendent shall take such steps as he deems appropriate to implement and enforce the division's policy.

C. On or before December 1, 2000, and biennially thereafter, the Superintendent of Public Instruction shall submit a report to the Chairmen of the House Committee on Education, the House Committee on Science and Technology, and the Senate Committee on Education and Health which summarizes the acceptable use policies filed with the Superintendent pursuant to this section and the status thereof.

D. In addition to the foregoing requirements regarding public school Internet use policies, the principal or other chief administrator of any private school that satisfies the compulsory school attendance law pursuant to § 22.1-254 and accepts federal funds for Internet access shall select a technology for its computers having Internet access to filter or block Internet access through such computers to child pornography as set out in § 18.2-374.1:1 and obscenity as defined in § 18.2-372.

E. The Superintendent of Public Instruction shall issue guidelines to school divisions regarding instructional programs related to Internet Safety.

2. That within 45 days of the enactment of this act, the Superintendent of Public Instruction shall issue a superintendent's memorandum advising school divisions of the provisions in this act and encourage cooperation with local law enforcement agencies in its implementation.

State and local officials need to follow the road map outlined by Virginia and begin integrating media literacy and Internet safety lessons into educational curricula at every level. Librarians need to be trained to play a role, too. And funding needs to be provided for all those efforts.

Exhibit 37: Media Literacy Organizations or Efforts

- **Action Coalition for Media Education** (www.acmecoalition.org)
- **Alliance for a Media Literate America** (www.AMLAinfo.org)
- **Cable in the Classroom** (www.ciconline.org)
- **Center for Media Literacy** (www.medialit.org)
- **Children and the Media** [a PBS project] (www.pbs.org/parents/childrenandmedia)
- **Media Awareness Network** [Canada] (www.media-awareness.ca/english/corporate/about_us/index.cfm)
- **Media Literacy Clearinghouse** (www.frankwbaker.com)
- **Media Education Foundation** (www.mediaed.org)
- **Media Literacy Online Project** (http://interact.uoregon.edu/medialit/MLR/home)
- **National Telemedia Council** (www.nationaltelemediacouncil.org)
- **National PTA** (www.pta.org/pr_category_details_1117232399312.html)
- **Project Look Sharp** (www.ithaca.edu/looksharp)

Many other media literacy organizations and efforts exist that can assist in these endeavors. These organizations and efforts are summarized in a 2003 report by Marjorie Heins and Christina Cho of the Free Expression Policy Project (FEPP) entitled, "Media Literacy: An Alternative to Censorship."[264] Exhibit 37 includes most of the groups and efforts discussed in the FEPP report as well as a few others.

A few of these efforts deserve special recognition. "Cable in the Classroom" (CIC) is a media literacy initiative sponsored by the National Cable and Telecommunications Association (NCTA), the cable industry's trade association.[265] It serves as a model for what other companies or industries could do if they wanted to get more serious about promoting media education.

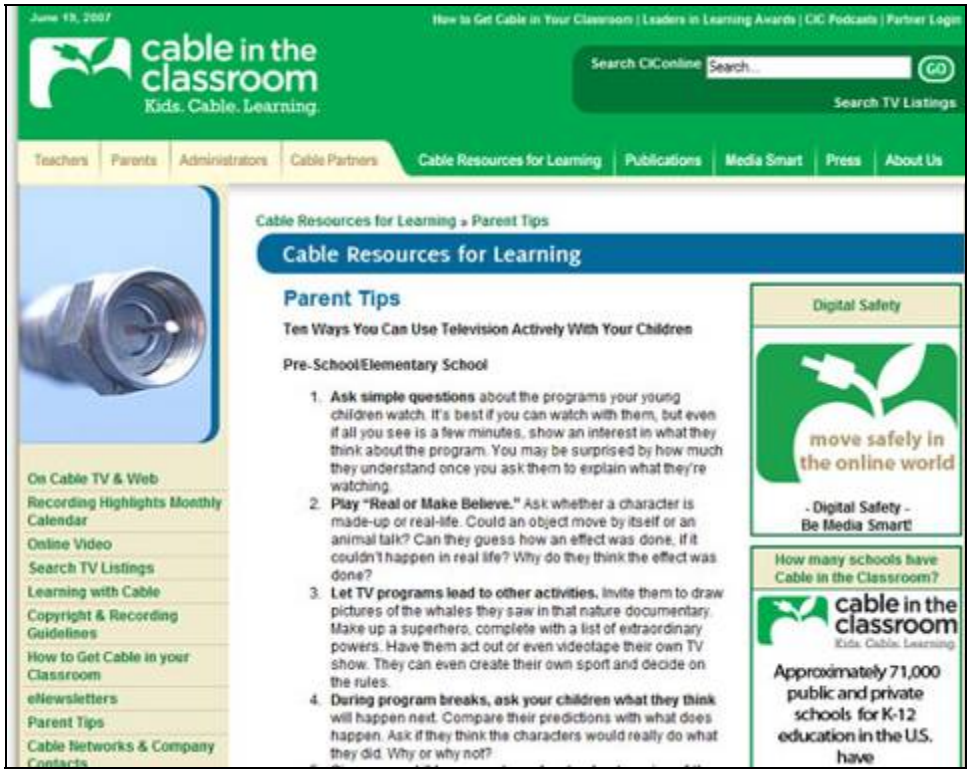
Government officials at the federal, state and local level should work together to devise media literacy campaigns focused on online safety, understanding the existing rating systems, how to use parental controls, and so on.

Started in 1989, the Cable in the Classroom program's mission is "to foster the use of cable content and technology to expand and enhance learning for children and youth

[264] Marjorie Heins and Christina Cho, "Media Literacy: An Alternative to Censorship," Free Expression Policy Project, 2003, www.fepproject.org/policyreports/medialiteracy.html
[265] www.ncta.com/ContentView.aspx?contentId=2695

nationwide."[266] CIC accomplishes this mission by providing video and data connections to schools and libraries, providing access to vast archives of educational video content and enriching cable programming, and providing other learning materials (including a magazine and newsletter) to educators, parents, and children. CIC also offers helpful parenting tips on its website and in its printed materials, such as "Ten Ways You Can Use Television Actively with Your Children,"[267] "Thinking Critically about Media: Schools and Families in Partnership,"[268] and "Navigating the Children's Media Landscape—A Parent's and Caregiver's Guide."[269] (Exhibit 38). CIC also offers schools and parents a downloadable "Recording Highlights Calendar," which notifies them when educational and enriching programming will be aired if they want to record it.[270] The calendar breaks down programming into several categories, including: arts, English language arts, history, languages, math, preschool, science / health, social and personal development, and social studies.

Exhibit 38:
NCTA's "Cable in the Classroom"



[266] "Frequently Asked Questions," Cable in the Classroom, www.ciconline.org/faq
[267] www.ciconline.org/parenttips
[268] www.ciconline.org/thinkingcritically
[269] www.ciconline.org/parentsguide
[270] www.ciconline.org/monthlycalendar

The Center for Media Literacy (CML) also deserves special recognition for its excellent media literacy kits and orientation guides.[271] Its report *Literacy for the 21st Century: An Overview and Orientation Guide to Media Literacy Education*, which was quoted in the introduction to this section, is probably the best layman's overview of media literacy available today.[272] CML's *Media Lit Kit* offers a step-by-step guide to integrating media literacy skills at every education level, from pre-K to college.[273]

(2) **Public and Parental Awareness Campaigns**: Beyond classroom media literacy efforts, government could undertake public awareness campaigns. Government officials at the federal, state and local level should work together to devise media literacy campaigns focused on online safety, understanding the existing rating systems, how to use parental controls, and so on. These campaigns should include broadcast (radio and TV) ads, Internet websites and advertising, and promotional posters and brochures that could be distributed at schools and government institutions. Government has undertaken (or lent its support to) such public awareness campaigns to address other concerns in the past and had a great deal of success, including the following:

Government efforts to promote awareness have been diffuse and largely uncoordinated among various agencies and programs.

- **Forest fire prevention**: Since the mid-1940s, the federal government has used the Smokey the Bear mascot to educate the public about the dangers of forest fires and wildfires.[274]
- **Anti-littering and Land stewardship**: The U.S. Forest Service began a widespread "Give a Hoot, Don't Pollute" anti-littering campaign in the early 1970s that featured the mascot Woodsy Owl. In recent years, the campaign has expanded its land stewardship mission and adopted a new slogan: "Lend a Hand—Care for the Land."[275]
- **Crime prevention**: Beginning in the early 1980s, the National Crime Prevention Council (NCPC) developed its popular "McGruff the Crime Dog" campaign to assist law enforcement agencies seeking to deter crime or build awareness about criminal activities.[276] The McGruff campaign, which included the "Take a Bite Out of Crime" motto, offers publications and teaching materials on a variety of topics; programs that can be

[271] www.medialit.org
[272] Elizabeth Thoman and Tessa Jolls, "Literacy for the 21st Century: An Overview & Orientation Guide to Media Literacy Education," Center for Media Literacy, 2005, p. 10, www.medialit.org/reading_room/article540.html
[273] www.medialit.org/bp_mlk.html
[274] See www.smokeybear.com and http://en.wikipedia.org/wiki/Smokey_the_Bear
[275] www.fs.fed.us/spf/woodsy
[276] http://mcgruff.org

implemented in communities and schools, local, regional, and national training programs; public service announcements broadcast nationwide starring McGruff the Crime Dog; and support for a national coalition of crime prevention practitioners.[277] The NCPC reports that "now 25 years after McGruff's first TV appearance, more than 75 percent of children recognize McGruff and over 4,000 law enforcement agencies own a McGruff suit."[278]

- **Physical fitness**: The President's Council on Physical Fitness promotes physical fitness and healthy living for citizens of all ages, but especially among children and teens. The program, which celebrated its 50th anniversary in 2006, circulates a wide variety of promotional information including classroom materials. Two prominent websites promote the Council's efforts: www.presidentschallenge.org and www.fitness.gov. To further boost the visibility of the program and its fitness agenda, the Council has recruited well-known athletes to serve as chair or spokespersons: actor and former bodybuilder Arnold Schwarzenegger, Olympian Florence Griffith Joyner, baseball player Stan Musial, college basketball coach Al McGuire, professional football coach George Allen, and professional football player Lynn Swann.
- **Seat-belt and air-bag safety**: Perhaps the most successful campaign has been the efforts of the U.S. Department of Transportation's National Highway Traffic Safety Administration,[279] numerous other state and local agencies, and many nonprofit organizations[280] to educate the public about the benefits of wearing seat belts while in automobiles. Of course, these efforts were also accompanied by enforcement efforts, such as the "Click It or Ticket" warnings used in many states. Regardless, the educational component of these campaigns clearly helped communicate the importance of seat belts to the general public.[281] The effort was later expanded to promote air bags in automobiles.

Government officials should seek to emulate these example if they want to construct a serious public awareness campaign about parental controls and online child protection efforts.

Currently, however, government efforts to promote awareness have been diffuse and largely uncoordinated among various agencies and programs. One notable exception at the federal level has been the OnGuardOnline.gov website, which "provides practical tips from the federal government and the technology

---

[277] www.ncpc.org/about
[278] www.ncpc.org/about
[279] www.nhtsa.dot.gov/portal/site/nhtsa/menuitem.cda13865569778598fcb6010dba046a0
[280] The National Safety Council, in particular, has played a major role in these educational efforts. See www.nsc.org/airbag.htm
[281] *Seat Belt Use in 2003 – Demographic Characteristics*, U.S. Department of Transportation, National Highway Traffic Safety Administration, DOT HS 809 729, May 2004, www.nhtsa.dot.gov/people/injury/airbags/809729.pdf

industry to help you be on guard against Internet fraud, secure your computer, and protect your personal information."[282] Six federal agencies collaborated to create the website.[283] Although the initiative doesn't focus exclusively on parental controls or online child protection, it does offer some helpful tips on that front. The effort includes a "Stop-Think-Click" promotion that recommends "Seven Practices for Safer Computing." And the Federal Bureau of Investigation offers similar tips on its "Parent's Guide to Internet Safety" website.[284] But, again, these efforts are largely uncoordinated and receive very little promotion from federal agencies or congressional lawmakers.[285]

Exhibit 39:
The Federal Government's "OnGuardOnline.gov" Website

[282] http://onguardonline.gov/index.html

[283] They are the Federal Trade Commission, the Department of Commerce, the Securities and Exchange Commission, the U.S. Postal Inspection Service, the Office of Justice Programs, and the Department of Homeland Security.

[284] www.fbi.gov/publications/pguide/pguidee.htm

[285] U.S. officials should look at the excellent online safety metasites that other nations have developed. The Australian government has established www.NetAlert.net, which serves as a model that other governments could seek to emulate. Europe's www.BeSafeOnline.org is another excellent online safety meta-site.

If policymakers want to encourage more widespread awareness and adoption of parental control tools and online child safety methods, they will need to expand their current efforts considerably. As was the case with the public awareness campaigns discussed above, in addition to websites and online tips, a serious awareness campaign will need a variety of public service announcements and outreach efforts, brochures and banners, and other promotional campaigns. Perhaps most importantly, such a campaign must include state and local officials and agencies that can communicate the messages at the local level through various institutions (schools, libraries, law enforcement agencies, civic clubs, etc.) as well as nonprofit organizations, and even corporations and trade associations can assist in the effort.

Such an approach is embodied in a bill introduced by Rep. Melissa Bean (D-IL) entitled the "Safeguarding America's Families by Enhancing and Reorganizing New and Efficient Technologies Act of 2006," or "SAFER NET" Act (H.R. 1008). The measure seeks to better coordinate and expand online safety education and efforts at the federal level. Specifically, Rep. Bean's bill would do the following:[286]

- Create a new Office of Internet Safety and Public Awareness at the Federal Trade Commission that is explicitly responsible for improving public awareness and education about Internet safety. This office would be the primary federal contact on Internet safety, serving as a resource and clearinghouse for consumers, the industry, and other Internet safety initiatives. It would also work with other entities (federal, state, local, private) to reduce redundancy and to promote best practices for promoting and ensuring internet safety. The office would also report to Congress annually on the state of Internet safety, emerging threats, and the costs to the economy.

- Launch a national public awareness campaign to educate Americans about online threats and about how to best protect themselves and their families from becoming the victims of online predators, financial schemes, ID theft, and more.

- Authorize federal grants to support efforts to promote Internet safety conducted by qualifying entities, such as schools, nonprofit organizations, state and local governments, law enforcement agencies, and businesses.

This bill represents an admirable attempt to better coordinate and expand Internet safety education. Importantly, there is no reason that Rep. Bean's effort couldn't be expanded to mention other parental control technologies and methods for other types of media besides the Internet. Rep. Bean also deserves

[286] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h1008ih.txt.pdf

credit for taking her message "on the road" by hosting an ongoing series of town hall meetings in her district to discuss online safety with her constituents. Presumably, if the legislation she introduced were ever implemented, the new FTC Office of Internet Safety and Public Awareness could create briefing plans and materials for other lawmakers who want to emulate Rep. Bean's efforts to educate constituents. Officials from that office might be available to assist lawmakers or even accompany them on town hall speaking tours to discuss parental controls and online child safety.

Such an education-based approach has the added benefit of remaining within the boundaries of the Constitution and the First Amendment.

Such an education-based approach has the added benefit of remaining within the boundaries of the Constitution and the First Amendment because government would not be seeking to restrict speech, but simply to better inform and empower parents regarding the parental control tools and techniques already at their disposal. The courts have shown themselves to be amenable to such educational efforts. For example, in a recent decision striking down an Illinois law that sought to regulate video game sales to minors, the Seventh Circuit Court of Appeals noted that parents are already actively involved in making decisions about the games their children buy. Noting that the parents are involved in well over 83 percent of their children's video game purchases, the court goes on to argue that:

> If Illinois passed legislation which increased awareness of the ESRB [Entertainment Software Rating Board voluntary rating] system, perhaps through a wide media campaign, the already-high rate of parental involvement could only rise. Nothing in the record convinces us that this proposal would not be at least as effective as the proposed speech restrictions.[287]

This is why education, not regulation, represents the superior approach to address content concerns and online child safety. If Congress enacts more regulations aimed at banning certain types of websites or online content, those measures will be bogged down in the courts for years to come. For example, the Child Online Protection Act (COPA) was passed by Congress in 1998 in an effort to restrict minors' access to adult-oriented websites. Almost 10 years later, the legislation remains stuck in jurisprudential limbo after endless legal wrangling about the constitutionality of the measure. If all the money that has been spent

[287] *Entertainment Software Association v. Blagojevich*, 7th Cir. Court of Appeals, WL 3392078, November 27, 2006, p. 16, www.jenner.com/files/tbl_s18News/RelatedDocuments147/2652/Seventh_Circuit_ILVideoGame.pdf

litigating this case had instead been spent on media literacy and online safety campaigns, it could have produced concrete, lasting results.

C. Private or Industry-Led Consumer Education Efforts

It's worth noting that several major private or industry-led consumer education efforts are under way to help families learn more about parental controls, ratings systems and online child safety efforts. For example:

- **Television / Broadcasting:** TV Watch, a coalition of 27 prominent individuals and organizations representing more than four million Americans, sponsors initiatives such as the "1-2-3 Safe TV" tool kit for parents.[288] The group circulates materials that provide parents easy-to-understand primers on how to safeguard their children against objectionable content on television.[289] The effort was spearheaded by media operators such as CBS Corporation, News Corp., and NBC Universal but also includes groups as diverse as the American Conservative Union, the Black Filmmakers Foundation, Center for Creative Voices in Media, the Creative Coalition, the Minority Media and Telecommunications Council and the U.S. Chamber of Commerce.[290]
- **Cable Television:** The National Cable and Telecommunications Association (NCTA) sponsors a $250 million public service campaign called "Cable Puts You in Control."[291] As part of the effort, the industry airs numerous educational ads and distributes materials to subscribers. These materials are also made available to consumers via in-store displays as retailers such as Best Buy and Circuit City. The effort also includes an education website called Control Your TV[292] that offers a variety of educational links and videos showing parents how to block access to certain channels or programs that they might find objectionable. The cable industry also sponsors the impressive Cable in the Classroom media literacy program discussed in the previous section.
- **Television / Cross-Media:** At a January 19, 2006, Senate Commerce Committee hearing, Jack Valenti, the former CEO of the Motion Picture Association of America (MPAA), announced that all media companies that "make and dispatch visual programming" were launching a joint 18-month marketing campaign "to inform and persuade the American people that they have the power" to control the content that appears on their television

[288] www.televisionwatch.org
[289] *Safe TV. Easy as 1-2-3: The TV Watch Guide to the TV Ratings and Parental Controls,* TV Watch, http://www.televisionwatch.org/HelpForParents/default.html
[290] By way of full disclosure, I serve on the advisory board of TV Watch.
[291] www.ncta.com/pdf_files/Fact-Sheet-on-Cables-Pledge_PDF_4-27-05.pdf
[292] www.controlyourtv.org

screens.[293]

This unprecedented $300 million campaign includes participation from the Consumer Electronics Association (CEA); the National Association of Broadcasters (NAB); MPAA; NCTA; Viacom; Time Warner; television broadcast networks ABC, CBS, Fox, and NBC Universal; and satellite TV providers DirecTV and EchoStar's Dish Network. The Ad Council and various advertising agencies assisted in the effort to help craft "simple messages" that were then broadcast and cablecast by all these media providers over at least an 18-month period.[294] The televised ads began airing on local broadcast stations and the top 100 cable systems on July 26, 2006.[295] Parents were also able to see the ads, and find a great deal of other useful information, on an interactive Internet website that came out of this effort called "The TV Boss."[296]

- **Cross-Media:** The Pause-Parent-Play website offers an excellent compendium of websites and services that parents can use to learn more about the media their children might want to see, hear, or play.[297] The effort is sponsored by a diverse coalition of companies and associations, including: Wal-Mart, the Girl Scouts, the YMCA, Microsoft, Comcast, Time Warner, News Corp., the Electronic Software Association, Viacom, NBC Universal, MPAA and the Recording Industry Association of America (RIAA). The coalition's website features numerous links answering questions about how TV ratings and screening tools work (like the V-Chip and cable and satellite set-top boxes).[298] The links provided on the Pause-Parent-Play website help parents better understand how to use these and other technologies. There's also a "Get the Facts" section on the site that offers detailed explanations of how many of the current rating systems work.[299]

- **Cross-Media:** Take Parental Control is a public service website provided by Playboy Enterprises.[300] It features parental control fact sheets for a wide variety of media, including: television, cable, cell phones, video games and Internet surfing. The website also features a useful glossary of terms describing various technologies and parental control tools. Public service announcements are included as well.

---

[293] Jack Valenti, "A Plan to Communicate to Parents That They Have the Power to Control All TV Programs in Their Homes," Testimony before the Senate Commerce Committee, January 19, 2006, http://commerce.senate.gov/pdf/Jack%20Valenti%20Testimony.pdf

[294] "Industries Unite in Unprecedented Effort to Educate Parents That They Have the Tools to Control TV Programming in Their Home," National Association of Broadcasters *Press Release*, January 19, 2006.

[295] Frank Ahrens, "TV Industry Unites on Viewer Education," *Washington Post*, July 25, 2006, p. D5; www.washingtonpost.com/wp-dyn/content/article/2006/07/24/AR2006072401197.html

[296] www.thetvboss.org

[297] http://pauseparentplay.org

[298] http://pauseparentplay.org/see/index.php#tv

[299] http://pauseparentplay.org/facts

[300] http://takeparentalcontrol.org

- **Video Games:** To supplement its other consumer awareness efforts described earlier, in November 2006 the Entertainment Software Rating Board (ESRB) announced an educational partnership with the Parents-Teacher Association (PTA) to "encourage and enable state and local PTAs to educate their community's parents about the [ESRB] ratings."[301] As part of this new educational campaign, 1.3 million brochures will be distributed to 26,000 PTAs nationwide in both English and Spanish. Additional online support and education will also be offered on both the ESRB and PTA websites. In December 2006, the ESRB also launched a nationwide television PSA campaign that encourages parents to use the video game ratings when buying games for their children. The spots were introduced at an event featuring Senators Hillary Clinton and Joe Lieberman.[302] The ESRB has also sponsored PSA campaigns featuring state attorneys general Mark Shurtleff of Utah and Thurbert Baker of Georgia.

- **Internet**: As mentioned in the section above on Internet tools, many helpful Net-filtering and safety technologies and services are highlighted on GetNetWise.org.[303] This site is comprehensive public service website sponsored by a wide array of Internet and computer companies, as well as a host of public interest organizations and parental and child activists.[304] The GetNetWise website offers a comprehensive "Online Safety Guide" and lengthy inventory of "Tools for Families" that can be custom-tailored to the needs and values of individual families.[305] Major corporate supporters include Dell, Microsoft, Verizon, Amazon.com, Yahoo!, AOL, AT&T, Comcast, Eathlink, Visa, Wells Fargo, and the RIAA. Key public interest organizations include the Center for Democracy and Technology, the American Library Association, the Children's Partnership, People for the American Way Foundation, the National Consumers League, Net Family News,[306] ProtectKids.com,[307] SafeKids.com,[308] and Wired Patrol.[309] Of course, GetNetWise is not the only online safety website that corporations support or cosponsor.

- **Internet**: Also mentioned in the Internet safety section above was Project Online Safety.com.[310] This collaborative online portal offers a directory of

---

[301] "PTA and ESRB Launch Nationwide Video Game Ratings Educational Partnership," Parent Teacher Association *Press Release*, November 15, 2006, www.pta.org/ne_press_release_detail_1163547309281.html

[302] "Senators Hillary Rodham Clinton and Joe Lieberman Join ESRB to Launch Nationwide Video Game Ratings TV PSA Campaign," Entertainment Software Rating Board *Press Release,* December 7, 2006, www.esrb.org/about/news/12072006.jsp

[303] www.GetNetWise.org

[304] http://kids.getnetwise.org

[305] See http://kids.getnetwise.org/safetyguide and http://kids.getnetwise.org/tools

[306] http://netfamilynews.org/index.shtml

[307] http://protectkids.com

[308] www.safekids.com

[309] www.wiredsafety.org

[310] www.projectonlinesafety.com

online safety tools and educational materials developed by technology companies, media organizations and nonprofits. Coalition members include: AT&T, BlogSafety.com, Cable in the Classroom, Charter, Comcast, Cox, Facebook, Fox Interactive Media (MySpace.com), the Internet Education Foundation, NCTA, Network Solutions, Qwest, Time Warner Cable and the National Center for Missing and Exploited Children (NCMEC). Each company provides an overview of its online safety efforts and links to various resources parents can use to keep their kids safe online or to educate them about online dangers. The coalition also provides support for PSAs on Internet safety.

- **Wireless:** As mentioned earlier, CTIA has also developed an awareness campaign called "Get Wise about Wireless," which "helps educate students about cell phone use and the responsible behaviors associated with using cell phones."[311] The program includes a variety of materials such as a teacher's guide and a family take-home pamphlet about safe and courteous cell phone use.[312] As part of this effort, CTIA also runs a student essay contest about sensible wireless use.[313]

D. A Voluntary Code of Conduct / Industry Pledge to Parents

The empowerment and education steps outlined in the preceding sections illustrate the impressive strides that industry and others have made to provide parents with the tools and information they need to protect their children from potentially objectionable content. But more can be done by industry to tie all these efforts together.

All modern media operators—broadcasters, cable and satellite operators, music providers, broadband providers, Internet service providers, search providers, web portals, social networking sites, game developers, online gaming services, and so on—need to take additional steps to show policymakers and the general public that they are serious about addressing concerns about access to objectionable content. If companies and trade associations do not step up to the plate and meet this challenge soon—and in a collective fashion—calls will only grow louder for increased government oversight or regulation.

One possibility that industry should consider is the adoption of a voluntary code of conduct.[314] This code of conduct, or set of industry "best practices," would be based on a straightforward set of principles and policies that could be

[311] www.wirelessfoundation.org/GetWise/index.cfm
[312] See www.wirelessfoundation.org/GetWise/teachers_guide2007.pdf and www.wirelessfoundation.org/GetWise/family_takehome2007.pdf
[313] www.wirelessfoundation.org/GetWise/contest.cfm
[314] This was originally proposed in: Adam Thierer, "Saving Online Free Speech: A Voluntary Code of Conduct for Internet Operators," Progress & Freedom Foundation *Progress Snapshot* 2.19, August 2006, www.pff.org/issues-pubs/ps/2006/ps_2.19_conduct_net_ops.pdf

universally adopted by the wide variety of operators mentioned above. These principles and policies, which could take the form of a pledge to parents and consumers, must also be workable throughout our new world of converged, cross-platform communications and media. Exhibit 40 outlines the basic elements of this voluntary "pledge."

For such a code of conduct to gain traction and be taken seriously, it will require the leadership of major online companies, digital media providers, and their respective trade associations. Such a commitment by these market leaders will help recruit smaller players while increasing credibility for the effort with policymakers, the public, and the press. Benchmarks will also be needed to evaluate the effectiveness of these efforts over time. Those evaluations can inform potential future adjustments to the voluntary code, especially as new services and technologies come online.

Two important caveats are in order. First, unlike previous industry "codes"—such as those pushed on the movie and comic book industry by government officials a half century ago—this code would not seek to delimit acceptable forms of speech or expression by those adopting it. Rather, the purpose here is to allow for the maximum amount of legal speech and expression while providing users with the information and tools needed to block or curtail the flow of potentially objectionable media content in their lives. Information and education lie at the core of this effort, not censorship.

Second, the creation of such a code would go a long way toward satisfying one of the leading criticisms of current industry policies or approaches: the lack of consistency or standardization. A voluntary code of conduct would have many similar elements and, hopefully, companies and trade associations might even work together to develop a common "look and feel" to their tools and systems. That being said, this code should not be considered a universal rating or filtering scheme that would replace all other systems. Ample room should remain for experimentation by those adopting such a code, especially for those who wish to provide more stringent controls to their users.

This process should not be viewed by industry actors as a burden, but rather as an opportunity to highlight the many steps each organization is already taking—or will commit to undertake in the near future—to address concerns about potentially objectionable media content and online child safety. By making a commitment to parents and consumers to help them get this job done in a unified and comprehensive manner, digital media providers and distributors will help head off the inevitable push for greater government involvement and regulation.

Exhibit 40: Digital Media Provider Voluntary Code of Conduct

We at (company or trade association name) pledge to take the following steps to help parents and all our customers or users create a better, safer online environment and modern media marketplace:

Pledge 1: When feasible, we will offer voluntary ratings or labels to provide clear information about proprietary content. For certain types of proprietary content, we will attempt to offer ratings or labels that clearly designate the nature of the content on the website or in the product. We will use machine-readable metadata tagging whenever possible to allow rating or labeling systems to be fully automated by the end user and work seamlessly across platforms and products. And where applicable, we will provide clear notices of the ratings, labels or other content descriptors on all content packaging or product and website promotions.

Pledge #2: We will offer parental controls or filters to help families block or control objectionable content. We will offer Internet filters, set-top box controls or other screening and blocking technologies to empower families to make decisions about the forms of content that are appropriate in their lives. Where applicable, we will also provide links or contact information for sites and services that provide additional assistance or types of controls.

Pledge #3: We will provide reasonable assistance to law enforcement in its effort to root out online threats or predators. We will cooperate with law enforcement officials who are conducting investigations into online crimes. Within reasonable bounds, we will preserve data necessary to help law enforcement officials track potential online criminals. On our websites, we will offer a link to the National Center for Missing and Exploited Children's (NCMEC) CyberTipline to allow users to report potential child pornography or abuse. Finally, when feasible, we will offer training assistance for law enforcement officials to help them better understand how to police and prosecute potential criminal activity online.

Pledge #4: We will offer various forms of education for parents, consumers and even children. On our website(s), we will provide clearly displayed links, buttons, or phone numbers (i.e., hotlines) for parental and child assistance. When possible, we will offer integrated "how-to" guides with all products or offer "out-of-the-box" setup guides to help users immediately enable parental controls and filters. We will also produce and widely circulate brochures or tip-sheets to help in this task. We will create or fund public service announcements or sponsor other parental and consumer education efforts to promote consumer awareness. Finally, we will craft clearly worded acceptable-use policies that lay out these policies and also make it clear what responsibilities that end users and parents must exercise for themselves and their own families.

In June 2007, the National Cable & Telecommunications Association (NCTA) announced that its members—which represent roughly 90 percent of all cable households nationwide—would adopt such an industry-wide code of conduct. Under the NCTA's new initiative, which is called "Cable Puts You in Control: PointSmart, ClickSafe," NCTA's member companies "pledge to help parents, families, customers and consumers create a better, safer online media environment and foster a better understanding and working knowledge of the digital media landscape."[315] The NCTA members pledge to offer parents an unprecedented level of assistance to help parents keep their children safe online. The commitments are in line with the model code of conduct outlined above.

The NCTA's efforts are being coordinated online through an impressive website (www.pointsmartclicksafe.org) that contains interactive tips, manuals, and public service announcements to assist and educate parents and children. The new effort complements two other important efforts that the cable industry has operated for several years and that were mentioned earlier: "Control Your TV.org"[316] and "Cable in the Classroom."[317] The "Control Your TV" initiative and website coordinates the cable industry's parental control efforts aimed at the video programming side of their business. And Cable in the Classroom is an impressive media literacy initiative that also provides broadband connectivity and educational programming to schools and libraries for classroom use.

The cable industry's new code of conduct illustrates how online operators can take parental controls and online child protection to the next level. The first order of business was creating parental control tools and making them widely available. After that, companies and trade associations need to concentrate on boosting awareness about those tools and making them even easier to use. That is what the NCTA is doing with its new initiative.

All modern media operators need to take additional steps to show policymakers and the general public that they are serious about addressing concerns about access to objectionable content.

In addition, the focus on consumer education and media literacy that pervades the cable pledge is vitally important. This new "PointSmart, ClickSafe" initiative as well as the Cable in the Classroom project serve as models for what other companies or industries could do if they wanted to get more serious about promoting media literacy and online safety education.

---

[315] www.pointsmartclicksafe.org
[316] http://controlyourtv.org
[317] www.ncta.com/ContentView.aspx?contentId=2695

Exhibit 41:
NCTA's "Point Smart. Click Safe" website
(www.pointsmartclicksafe.org)

V. Getting Serious about Online Child Abuse

A. Putting the Problem in Perspective

This section will discuss online child safety and the specific threat posed by cyber-predators. These are issues of great concern for parents and policymakers today, and these concerns have prompted recent calls for drastic regulatory mandates like age verification of minors before they go online, or extensive data retention requirements for Internet service providers and other websites. This section will argue that there are better ways to address these concerns.

A National Child Abduction Epidemic?

Debates about online child safety are often driven by fear—fear of bad guys lurking online and waiting to snatch up our children. Indeed, there have been a handful of highly publicized cases of minors being contacted and later abducted or abused by child predators on social networking sites.[318] Such cases do not mean that a national epidemic of Internet-related child abductions is occurring, however.

Debates about online child safety are often driven by fear—fear of bad guys lurking online and waiting to snatch up our children.

Generally speaking, abductions by strangers "represent an extremely small portion of all missing children [cases]." That conclusion was a central finding of the 2002 *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children* (NISMART), a study conducted by the Department of Justice's Office of Juvenile Justice and Delinquency Prevention.[319] Although the survey is several years old and suffers from some data and methodological deficiencies, it remains the most comprehensive survey of missing and abducted children in the United States.

The NISMART survey broke down juvenile abductions into two categories—family versus non-family. It found that the vast majority of kidnapping victims were abducted by family, friends of the family, or people who had a close relationships with (or the trust of) the minors. Only 115 of the estimated 260,000 abductions—or less than a tenth of a percent—fit the stereotypical abduction scenario that parents most fear: complete strangers snatching children and

[318] Claire Osborn, "Teen, Mom Sue MySpace.com for $30 Million," *Austin American-Statesman*, June 20, 2006.

[319] Andrea J. Sedlak, David Finkelhor, Heather Hammer, and Dana J. Schultz, "National Estimate of Missing Children: An Overview," *National Incidence Studies of Missing, Abducted, Runaway, and Thrownaway Children* (NISMART), October 2002, p. 7, www.missingkids.com/en_US/documents/nismart2_overview.pdf

transporting them miles away.[320] Despite that finding, public policy debates and media reports remain preoccupied with the horror stories about abductions by random strangers, leaving the impression that the problem is much larger than the more serious issues of family or acquaintance abductions.[321]

Research has shown that this conclusion is also true of child abuse and sex offenders in general, not just abductions. As psychologist Anna C. Salter, author of *Predators: Pedophiles, Rapists, and Other Sex Offenders*, points out, "[Sex offenders] are part of our communities, part of our network of friends, worse yet, sometimes part of our families."[322] And former FBI special agent Kenneth V. Lanning, author of *Child Molesters: A Behavior Analysis*, notes the following:

> The often forgotten piece in the puzzle of the sexual victimization of children is acquaintance molestation. This seems to be the most difficult manifestation of the problem for society and the law to face. People seem more willing to accept a sinister stranger from a different location or father/stepfather from a different socioeconomic background as a child molester than a clergy member, next-door neighbor, law-enforcement officer, pediatrician, teacher, or volunteer with direct access to children. The acquaintance molester, by definition, is one of us. He is not just an external threat. We cannot easily distinguish him from us or identify him by physical traits. These kinds of molesters have always existed, but society and the criminal-justice system have been reluctant to accept the reality of these cases.[323]

---

[320] A recent study of cases about missing children in Ohio revealed a similar trend. Of the 11,074 documented missing child cases in 2005, just 5 involved abduction by strangers compared with 146 abductions by family members. *2005 Annual Report,* Ohio Missing Children Clearinghouse, p. 4; www.ag.state.oh.us/victim/pubs/2005ann_rept_mcc.pdf

[321] Indeed, one recent study suggests that perception has replaced reality in the minds of many in the press and general public, who have increasingly come to believe that stranger abductions account for most missing child incidents. A 2006 analysis of *New York Times* articles about kidnappings, by Glenn W. Muschert, Melissa Young-Spillers, and Dawn Carr in the *Justice Policy Journal*, argued that "the *Times* disproportionately focuses on stereotypical kidnapping incidents, while social science data suggest that familial abductions are far more prevalent." And abduction estimates made by some activists were also "highly exaggerated," they found. Unsurprisingly, for those reasons, the authors note that various public opinion polls have revealed that most people believed that abductions by strangers accounted for most missing child cases even though the exact opposite was true. Glenn W. Muschert, Melissa Young-Spillers, and Dawn Carr, *Justice Policy Journal*, vol. 3, no. 2, Fall 2006, pp. 4-6.

[322] "Sex offenders only very rarely sneak into a house in the middle of the night. More often they come through the front door in the day, as friends and neighbors, as Boy Scout leaders, priests, principals, teachers, doctors, and coaches. They are invited into our homes time after time, and we give them permission to take our children on the overnight camping trip, the basketball game, or down to the Salvation Army post for youth activities." Anna C. Salter, *Predators: Pedophiles, Rapists, and Other Sex Offenders* (New York: Basic Books, 2003), p. 5, 76.

[323] Kenneth V. Lanning, *Child Molesters: A Behavior Analysis*, National Center for Missing & Exploited Children, 2001, www.missingkids.com/missingkids/servlet/ResourceServlet?LanguageCountry=en_US&PageId=469

Clearly, the problem of family and acquaintance abductions and sex abuse predated the rise of the Internet, and it will unlikely be diminished by age verification of minors on social networking websites or other websites. But the argument could be made that abductions by strangers—while exceedingly rare—could be reduced even further by age-verifying minors or adults before they enter certain sites.

This potential reduction may be true, but it is important to remember that predators can't magically reach through a computer screen and grab our kids. Predators must meet them somewhere in the physical world (i.e., a mall, park, playground, etc.). The danger of the Internet is that it allows predators to groom minors over a protracted period, while doing so *from a distance*. But the fact that they are doing so from a distance—and over electronic communications networks, no less—means that we have actually gained some important advantages in our effort to combat child predation. Many of the predators leave digital tracks for us to follow. Thus, to the extent that disturbing things are happening online or being facilitated by the Internet in any fashion, at least there is a digital record of those activities or crimes. The electronic tracks have made it easier to recover children or to track perpetrators on many occasions.[324]

It is important to remember that predators can't magically reach through a computer screen and grab our kids.

Of course, digital records have also made it easier to catch minors engaging in foolish behavior after they post information or photos about their actions online.[325] In past generations, parents often warned their kids to behave themselves in public or else "it will go down on your permanent record." It was largely just a scare tactic, because there really was no permanent record of the mundane activities of youth. Today, however—for better or for worse—*the Internet is becoming "your permanent record."* No doubt, this raises some serious, long-term privacy concerns. But the one positive aspect is that the existence of electronic records makes it easier for parents, website operators, or law enforcement officials to deal with online troublemakers of all varieties.[326] (As will be discussed at greater length below, that is why education is essential to

[324] See Mark Sherman, "Chat Rooms Help FBI Hunt for Pedophiles," *USA Today*, May 15, 2006, www.usatoday.com/tech/news/2006-05-15-fbi-chat-rooms_x.htm

[325] Wendy Davis, "Teens' Online Postings Are New Tool for Police," *Boston Globe,* May 15, 2006, www.boston.com/news/nation/articles/2006/05/15/teens_online_postings_are_new_tool_for_police; Andrew L. Wang, "Teen Blog Watch is On," *Chicago Tribune*, May 23, 2006.

[326] Eric Tucker, "Police Departments Turning to YouTube to Catch Suspects," *Boston Globe,* February 24, 2007, www.boston.com/news/local/rhode_island/articles/2007/02/24/police_departments_turning_to_youtube_to_catch_suspects

make sure both kids and their parents understand that serious consequences are associated with what they post online.)

"At-Risk" Youth are the Real Concern

Not only is it a myth that there is a growing epidemic of Internet-facilitated child abductions, but it is also a myth that all children are equally susceptible to falling prey to online predators. In reality, the population of "at-risk" youngsters who are most likely to become the victim of online predators is very small.

A 2004 study by researchers from the University of New Hampshire's Crimes Against Children Research Center surveyed more than 2,500 cases in which juveniles became the victims of sex crimes by people they met through the Internet.[327] The authors found that those children—almost all of whom were teenagers—were not, generally speaking, the victims of the stereotypical scenario that most parents and policymakers fear: "strangers who are pedophiles and who deceive and lure children, frequently over long distances, into situations where they can be forcibly abducted or sexually assaulted."[328] In fact, the opposite was the case.

Not only is it a myth that there is a growing epidemic of Internet-facilitated child abductions, but it is also a myth that all children are equally susceptible to falling prey to online predators.

The study found that "although they undoubtedly manipulated juveniles in a variety of ways, the offenders in the Internet-initiated crimes did not generally deceive victims about being older adults who were interested in sexual relationships. Victims usually knew this propensity before their first face-to-face encounters with offenders."[329] The survey results supporting this finding are startling:

- Only 5% of the adult offenders lied about their age and tried to pass themselves off as being minors.
- Only 21% of the adult offenders lied about their sexual desires with the minor.

Yet, despite the fact that most offenders did not hide their desires:

- The great majority of victims (83%) who met with offenders face-to-face voluntarily went somewhere with them afterward (a hotel,

[327] Janis Wolak, David Finkelhor, and Kimberly Mitchell, "Internet-initiated Sex Crimes against Minors: Implications for Prevention Based on Findings from a National Study, *Journal of Adolescent Health*, vol. 35, no. 5, 2004, pp. 11-20, www.unh.edu/ccrc/pdf/CV71.pdf
[328] *Ibid.,* p. 18.
[329] *Ibid.*

movie, restaurant, etc.), and many (41%) spent at least one night with the offender.

- Most victims (73%) willingly met with offenders more than once.
- In 89% of the cases, the victims willingly engaged in some sort of sexual activity with the offender; only 5% of the cases involved violence or rape.

That those children would consent to meet with older strangers and engage in such acts is shocking and disturbing, and most parents would find it unfathomable that their own children would voluntarily involve themselves with older men in this fashion. But therein lies the real problem. The researchers in this study found that most youngsters involved in those cases did not have a good relationship with their parents. In many cases, the victims reported a high degree of conflict with their parents or very little parental interaction and mentoring. In some cases, parents were absent from the home altogether. Loneliness and depression were also prevalent traits in many of the youngsters. And some of the boys who became willing victims were "gay or questioning" about their sexuality and were scared to talk to their parents or educators about it.

Those children are at-risk youth who need help. What they most need is love and understanding. When they cannot get them because of parental estrangement or incompetence, it is not surprising that some will look elsewhere for acceptance. As Nancy E. Willard, author of *Cyber-Safe Kids, Cyber-Savvy Teens* notes:

Educators, health officials, and other organizations need to devise better strategies for assisting at-risk youth.

> All humans crave companionship and acceptance. Children who, for whatever reason, do not have healthy relationships and do not feel accepted in the "real world" will be inclined to seek out online connections and communities in which they feel accepted. And this can lead to greater danger online.[330]

Although the Internet and social networking websites provide them with one potential way of finding help or building rewarding friendships, the danger exists that they might be so desperate for such acceptance that they would even seek it from some older strangers who might want to befriend them only to satisfy perverted sexual desires.

[330] Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), p. 155-6.

But it would be wrong to assume that *all* youth share those same problems or would voluntarily meet—or engage in sexual activity with—an older man. Rather, only a handful of at-risk youth give rise to this problem. And even if we could find an effective way for all Internet sites to age-verify their users, many of these at-risk youth would likely still seek out acceptance from older figures using alternative means. Indeed, 79 percent of the victims in the study mentioned earlier were also contacted by the offenders by telephone, and almost 20 percent received correspondence by traditional mail. But no one would seriously consider trying to solve such a problem by age-verifying minors before they use phones or send letters.

Educators, health officials, and other organizations need to devise better strategies for assisting such at-risk youth. The first step is finding them. Again, this step is where the Internet and social networking sites actually *help* solve problems. For example, John Draper, director of the National Suicide Prevention Lifeline,[331] has said that referrals from MySpace.com users have become the largest source of calls to the hotline. He says that some kids are increasingly using their social networking profiles "to in some way convey that they had suicidal intent. There is very much the potential for saving lives because the first people to hear about kids at risk are other kids."[332] In fact, the organization has recently established its own MySpace profile to enable easier reporting of problems.[333]

Another independent MySpace suicide prevention site—"SOS" (Students Overcoming Suicide)—aims "to prevent and raise awareness about teenage suicide in the place where teens are most reachable; schools... Through SOS, our goal is to reach out to those in need, and offer hope to those who would otherwise have nowhere else to turn. In doing so, we want to show that nobody is truly alone in this world, no matter how bad it may seem. SOS aims to bring teens together in an attempt to unite and overcome feelings of despair, isolation, and hopelessness." [334]

Many other examples of peers assisting other at-risk peers can be found on social networking sites. On MySpace.com alone, notable examples include: "Helping Teens,"[335] "Teens Helping Teens,"[336] and the "Teen Support Alliance,"[337] all of which let youth counsel each other or suggest places where others might find help.

---

[331] www.suicidepreventionlifeline.org
[332] Quoted in Larry Magid and Anne Collier, *MySpace Unraveled: A Parent's Guide to Teen Social Networking* (Berkeley, CA: Peachtree Press, 2007), p. 174.
[333] www.myspace.com/suicidepreventionlifeline
[334] www.myspace.com/studentsovercomingsuicide
[335] www.myspace.com/helpingteens
[336] www.myspace.com/whymeteenshelpingteens
[337] http://groups.myspace.com/Teensupportalliance

Teens Soliciting Teens

In this debate, much is also made of a statistic culled from the second Youth Internet Safety Survey (YISS-2) from the National Center for Missing and Exploited Children, which found that one out of every seven (13%) children has received a sexual solicitation while online.[338] Although this figure represents a decline from the 1-in-5 (19%) finding from the first survey (YISS-1), it's still a disturbing number.

Importantly, however, the YISS survey noted that a significant percentage of those "solicitations" are kids talking to other kids. In other words, when 17-year-old Johnny propositions 16-year-old Jenny, it counts as a "solicitation." Of course, teens were delivering salacious solicitations to each other long before the Internet came along, but parents had no way to track sexual solicitations unless they found a dirty note in a schoolbag or pants pocket.

Perfect age verification is a quixotic objective and the pursuit of it could create a false sense of security for both parents and children.

This reality is not to condone the rude and raunchy behavior that some teens engage in, but we need to be realistic about the issue and to understand that, in a certain sense, this problem has always been with us. It's just more visible to us now. For the first time, we are measuring things that were previous unmeasured or unmeasurable. Regardless, teens trash-talking to other teens is a problem that will not disappear with the regulation of the Internet or the imposition of age verification on social networking sites.

B. Wrong Solution: Mandatory Age Verification

Many policymakers are advocating mandatory age verification of minors as a potential solution to some of the concerns expressed above.[339] In particular, many state attorneys general (AGs) are demanding that social networking websites such as MySpace, Facebook, Xanga, and others verify the age of their users before they are allowed on such sites.[340]

---

[338] Janis Wolak, Kimberly Mitchell, and David Finkelhor, *Online Victimization: Five Years Later*, National Center for Missing and Exploited Children, 2006, www.missingkids.com/en_US/publications/NC167.pdf

[339] This section is condensed from a much longer study on the issue I published in March 2007. See Adam Thierer, "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," Progress & Freedom Foundation *Progress on Point* 14.5, March 21, 2007, www.pff.org/issues-pubs/pops/pop14.5ageverification.pdf

[340] Emily Steel and Julia Angwin, "MySpace Receives More Pressure to Limit Children's Access to Site," *Wall Street Journal*, June 23, 2006, http://online.wsj.com/public/article/SB115102268445288250-YRxkt0rTsyyf1QiQf2EPBYSf7iU_20070624.html?mod=tff_main_tff_top

That is unfortunate because, as will be shown below, perfect age verification is a quixotic objective and the pursuit of it could create a false sense of security for both parents and children. It is also important that lawmakers do nothing that could force mainstream, domestic social networking sites offshore or, even worse, that could drive the users we are trying to protect to offshore sites. Whatever their concerns are about current domestic sites, parents and policymakers should understand that those sites are generally more accountable and visible than offshore sites over which we have virtually no influence but that have the same reach as domestic sites.

The Complexities of Human Identification

Generally speaking, the problem that age verification is supposed to solve is to keep older people away from youngsters, at least in certain circumstances. Also, some proponents wish to use age verification to ban preteen access to social networking sites. To accomplish either of those objectives, we must be able to effectively verify everyone's age by consulting reliable records about those looking to create an account on a social networking site. In other words, when Janie Smith comes to a social networking site for the first time, the site must be able to verify not only that she is Janie Smith, but that she really is as old as she claims to be. But this verification is easier said than done.

Whatever their concerns are about current domestic sites, parents and policymakers should understand that those sites are generally more accountable and visible than offshore sites.

Consider first what is required to verify an *adult's* identity. When government officials or even corporations seek to verify someone's identify or age, they can rely on birth certificates, Social Security numbers, driver's licenses, military records, home mortgages, car loans, other credit records, or credit cards.

But even with all those pieces of information, challenges remain. Is the information publicly accessible or restricted by legal or other means? Are all the underlying pieces of information and documentation trustworthy, or have they been manipulated or misreported in some way? Has someone faked his or her identity? And so on. Thus, while the identity authentication systems—both public and private—have improved significantly in recent decades, they still face some inherent challenges and concerns about fraud.[341]

The current concern about "identity theft" demonstrates the complexities and level of difficulty involved in stamping out this problem. Even U.S. passports, which are relatively robust identification documents that contain authentication

[341] For a comprehensive discussion of such matters, see Jim Harper, *Identity Crisis: How Identification Is Overused and Misunderstood* (Washington, DC: Cato Institute, 2006).

data, are occasionally forged with success. "It is safe to assume that future age verification efforts will yield failures on par with other identification/authentication mechanisms," says information security expert Jeff Schmidt, CEO of Authis, Inc.[342] "When one considers how frequently college students successfully circumvent age verification requirements in person and with government issued documents, one can begin to grasp the challenges that lie ahead."[343]

Importantly, we're talking just about adults here. When the focus of identity verification efforts shifts to minors, the endeavor becomes far more complicated. Minors don't have home mortgages or car loans. They don't have military records and most have never worked. Most don't have driver's licenses or credit cards either.

When the focus of identity verification efforts shifts to minors, the endeavor becomes far more complicated.

Of course, minors do have birth certificates, Social Security numbers, and school records, but both parents and government officials have long demanded that access to those records be tightly guarded. That's for a very good reason: As a society, we take privacy seriously—especially the privacy of our children. Laws and regulations have been implemented that shield such records from public use, including the Family Educational Rights and Privacy Act of 1974 and various state statutes.[344]

Also, to the extent that age verification of adults works for some websites—online dating services, for example—it is important to realize that in most of those cases *the users want to be verified.* In that context, identify authentication increases marketability of a user's "profile," or it allows him or her to participate more actively in an environment where trust is essential. This fact makes it far more likely that age verification will work because user compliance is driven by market forces, not regulation. That compliance will not be the case when users—especially kids—inherently resist the idea of being age-verified before they go onto certain websites. (We should also not forget that some kids will share their online credentials or passwords with friends.)

It is also important to realize that age verification and background checks are not synonymous. Information security expert John J. Cardillo, president and CEO of Sentinel, a leading authentication firm, argues that:

> Most people are ignorant of what we do. They hear the words "check" or "verification" and they assume a full background check will be run on the individual. When this is sponsored by an AG, the chief law enforcement officer of their state, there's a perception that the criminal background

[342] Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.
[343] Ibid.
[344] www.ed.gov/policy/gen/guid/fpco/ferpa/index.html

> checks are inclusive in whatever they're proposing. Age verification, on its own, doesn't indicate whether or not a person is a convicted sex offender. Mandated age verification, as proposed, would allow the hundreds of thousands of offenders … who are over 18, unrestricted access to sites. Worse, it would allow these offenders the ability to vouch for children that might or might not exist. This is where it gets most dangerous. People might assume that "verified" users have undergone some type of vetting, and let their guard down just that little bit the offenders need to exploit. In the case of convicted sex offenders, age verification actually helps them by giving them an additional layer of legitimacy.[345]

Again, this points to the danger of creating a false sense of security online by mandating a solution that doesn't address the real problem.

Finally, the special challenges raised by the nature of the Internet and online communication must be reiterated. Finding a dependable source of identity or age information and then reliably matching it to someone thousands of miles away on the Internet (perhaps in another jurisdiction, or even another country) is a daunting challenge—made even more difficult by the fact that a remote individual may be actively attempting to subvert the age verification process. Solving this problem necessitates authentication data that are appropriate for online interaction. In the real world, we perform in-person authentication with a photo or physical description; the online world requires a username / password combination, biometric authenticator, or physical security token. An arms-race scenario is obviously at work here, and because a perfect solution is impossible, we must guard against a false sense of security. Lastly, because technology is evolving at such a rapid pace in this area, there is a risk that legislative solutions will become obsolete very rapidly.

Credit cards are often viewed by policymakers as the silver bullet solution for age verification. But they are not a silver bullet.

Why Credit Cards Won't Work

Although there are many potential variations of age verification, the leading varieties mentioned in these debates are credit card authorizations and parental permission-based systems of authentication. Unfortunately, both methods have serious flaws and drawbacks.

Credit cards are often viewed by policymakers as the silver bullet solution for age verification. Even though credit card companies typically do not wish their cards to be used as age verification tools, government has advocated their use in that way in the past. But they are not a silver bullet.

[345] John J. Cardillo, e-mail conversation on file with author, March 11, 2007.

"Mere possession of a credit card is not a reliable assertion of identity or age," argues Jeff Schmidt of Authis.[346] Credit cards can be a rough proxy for age on the assumption that only adults over the age of 18 have credit cards, but that assumption is false. Many minors are given credit cards by their parents. Youngsters can borrow or steal credit cards from their parents or others. And Schmidt notes that newly created stored value cards, specifically marketed for use by children, "are in many cases indistinguishable from actual credit cards—both in physical appearance and in the back-end transaction processing systems."[347] Sentinel's John Cardillo points out additional reasons why credit cards are not effective age verification tools:

> When a card is used for verification purposes, an authorization on that card is run for $1.00 (or less), however a charge isn't put through. The card typically isn't reconciled against any database for name and/or age, nor is a signature checked. Because of the insignificant dollar amount, the only thing that's checked for security purposes, in some instances, is zip code. Anyone who's ever bought gasoline with a credit card knows this to be true. Our names and ages aren't checked at the pump. Check your statement online next time you gas up. You'll see an authorization for $1.00 and the actual charge a few days later. The same merchant banks handle the transactions online. In other words, in most cases, all that's being verified is that the card account isn't closed or stolen. Who's using it is irrelevant.[348]

Moreover, "many parents may feel uncomfortable giving their credit card number online at children's Web sites where there is no transaction involved,"[349] noted a joint filing by a coalition of major commercial organizations, including the American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, the Direct Marketing Association, Inc., and Magazine Publishers of America. In a June 2005 filing to the Federal Trade Commission, these organizations noted that "in light of current online scams, heightened concerns about online security, and the rise of such practices as phishing, parents may be reluctant to provide credit card numbers absent a transaction."[350] But that begs the question: If lawmakers required social networking sites to process a credit card transaction to age-verify, is that fair? In particular, is it fair for low-income families? And what about those families that do not possess a credit card?

---

[346] Jeff Schmidt, e-mail conversation on file with author, February 19, 2007.
[347] *Ibid*.
[348] John J. Cardillo, e-mail conversation on file with author, March 11, 2007.
[349] American Advertising Federation, American Association of Advertising Agencies, Association of National Advertisers, the Direct Marketing Association, Inc., and Magazine Publishers of America, Filing in COPPA Rule Review 2005, June 27, 2005, p. 5.
[350] Ibid.

Finally, the law is not even settled about using credit cards for access to adult-oriented websites. Congress passed the Child Online Protection Act (COPA) in 1998 in an effort to restrict minors' access to adult-oriented websites. The measure provided an affirmative defense to prosecution if a website operator could show that it had made a good-faith effort to restrict site access by requiring a credit card, adult personal identification number, or some other type of age-verifying certificate or technology. But the legislation was immediately challenged and has gone to the Supreme Court for review *twice*. And the law is still being debated in a lower court. Thus, almost 10 years after its initial passage, the legislation remains stuck in jurisprudential limbo after endless legal wrangling about its constitutionality.

Because websites are far away from the parents, how is the site operator going to ensure that the person vouching for the child's age is really the parent or even an adult?

Incidentally, COPA established an expert Commission on Online Child Protection to study methods for reducing access by minors to harmful material on the Internet. As part of its final report, the COPA commission said that credit card-based age verification would be completely inappropriate for instant messaging and chat, which were the precursors of social networking. The commission found: "This system's limitations include the fact that some children have access to credit cards, and it is unclear how this system would apply to sites outside the U.S. It is not effective at blocking access to chat, newsgroups, or instant messaging."[351]

Parents Vouching for Minors

In 2007, legislation was introduced in Georgia, North Carolina,[352] and Connecticut[353] that would require social networking sites not only to obtain parental approval but also to take steps to verify that they are the actual parents of the child. For example, the Georgia bill would make it illegal for a minor to maintain an account or webpage on a social networking site "without the permission of the minor's parent or guardian and without providing such parent or guardian access to such profile web page."[354]

This approach will appeal to many because it can be likened to a parent signing a "permission slip" for a child. Unfortunately, parental permission-based approaches are more complicated for online activities. Because websites are far

[351] Commission on Online Child Protection, Final Report, October 20, 2000, www.copacommission.org/report/ageverification.shtml. Also see Computer Science and Telecommunications Board, National Research Council, *Youth, Pornography, and the Internet,* (Washington, DC: National Academy Press, 2002), pp. 206-9, 339-49.
[352] www.ncleg.net/Sessions/2007/Bills/Senate/HTML/S132v0.html
[353] Susan Haigh, "Conn. Bill Would Force MySpace Age Check ," *Yahoo News.com*, March 7, 2007, www.msnbc.msn.com/id/17502005
[354] www.legis.ga.gov/legis/2007_08/fulltext/sb59.htm

away from the parents, how is the site operator going to ensure that the person vouching for the child's age is really the parent or even an adult? Would the verifier mail or fax notarized documents? Those documents can be forged, of course. Mandatory follow-up phone calls would be cumbersome, costly, and potentially viewed as intrusive. And the use of credit cards to satisfy the permission requirement might raise some of the same problems already discussed.

Despite these potential drawbacks, this was the general framework established by the Children's Online Privacy Protection Act (COPPA) of 1998, which required websites that marketed to children under the age of 13 to get "verifiable parental consent" before allowing children access to their sites. The Federal Trade Commission (FTC), which is responsible for enforcing COPPA, adopted a so-called sliding scale approach to obtaining parental consent. The sliding scale approach allows website operators to use a variety of the methods described above to comply with the law. The FTC also authorized four "safe harbor" programs operated by private companies that help website operators comply with COPPA.[355]

Because users would sacrifice a great deal of autonomy and functionality once online, many would likely rebel against the system or would seek to subvert it in some fashion.

In a recent report to Congress, the FTC argued that no changes to COPPA were necessary at this time because it had "been effective in helping to protect the privacy and safety of young children online."[356] In discussing the effectiveness of the sliding scale methods, however, the agency also found that "none of these mechanisms is foolproof" and that "age verification technologies have not kept pace with other developments, and are not currently available as a substitute for other screening mechanisms."[357]

One of the problems associated with COPPA is that "Children quickly learned to lie about their age in order to gain access to the interactive features on their favorite sites," notes Denise G. Tayloe, CEO of Privo, Inc., one of the four FTC-approved safe harbor programs.[358] "As a result, databases have become tainted with inaccurate information and chaos seems to be king where COPPA is

[355] The programs are administered by: the Children's Advertising Review Unit of the Council of Better Business Bureaus (CARU); the Entertainment Software Rating Board (ESRB); TRUSTe; and Privo.

[356] Federal Trade Commission, *Implementing the Children's Online Privacy Protection Act: A Report to Congress,* February 2007, p. 1, www.ftc.gov/reports/coppa/07COPPA_Report_to_Congress.pdf

[357] *Ibid.*, p. 12-13.

[358] Denise Tayloe, "It's Time to Comply with COPPA," *Privacy Advisor,* vol. 6, no. 10, October 2006, p. 5.

concerned," she says.[359] Nonetheless, Tayloe argues that, despite these flaws, COPPA is important. Even though "there is no perfect solution" and it is not possible to completely "stop a child from lying and putting themselves at risk," Tayloe points out that the law "provides a platform to educate parents and kids about privacy."[360] Of course, providing a platform to educate parents and kids is important, but it is not necessarily synonymous with strict age verification.

Nonetheless, these permission-based verification schemes might work for smaller, closed online communities in which the kids and parents are willing to take the time (and expense) to undertake extensive authentication. For example, smaller social networking sites such as ZoeysRoom.com, Imbee.com, ClubPenguin.com, and Tweenland.com have extremely strict enlistment policies, primarily because they target or allow younger users. As Sue Shellenbarger of the *Wall Street Journal* explains:

> The under-16 sites pose few of the hazards linked to networking sites for older people. The activities range from chats and blogging to creating virtual pets or characters and acting out roles in virtual cities. For a child to register, the sites typically require a parent's email permission, a parental signature on a permission form, or a parent's credit card verification. Some limit young children's interchanges to drop down menus of preapproved words and phrases. Most filter content for inappropriate material and employ live adult monitors who ensure that kids' conversations don't stray off course. Some limit chats or blog access to participants who are already preapproved and already known to a child's family.[361]

Ironically, one can probably safely assume that the kids using such services are not in the high-risk group discussed earlier. The parents who use such services are probably doing a fine job of mentoring their kids and don't really need to resort to such restrictive solutions. Nonetheless, such highly restrictive "walled garden" approaches do provide parents with greater ease of mind. That's not necessarily because of the strict enlistment policies so much as the extreme limitations on what kids can do on those sites or with whom they can communicate while online.

Regardless of how well the above schemes work in practice for these smaller, more closed online communities—and some experts do question how

---

[359] Tayloe, *Ibid*. Others have confirmed that this is taking place. Parry Aftab of Wired Safety notes that "Preteens quickly learned that if they say they are under thirteen they will be prohibited from using many sites. So they regularly lie about their age everywhere online." Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 5, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf

[360] Denise Tayloe, e-mail conversation on file with author, March 15, 2007.

[361] Sue Shellenbarger, "How Young is Too Young When a Child Wants to Join the MySpace Set?" *Wall Street Journal*, October 19, 2006, p. D1.

well they actually work[362]—such solutions lack scalability. Schemes that demand laborious and expensive enrollment requirements, or that greatly limit functionality and interactivity after users sign up, will almost certainly not work for larger social networking sites with a massive community of users. The administrative burdens would be significant for both site operators and parents alike. For example, Parry Aftab of Wired Safety notes that COPPA has made it much more difficult for some smaller website operators to stay afloat. "The cost of obtaining verifiable parental consent for interactive communications is very high, estimated at more than $45 per child, and even at that price [consent is] difficult to obtain."[363]

And because users would sacrifice a great deal of autonomy and functionality once online, many would likely rebel against the system or would seek to subvert it in some fashion. If such a system significantly slows or impedes the creation of new accounts for domestic social networking sites, it will create a perverse incentive for kids to seek other sites with less-restrictive policies, including offshore sites.

One can imagine other ways that parents could work together and use publicly available information about kids to credential them before they go online. But the scalability of those solutions will always likely limit their effectiveness.

C. Wrong Solution: Extensive Data Retention Mandates

Internet service providers, search engine providers, and many other interactive digital service providers and website operators routinely collect data about online activities. They use this information for a variety of purposes, but they usually do not release it publicly or to government officials. And much, if not all, of this information is eventually discarded.

---

[362] Internet security expert Cardillo argues that even these sites and schemes are vulnerable:

> During an analysis of the security processes of certain sites we tested Imbee's. Our security team was able to create several fake children. More troubling was the inconsistency of the information used to do so. We used a fake name for the parent, a different fake name created for the Yahoo! e-mail account used at registration, and my credit card info (because the name on the CC is irrelevant). Fictional child, and three fake identifiers on supposedly the same adult. Not one red flag was raised, and we were allowed onto the site without a problem. Our team was able to do this multiple times. Had we been a real bad guy, we could have, at any time, chatted with other kids on the site as a child. One of several different children actually. Not only isn't it a security solution, it's downright dangerous.
>
> Thus, the real bad guys out there intent on doing harm to children might still be able to exploit this sort of process. Because many predators have children of their own, they might use this approach to obtain an ID for their own kids and then go online under their child's name to prey on other children. But because they are "verified," a false sense of security now exists. Again, this is a major problem.

[363] Parry Aftab, Filing in COPPA Rule Review 2005, June 27, 2005, p. 2, www.ftc.gov/os/comments/COPPArulereview/516296-00021.pdf

Many lawmakers argue that data about subscribers or consumers should be retained for much longer periods to aid law enforcement efforts. State AGs and federal and state law enforcement officials are increasingly argue for extensive data retention mandates to better monitor online networks and websites for potentially criminal activity. These officials contend that such mandates will help them track child pornography or child predators as well as potential terrorist activities.

In 2006, members of Congress [364] and officials at the Justice Department[365] floated new proposals that would have required ISPs and others (including search engines and social networking sites) to retain data on their customers and traffic flows for long periods (typically between six months and three years, if not longer). These proposals mimic data retention laws that have been implemented in the European Union.[366]

The Two Sides

Let's step back and consider this issue from two very different perspectives. On one side, we have law enforcement officials telling us that data retention is an essential tool for tracking down bad guys (namely, terrorists and child predators) in our modern world of digital communications. In essence, imposing extensive record-keeping requirements on ISPs and others would create massive databases on end-user activities and traffic flows. Those records could later be searched to determine if criminal activity had been plotted or carried out. For example, who did Terrorist Suspect X communicate with over a two-year period? Or how many youngsters did Suspected Pedophile Y attempt to communicate with over the past year? And so on.

How much innocent activity or speech will be monitored by companies or the government during this process? How much information is being collected overall? Where is it all being stored? Is it secure?

On the other side, there are those who are concerned about ISPs becoming "watchdogs" that are essentially deputized by the state to police private networks for various activities.[367] Will the deputization of the middleman

[364] Declan McCullagh, "Congress May Consider Mandatory ISP Snooping," *CNET News.com*, April 28, 2006, http://news.com.com/Congress+may+consider+mandatory+ISP+snooping/2100-1028_3-6066608.html?tag=nl

[365] Declan McCullagh, "Gonzales Pressures ISPs on Data Retention," *CNET News.com*, May 26, 2006, http://news.com.com/2100-1028_3-6077654.html

[366] Jo Best, "Europe Passes Tough New Data Retention Laws," *CNET News.com*, December 14, 2005, http://news.com.com/Europe+passes+tough+new+data+retention+laws/2100-7350_3-5995089.html?tag=nl

[367] Declan McCullagh, "Your ISP as Net Watchdog," *CNET News.com*, June 16, 2005, http://news.com.com/Your+ISP+as+Net+watchdog/2100-1028_3-5748649.html?tag=nl

only require them only to assist in the pursuit of terrorists and child predators, or will it grow to encompass much more activity that government officials might want monitored? Even if it doesn't, how much innocent activity or speech will be monitored by companies or the government during this process? How much information is being collected overall? Where is it all being stored? Is it secure? And there are a host of other privacy-related concerns one could think of.

A Bit of Ancient History

To understand where the government is coming from and why it is asking for this authority, it is important to recall how this process worked in the past. Back in the days of a regulated communications monopoly, the monopolist (namely, AT&T) was willing to comply with whatever the government demanded on these matters because (a) cost recovery was possible or even guaranteed through rate-of-return regulatory proceedings, and (b) it was more commonly understood that this was part of the regulatory compact or *quid pro quo*. Indeed, if you go back and read cold war-era histories that incorporate a communications component, you will discover how AT&T bent over backward to cooperate with the feds on these matters. And it was an open secret that top AT&T engineers and government officials often worked together on network surveillance or data retention. (Indeed, AT&T officials would occssionally move in and out of government positions at the National Security Agency or other law enforcement or surveillance agencies).

It's unclear where companies would even store all the information that government wants them to collect.

But the world has changed since then and the communications industry has expanded to include more companies, sectors and technologies. Thus, even if the government can demand that telecom companies like AT&T, Qwest and Verizon to retain all the information government wants collected, how far does that really get them? What about Comcast, Time Warner, Cox, Google, Yahoo!, Microsoft, eBay, MySpace.,com, Facebook, Live Journal, and the countless other companies that move or retain data about users or customers? And what about offshore sites that carry Internet traffic?

A More Balanced Approach

In other words, government still wants to play the game the old way but now must contend with dozens (and potentially hundreds) of stakeholders instead of just one big communications monopoly. That is what makes this issue so challenging today. The government has legitimate national interests here, but that does not mean it should be able to impose massive unfunded mandates on everyone to accomplish those goals.

The better approach would be limited, targeted data *preservation* requirements. Specifically, the government should be able to ask an ISP (or any other Internet company) to retain data but:

(a) only through a well-established judicial subpoena process;

(b) only for specific individuals who officials have probable cause to believe are engaging in illegal activities (terrorism, child porn, etc.); and,

(c) only for a limited period (officials should seek additional subpoenas for extended data retention).

There is a world of difference between this sort of data preservation policy and the data retention mandates that many lawmakers are proposing today, which would require ISPs and other Internet companies to retain massive amounts of customer data for an extended period. Moreover, it's unclear where companies would even store all the information that government wants them to collect. After all, we're potentially talking about terabytes or even petabytes of daily data traffic flows that would have to be stored in server farms as tall as skyscrapers.

And that raises some serious concerns about who should have access to such data and how those parties would protect all that information from unauthorized uses. As John Morris, a lawyer with the Center for Democracy and Technology, notes, "If Congress were to require ISPs to retain extensive amounts of data, such databases would be gold mines for abuse, including unwanted marketing and identify theft." Morris argues that "a broad range of other prosecutors, divorce lawyers, advertising executives, and hackers would misuse the data."[368] John D. Ryan, chief counsel of compliance and investigations for AOL, points to additional concerns:

> [A] careful assessment of these proposals will show that they are in fact counterproductive and the efforts to create this massive and costly database will fall far short of its intended goal. Warehousing of data requires the allocation of enormous resources to maintain and secure that data. Those resources would be better focused on supporting law enforcement in the investigation of real-time active cases. Additionally, creating such a voluminous database will actually frustrate law enforcement's goal of locating and identifying the suspects they are pursuing. As databases grow in size and complexity the risk of data corruption increases as well. As a result, the possibility of not finding the requested information increases as does the potential for a false match.

[368] Quoted in "Are More Laws Needed to Protect Kids Online," *Wall Street Journal Online*, November 10, 2006, http://online.wsj.com/public/article/SB116299783252817209-lqXuBka9GdpFDf3LJtAdvnYbpfQ_20061209.html?mod=tff_main_tff_top

> Finally, even the best efforts at creating these massive databases are destined to fall short of their desired goal because they are easily circumvented. There are thousands of Internet access points that would not be covered by this data retention net, including universities and other academic institutions, libraries, governments, the military, employers, and tens of thousand of wireless hotspots. A determined predator need only utilize one of these services to avoid the net.[369]

Incidentally, almost everyone in the Internet and communications industry has already said they can live with the targeted data *preservation* approach outlined above. Indeed, companies already retain data upon request in this fashion. ISPs, social networking site operators, and most other Internet operators will retain data for as long as government wants if law enforcement officials come to them with a specific request about a problematic user. Federal law already requires Internet providers to retain data for up to 90 days upon request from law enforcement and also report any child pornography they discover to the National Center for Missing and Exploited Children so they can work with law enforcement officials to investigate. This is a much more sensible approach to the problem then the sort of blanket (and unfunded) data retention mandates that some lawmakers are currently proposing.

The best way to deal with concerns about online child safety is through a "3-E Solution," which stands for "education, empowerment, and enforcement."

D. Right Solutions: Education, Empowerment, and Enforcement

The best way to deal with concerns about online child safety is through a "3-E Solution," which stands for "education, empowerment, and enforcement."[370] The empowerment and education components have already been discussed extensively in previous sections of this report. But, to reiterate, it is essential that parents take steps to mentor and monitor their children as they enter the world of cyberspace. And industry should empower parents with more and better tools to help them do that job. But the tools discussed throughout Part III provide a great deal of assistance already.

As Part IV made clear, education is even more important. "You need to take a holistic approach" to such problems, notes Ron Teixeira, executive

[369] John D. Ryan, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites," Testimony before the House Committee on Commerce and Energy, Subcommittee on Oversight and Investigations, June 27, 2006, p. 6, http://energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Ryan.pdf

[370] Adam Thierer, "Child Protection and the Internet: The '3-E' Solution (Empower, Educate & Enforce)," Submission to the Advisory Committee of the Congressional Internet Caucus, 2006, www.netcaucus.org/books/childsafety2006/pff.pdf

director of the National Cyber Security Center."[371] Teixeira argues that it is essential that we drill basic lessons into our children—the digital equivalent of "don't take candy from strangers," for example—to ensure that they are prepared for whatever technologies or platforms follow social networking sites.[372] "Education is the way you teach children to be proactive, and that will stay with them forever," he rightly concludes.[373] As Parry Aftab of Wired Safety argues, it's about teaching our kids to "use the filter between their ears" and "make responsible decisions about their use of technology."[374] Critical thinking, in other words, is the best form of self-protection.

As will be discussed next, the final "E" in the 3-E Solution is enforcement, as in stepped up law enforcement efforts to find and adequately prosecute child predators.

Getting Sentencing Right

The most essential role that government has is to protect people from harm, especially helpless kids. It is not the job of private companies to enforce law and order or bring criminals to justice. That is the government's job. Unfortunately, our government isn't doing a very good job of it when it comes to online child safety.

Here is the sobering fact to consider: a 2003 Department of Justice study reported that the average sentence for child molesters was approximately seven years and, on average, they were released after serving just three of those seven years.[375] That is an extremely troubling statistic. If you have young children in your home, then it is even more upsetting. When our government is putting people who viciously hurt innocent children behind bars for just seven years and then letting them out after only three, then our government has failed us at a very fundamental level.

Worse yet, policymakers then point fingers at everyone else and scold Internet companies and ISPs for not doing enough to protect children from predators, all the while conveniently ignoring the government's own failed policies that allow those predators to be on the streets and behind keyboards in the first place. It's not "market failure" at work when child predators are lurking online; it is

---

[371] Quoted in Anick Jesdanun, "Age Verification at Social-Network Sites Could Prove Difficult," *Associated Press Financial Wire*, July 14, 2006.

[372] "With the expanded ability to meet and interact with new people online comes the need for a new skill—online stranger literacy. Online stranger literacy is the ability to determine the trustworthiness and safety of individuals who are unknown in person, with whom one is communicating online. It is the 'people' equivalent of information literacy." Nancy E. Willard, *Cyber-Safe Kids, Cyber-Savvy* Teens (San Francisco, CA: Jossey-Bass, 2007), p. 120.

[373] *Ibid.*

[374] Parry Aftab, Filing in COPPA Rule Review 2005 before the Federal Trade Commission, June 27, 2005, p. 4.

[375] "5 Percent of Sex Offenders Rearrested for Another Sex Crime within 3 Years of Prison Release," U.S. Department of Justice, Office of Justice Programs, November 16, 2003, www.ojp.usdoj.gov/bjs/pub/press/rsorp94pr.htm

government failure *in the extreme*. We are never going to solve this problem until we hunt down the bad guys and lock them up for a long, long time.

Consider a startling October 2006 special report by *Wired* reporter Kevin Poulsen.[376] In his article, Poulsen explained how he helped New York law enforcement officials track down and apprehend a sex offender by writing a program that searched MySpace's member profiles for registered sex offenders. Here's what was shocking about the specific perpetrator that they nabbed, a 39-year-old man named Andrew Lubrano:

> Lubrano was sentenced to three years probation in 1987 for sexual abuse against a 7-year-old boy, according to police. In 1988, he got another probation term for second-degree sex abuse. In 1995, he earned a 3 to 9 year prison term for sexually abusing two boys he'd been babysitting, one 11, the other 9. The parole board turned Lubrano down three times, and he was cut loose in September 2004 largely unsupervised, having served every day of his nine-year max. By November 2005 he was on MySpace, making friends.

When this story broke, many critics were quick to jump on MySpace and other social networking sites as the root of this problem. But is the existence of MySpace or other social networking sites really the problem here? Or is it the fact that this child abuser was sitting behind a keyboard when he should have been sitting in a jail cell? Why is it MySpace's problem to solve instead of the government's?

The most essential role that government has is to protect people from harm, especially helpless kids. It is not the job of private companies to enforce law and order or bring criminals to justice. That is the government's job.

What's even more troubling is that after letting the child abusers out of jail, governments then expend considerable sums of money and law enforcement resources for "community supervision" and "sex offender registries" to give us a better idea of where all the child molesters live in our neighborhoods. This is of little consolation to most parents who would probably feel much more comfortable having these predators locked up in a prison instead of living somewhere in their communities.

What we must ask ourselves as a society is this: With the exception of murder, is there any crime more heinous than child rape or child sexual abuse? If we can agree that sexual abuse of children is indeed that serious, then we ought to be considering sentences that are significantly longer than just three to seven

[376] Kevin Poulsen, "MySpace Predator Caught by Code," *Wired.com*, October 16, 2006, www.wired.com/science/discoveries/news/2006/10/71948

years to ensure that convicted child abusers aren't out on the streets and sitting behind keyboards looking to prey upon children again. President Bush recently signed the "Adam Walsh Child Protection and Safety Act of 2006," which increases mandatory minimum sentences for various crimes against children.[377] That's certainly a helpful step in the right direction, but more can be done.

In particular, it is also essential that law enforcement officials receive the resources and training necessary to adequately monitor online networks for predators and to bring them to justice when they are found.[378] For example, law enforcement agencies need online forensic labs and experts to help investigate online crimes. And they need to be trained to conduct proper sting operations to find predators before they harm our children. As outlined next, industry is already assisting law enforcement officials in this regard.

Industry Assistance and Training for Law Enforcement

Many leading Internet operators provide valuable assistance to law enforcement agencies or partner with law enforcement officials on investigations to help protect children. For example:

- **AOL:** Since 1996, AOL has been working with law enforcement officials to trace and apprehend child predators or child pornographers. AOL was an earlier pioneer of 24/7 law enforcement hotlines and was the first ISP to initiate an Amber Alert program.[379] AOL personnel also offer extensive cybercrime, digital evidence, and computer forensic science courses to a wide variety of federal and state law enforcement officers.[380] And AOL provides free litigation support and expert witnesses to prosecutors for criminal cases involving records obtained from the company.[381]
- **Microsoft:** Like AOL, Microsoft sponsors computer forensic and technical training programs for law enforcement officials both here and abroad and

[377] President Bush recently signed the "Adam Walsh Child Protection and Safety Act of 2006," which increases mandatory minimum sentences for various crimes against children. See "President Signs H.R. 4472, the Adam Walsh Child Protection and Safety Act of 2006," White House *Press Release,* July 27, 2006, www.whitehouse.gov/news/releases/2006/07/20060727-6.html

[378] Senators John McCain (R-AZ) and Charles Schumer (D-NY) recently introduced legislation, S. 519, that would require all convicted sex offenders to register their e-mail addresses with law enforcement officials so that their online activities could be monitored. The e-mail addresses could also be monitored by social networking sites to ensure that sex offenders were not on those sites. While there is nothing stopping offenders from changing their e-mails to avoid detection, the legislation also stipulates that any offender caught doing so will be eligible for an additional 10 years of jail time on top of the sentence for any other underlying offense.

[379] John D. Ryan, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites," Testimony before the House Committee on Commerce and Energy, Subcommittee on Oversight and Investigations, June 27, 2006, pp. 3-4, http://energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Ryan.pdf

[380] Ibid., p. 4-5.

[381] Ibid., p. 5.

has compliance officers on hand 24/7 to field law enforcement inquiries.[382] In 2003, Microsoft developed the Child Exploitation Tracking System (CETS), "an open standards-based software tool that enables law enforcement to better gather and share evidence of online child exploitation over a secure system based on legal agreements in place. CETS permits investigators to easily import, organize, analyze, share and search information from the point of detection through the investigative phase to arrest and conviction."[383]

- **Google:** Google has a legal team devoted to responding to law enforcement requests for assistance and the company responds to hundreds of subpoenas each year to assist child safety investigations.[384] Google strictly prohibits advertising about illegal content in any of its products or sites and encourages users to report any illegal content they encounter to the Google Help Center to ensure that it is immediately passed along to law enforcement officials. It's also worth noting that Google allows other organizations to freely use its Google Maps technology to easily track convicted sex offenders living in their communities. For example, www.mapsexoffenders.com and www.familywatchdog.us both rely on the Google Maps service to trace convicted sex offenders.
- **Yahoo!:** Yahoo! also has a compliance team in place to handle online emergencies 24 hours a day and provides training and assistance to law enforcement officials. Yahoo! created its "Law Enforcement Compliance Manual" to ensure that law enforcement officials know how Yahoo! can assist them in online investigations.[385] In particular, Yahoo! provides assistance through the Internet Crimes Against Children (ICAC) task forces, the American Prosecutors Research Institute, and the newly launched Financial Coalition Against Child Porn.
- **MySpace.com**: MySpace has created and widely distributed its "Law Enforcement Officer Guide" that instructs law enforcement agencies on

[382] Philip K. Reitinger, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites," Testimony before the House Committee on Commerce and Energy, Subcommittee on Oversight and Investigations, June 27, 2006, pp. 4-5, http://energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Reitinger.pdf

[383] Ibid., p. 4.

[384] Nicole Wong, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites," Testimony before the House Committee on Commerce and Energy, Subcommittee on Oversight and Investigations, June 27, 2006, p. 5, http://energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Wong.pdf

[385] Elizabeth Banker, "Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites," Testimony before the House Committee on Commerce and Energy, Subcommittee on Oversight and Investigations, June 27, 2006, p. 8, http://energycommerce.house.gov/reparchives/108/Hearings/06272006hearing1954/Banker.pdf

how to work with MySpace regarding subpoenas and requests for information.[386]

In addition, these companies and many others work closely with the National Center for Missing and Exploited Children (NCMEC) to combat online child pornography or predation in a variety of ways.[387] NCMEC has developed a wide variety of excellent resources to teach children about online safety. For example, in 2006 NCMEC partnered with Duracell to create the "Power of Parents" program and website which helps parents teach their kids about both online and offline safety.[388] The site offers free storybooks and "teachable moment" manuals to help parents talk to their kids about protecting themselves.[389]

In May 2007, NCMEC also launched the "Take 25" project to coincide with the 25th anniversary of President Ronald Reagan designating May 25th as "National Missing Children's Day."[390] NCMEC's new program encourages families to take 25 minutes to talk with their children about safety and abduction prevention. Dozens of events across the nation were planned to highlight the effort.[391]

[386] www.netcaucus.org/books/childsafety2006/myspace.pdf
[387] For more information about what these and other companies are doing to assist law enforcement efforts and officials, see "What ICAC Members Are Doing to Help Protect Children Online," Internet Caucus Advisory Committee, 2006, http://www.netcaucus.org/books/childsafety2006/
[388] www.powerofparentsonline.com
[389] www.powerofparentsonline.com/teaching%5Ftools
[390] www.take25.org
[391] www.take25.org/events

VI. Conclusion

> *"Responsibility – A detachable burden easily shifted to the shoulders of God, Fate, Fortune, Luck or one's neighbor. In the days of astrology it was customary to unload it upon a star."*
> -- Ambrose Bierce, *The Devil's Dictionary*

This study has demonstrated that parents now have multiple layers of protection at their disposal to shield their children from potentially objectionable media content or to protect them while they are online. These tools include the various content rating and labeling systems, the V-Chip, set-top box parental controls (including gaming console controls), personal video recorders, Internet and mobile media filtering and screening services, monitoring tools, and so on.

And the many industry-led educational efforts highlighted here prove that, contrary to what some critics claim, media creators and information distributors *are* taking steps to help parents make content determinations and better control child access to unwanted media. As this report has made clear repeatedly, education is absolutely essential at every point in this process.

Critics can always argue that media and communications companies should "do more" to address the concerns that parents have, but it's important to realize that they are already doing quite a bit. Of course, whether parents are taking advantage of those tools and options is another matter entirely. *But if, for whatever reason, parents are not taking advantage of these tools and options, their inaction should not be used to justify government regulation as a surrogate for household / parental choice. Parents have been empowered. It is now their responsibility to take advantage of the tools and controls at their disposal to determine what is acceptable in their homes and in the lives of their children.*

Some media critics and policymakers will continue to have their doubts, however, and claim that the tools are not good enough. Oftentimes this is just an effort to disguise a desire by some to sanitize or even eliminate certain types of speech or artistic expression from society altogether. Other times, however, their concerns will be rooted in a heartfelt desire to give parents more tools or information to control potentially objectionable media or keep their children safe from online threats.

The controls and ratings will likely continue to be refined to satisfy these concerns. And new tools and educational efforts will be developed and deployed. Regardless, parents are already being offered an extensive array of empowerment tools to sort and filter content they might find objectionable and to keep their kids safe online. This is being done much more quickly, much more closely tailored to the parents' own desires, and without the censorship concerns typically associated with government regulatory efforts.

In the extreme, if parents want to take radical steps to limit children's potential access to objectionable programming, they can get rid of certain media devices altogether or severely restrict the availability of such devices in the home. While impractical for most, some families do reject televisions, for example, and still find many other ways to access important information and entertainment.[392]

Finally, and perhaps most sensibly, parents can always sit down with their children, consume media programming with them, and talk to them about what they are seeing and hearing. For those parents willing to accept the reality that children *will* be confronted with many troubling or sensitive topics from peers at school or from other sources outside their control, this option makes a great deal of sense. Most parents already do this, of course. A recent Kaiser survey of media usage by children under six years of age found that 69 percent of parents were in the room when children were watching TV, for example.[393] At the end of the day, there is simply no substitute for talking to our children in an open, loving, and understanding fashion about the realities of this world, including the more distasteful bits.

It's about parental responsibility. And now that we've been empowered to take responsibility over the media in our lives and the lives of our children, we cannot blame "God, Fate, Fortune, Luck," or even the government for our own failures to be good stewards for our children.

[392] See, for example, Rich Karlgaard, "Net—One, TV—Zero," *Forbes.com*, November 29, 2004, www.forbes.com/columnists/business/forbes/2004/1129/041.html

[393] *Zero to Six: Electronic Media in the Lives of Infants, Toddlers and Preschoolers*, Kaiser Family Foundation, Fall 2003, p. 11, available at www.kff.org/entmedia/entmedia102803pkg.cfm

Related PFF Publications

- "The Right Way to Regulate Violent TV," by Adam Thierer, PFF Progress on Point 14.10, May 14, 2007.
- "Age Verification for Social Networking Sites: Is it Possible? Is it Desirable?" [event transcript], PFF Progress on Point 14.8, May 11, 2007.
- "Social Networking and Age Verification: Many Hard Questions; No Easy Solutions," by Adam Thierer, PFF Progress on Point 14.5, March 21, 2007.
- "Rep. Bean's 'SAFER Net Act': An Education-Based Approach to Online Child Safety," by Adam Thierer, PFF Progress on Point 14.3, February 22, 2007.
- "Joint Amicus Brief of The Center for Democracy & Technology and The Progress & Freedom Foundation in the U.S. 2nd Circuit Court of Appeals in the matter of *Fox Television Stations v. FCC,*" by Adam Thierer, John B. Morris, Jr., and Sophia Cope, November 30, 2006
- "Do's and Dont's for Global Media Regulation: Empowering Expression, Consumers and Innovation," by Patrick Ross, Progress on Point, 2.20
- "Saving Online Free Speech: A Voluntary Code of Conduct for Internet Operators," by Adam Thierer, Progress Snapshot, 2.19
- "Social Networking Websites & Child Protection: Toward a Rational Dialogue," by Adam Thierer, Progress Snapshot 2.17, June 2006.
- "Is MySpace the Government's Space?," by Adam Thierer, Progress Snapshot 2.16, June 2006.
- "Parents Have Many Tools to Combat Objectionable Media Content," by Adam Thierer, PFF Progress on Point 13.9, April 2006.
- "Fact and Fiction in the Debate Over Video Game Regulation," by Adam Thierer, PFF Progress on Point 13.7, March 2006.
- "Examining the FCC's Complaint-Driven Broadcast Indecency Enforcement Process," by Adam Thierer, PFF Progress on Point 12.22, November 2005.
- "Regulation Without Frontiers: Europe Shows U.S. Policymakers How Not to Embrace Convergence," by Patrick Ross, PFF Progress Snapshot 1.15, September 2005.
- "The Politicization of ICANN and the Domain Name System: The ".xxx" Case Study," by Solveig Singleton and Adam Thierer, PFF Progress Snapshot 1.10, September 2005.
- "New Worlds to Censor," by Adam Thierer, *Washington Post* editorial, June 7, 2005.
- "Can Broadcast Indecency Regulations Be Extended to Cable Television and Satellite Radio?" by Robert Corn-Revere, PFF Progress on Point 12.8, May 2005.
- "'Kid-Friendly' Tiering Mandates: More Government Nannyism for Cable TV," by Adam Thierer, PFF Progress Snapshot 1.2, May 2005.
- "Thinking Seriously about Cable & Satellite Censorship: An Informal Analysis of S-616, The Rockefeller-Hutchison Bill," by Adam Thierer, PFF Progress on Point 12.6, April 2005.