



Summer 6-1-2009

Virtual Parentalism

Joshua A.T. Fairfield

Washington and Lee University School of Law, fairfieldj@wlu.edu

Follow this and additional works at: <https://scholarlycommons.law.wlu.edu/wlulr>



Part of the [Family Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Joshua A.T. Fairfield, *Virtual Parentalism*, 66 Wash. & Lee L. Rev. 1215 (2009).

Available at: <https://scholarlycommons.law.wlu.edu/wlulr/vol66/iss3/11>

This Article is brought to you for free and open access by the Washington and Lee Law Review at Washington and Lee University School of Law Scholarly Commons. It has been accepted for inclusion in Washington and Lee Law Review by an authorized editor of Washington and Lee University School of Law Scholarly Commons. For more information, please contact christensena@wlu.edu.

Virtual Parentalism

Joshua A.T. Fairfield*

Abstract

Parents, not laws, ultimately protect children both online and offline. If legislation places adults at legal risk because of the presence of children in virtual worlds, adults will exit those worlds, and children will be isolated into separate spaces. This will not improve safety for children. Instead, this Article suggests that Congress enact measures that encourage filtering technology and parental tools that will both protect children in virtual worlds, and protect free speech online.

Table of Contents

I. Introduction	1216
II. Parentalism and Cyberbalkanization.....	1218
A. Cyberbalkanization	1219
B. Speech and Child Protection Online.....	1224
C. The Effect of Isolation on Children	1231
III. Filtering and Virtual Worlds.....	1233
A. Basic Chat Filtering	1234
B. Filtering Reality: Instancing and Quest-Phasing.....	1234
C. Making Filtering Better	1237
D. Commerce, Anonymity, and Filtering	1239
IV. Necessary Law Enforcement in Virtual Worlds.....	1240
V. Conclusion.....	1242

* Associate Professor of Law, Washington & Lee University School of Law. Thanks to all the participants of the Protecting Virtual Playgrounds: Children, Law, and Play Online Symposium at Washington & Lee University. Thanks to Russ Miller, Robin Wilson, Joan Shaughnessy, Sam Calhoun, Ted Castronova, Greg Lastowka, and Berin Szoka for comments and suggestions. This Article is dedicated to the memory of Louise Halper, without whose guidance and support this symposium would not have been possible.

I. Introduction

When lawmakers consider kids and virtual worlds, the urge to legislate appears overwhelming.¹ The mix of children and new media has always inspired calls for crackdowns. Plays, novels, comic books, movies, television, and Socratic philosophy were all broadly charged with corrupting the youth when they first appeared. Given the growth of virtual worlds such as *World of Warcraft* and *Club Penguin*, and the explosive popularity of social networking sites and games, legislation may be inevitable.²

Laws protecting kids have always been popular and necessary. But parents, not laws, ultimately protect children.³ This Article argues that parents and communities cannot—and should not—be replaced by laws as sources of protection for children. In virtual worlds, parents play with their children, and

1. The ramp-up to virtual world regulation to protect children has thus far included hearings, see *Congress Holds First Hearing on Virtual Worlds: Linden Lab CEO Philip Rosedale Testifies*, VIRTUALLY BLIND, Apr. 1, 2008, <http://virtuallyblind.com/2008/04/01/congress-virtual-worlds> (last visited Sept. 29, 2009) (on file with the Washington and Lee Law Review), and a directive to the Federal Trade Commission to examine and report on the availability of explicit materials within virtual worlds to minors. See H.R. REP. NO. 110-92, at 68 (2008) (expressing concern over explicit content accessible by minors). Specifically, the House Report stated:

The Committee is concerned about reports of explicit content that can be easily accessed by minors on increasingly popular virtual reality web programs. The Committee directs the FTC to issue a consumer alert to educate parents on the content that is available to children on virtual reality web programs. In addition, no later than 9 months after enactment of this Act, the Commission shall submit a report to the Appropriations Committee discussing the types of content on virtual reality sites and what steps, if any, these sites take to prevent minors from accessing content.

Id.

2. See *Stardoll Doubles Membership over Year to Hit 20M Registered Users*, VIRTUAL WORLDS NEWS, Aug. 15, 2008, <http://www.virtualworldsnews.com/2008/08/stardoll-double.html> (last visited Sept. 29, 2009) ("Stardoll announced yesterday that it had reached 20 million registered users, double the 10 million registered users that Stardoll announced just over a year ago and continuing to grow at about 25 thousand new registrations per day.") (on file with the Washington and Lee Law Review); *Strategy Analytics: Virtual Worlds Projected to Mushroom to Nearly One Billion Users: \$8 Billion Market Value Projected for User Services Value Projected for User Services*, REUTERS, June 3, 2008, <http://www.reuters.com/article/pressRelease/idUS185045+03-Jun-2008+BW20080603> (last visited Sept. 29, 2009) ("[O]ver the next ten years some 22 percent of global broadband users will have registered for one or more virtual worlds resulting in a market approaching one billion registrants and an eight billion dollar services opportunity.") (on file with the Washington and Lee Law Review).

3. See JOHN PALFREY & URS GASSER, BORN DIGITAL: UNDERSTANDING THE FIRST GENERATION OF DIGITAL NATIVES 105 (2008) ("Changes in the law and regulation are not the primary ways to protect our kids, but the role of the state is important all the same. The law, as a general matter, can offer a backstop in terms of keeping children safe.").

online communities have developed norms of child protection. If legislation reinforces these norms, it is a positive development.⁴ But if, as seems likely, legislation disrupts communities by separating families out into separate "child-friendly" and "mature" worlds, children will lose much of the protection they currently enjoy in virtual worlds. Virtual worlds are, among other things, communities of real-world people. And, like real-world communities, these communities have their own norms that often operate to constrain behavior.⁵ Before we legislate, we ought to note what tools and norms are already in place. Recognition of these norms is an important part of introducing order to virtual worlds. Without such an inquiry, laws might displace useful norms and make things worse.

It is important to note what this Article does not assert. It does not argue that game gods (the companies that create and maintain virtual worlds) should not aggressively seek out and ban sexual predators or assist law enforcement in stopping predators online.⁶ They can and must. And this Article does not argue that police should not aggressively investigate and arrest virtual world denizens who target children for sexual gratification.⁷ Again, police can and must act against real predators.⁸

This Article makes three limited points. First, that parentalism legislation is likely to disrupt speech and ultimately break up virtual world communities. Second, that this balkanization will isolate children from the very communities that protect them. And third, that communities and the virtual worlds industry may be able to avoid this by developing better filters to protect children in virtual worlds.

4. See *id.* at 98 ("The best way to mitigate the Internet safety risks that our children face is to combine . . . education, technology development, social norms, and the law.").

5. See ROBERT C. ELLICKSON, *ORDER WITHOUT LAW* 123–36 (1991) (providing a taxonomy of self-help methods communities use to regulate without reference to law).

6. See *Facebook Drops Sex Offenders*, L.A. TIMES, Feb. 20, 2009, at A11 (reporting that Facebook has removed over 5,000 sex offenders from its site and MySpace has removed over 90,000 sex offenders from its site); *Sex Offenders Face Website Bans*, BBC NEWS, Apr. 4, 2008, http://news.bbc.co.uk/2/hi/uk_news/7328170.stm (last visited Sept. 29, 2009) ("Sex offenders' e-mail addresses are to be passed to social networking sites like Facebook and Bebo to prevent them contacting children.") (on file with the Washington and Lee Law Review); see also Keeping the Internet Devoid of Sexual Predators Act of 2008 (KIDS Act of 2008), 42 U.S.C. § 16915a *et seq.* (2006) (stating requirements for sex offenders regarding websites).

7. See generally Madeleine Mercedes Plasencia, *Internet Sexual Predators: Protecting Children in the Global Community*, 4 J. GENDER RACE & JUST. 15 (2000) (detailing the numerous instances of police enforcement against predators who seek real-world meetings with children).

8. See generally *supra* note 7 and accompanying text (discussing instances in which police took action against sexual predators).

II. Parentalism and Cyberbalkanization

Imagine that you join a movie discussion group in a virtual world. The discussion is held in the virtual private home of one of the discussants. The discussants, through their avatars, analyze the recently-released and deeply controversial Academy nominated movie, *The Reader*, which involves a complicated discussion of sexual misconduct toward minors, individual guilt, and collective guilt for the crimes of the Third Reich.⁹ The conversation veers from the sexual to the political. Because the discussion occurs within a virtual world, members of the discussion group are able to import stills from the movie into the virtual world to underscore their arguments, or are able to shape the reality around them to reflect scenes from the movie.

Imagine your surprise if you and the other discussants were subsequently arrested by the real-world police for lewd and lascivious conduct toward a minor.¹⁰ The reason? One of the "adults" at the meeting was actually a fifteen-year-old boy, posing as an adult avatar. No one at the meeting had the slightest idea that a child was sitting behind one of the adult avatars; in fact, the home was in an area that children were not supposed to enter at all.

This case is intentionally hard. On the one hand, we have real-world laws that apply to conduct between adults and children regardless of the knowledge of the adult. For example, statutory rape is a strict liability crime: It is no defense for an adult to claim that she did not know the age of the minor.¹¹

On the other hand, internet anonymity has shaped policy and law online. If website operators were liable every time a child posing as an adult accessed mature content, we would have to shut the Internet down. Therefore, the governing rule thus far has been that the First Amendment prevents the

9. THE READER (Mirage Enterprises et al. 2008).

10. See, e.g., ALA. CODE § 13A-6-60 *et seq.* (2007) (listing the Alabama statutory sexual offenses); CAL. PENAL CODE § 288 (West 2008) (listing the elements and penalties of the California statutory offense of lewd or lascivious acts); N.C. GEN. STAT. § 14-202.1 (2007) (listing the elements of the North Carolina statutory offense of taking indecent liberties with children); see also Dalia Lithwick, *Teens, Nude Photos and the Law*, NEWSWEEK, Feb. 23, 2009, at 18 (discussing whether every case of lewdness should be prosecuted by police to the fullest extent of the law and whether the law encompasses too much conduct); "Sexting": *Racy Teen Messaging Could Be Illegal*, NPR Talk of the Nation (National Public Radio, radio broadcast Feb. 18, 2009) (discussing whether sex message texting amongst teens should be legally restricted), available at 2009 WLNR 3200250.

11. See, e.g., *Commonwealth v. Disler*, 884 N.E.2d 500, 509 (Mass. 2008) ("[T]he Commonwealth is not required to prove the defendant's knowledge of the victim's age as an element of the crime."); *People v. Nyx*, 734 N.W.2d 548, 565–66 (Mich. 2007) ("Because there was no indication that the Legislature intended to abrogate the common law, this Court held that sexual penetration of a victim who is at least 13 but less than 16 constitutes a strict liability offense and, therefore, 'reasonable mistake of age' is not a defense.").

application of criminal law to the unwitting transmission of adult content to children.¹²

This Article explores the hard choices we will have to make in selecting child-protecting laws for virtual worlds. If we are clumsy, we could either leave children unprotected or drive adults out of virtual worlds altogether, functionally destroying the promise of the technology.

A. Cyberbalkanization

Imposing liability on unwitting adults for communications received by minors will cause adults and children to move into separate virtual worlds. We should act cautiously before segregating children from adults online. Scholars have long pointed out the dangers of internet segregation.¹³ Online forums, blogs, and even news outlets provide information consumers with the necessary tools to confirm pre-existing opinion rather than engage in democratic discourse.¹⁴ Fragmented discourse creates an "echo chamber" effect, in which groups that only speak internally reinforce the most extreme positions in the group.¹⁵ There are criminal risks as well as political ones.¹⁶ Groups with common perverse interests gather online, and reinforce each others' preferences as "normal."¹⁷ These perversion support groups are the stuff of internet legend.¹⁸ The creation of these internet backwaters should be of concern to the

12. See *infra* Part II.B (discussing speech and child protection online).

13. See CASS R. SUNSTEIN, *REPUBLIC.COM 2.0*, at 21 (2007) (discussing the threat that the ability to filter presents to democracy).

14. See *id.* at 51–55 (discussing how consumers can obtain information through electronic channels without offering an untested opinion in democratic discourse).

15. See *id.* at 6, 76–78 (discussing how the characteristics of online discourse creates an environment that fosters extreme positions that normally would not carry any legitimacy through democratic discourse).

16. See *id.* at 57 (describing at length the criminal risks involved when consumers do not test their views through democratic discourse).

17. See Plasencia, *supra* note 7, at 17 (commenting on the ease in which pedophiles can interact with others in chat groups). Plasencia specifically stated:

With quick and anonymous virtual travel made possible through the Internet, pedophiles are "logging on" and forming chat groups, swapping pornographic images and sharing true stories of sexual activity with children. This process of bonding with other pedophiles by forming support sites in cyberspace has been referred to as "virtual validation."

Id. (citations omitted).

18. See *id.* (discussing activities of perversion support groups).

law. Instead, current regulatory approaches will likely create more such backwaters, to the detriment of children.¹⁹

There are two additional reasons to be cautious about segregating adults from children. The first is that parental involvement with children's activities is the best way to keep children safe.²⁰ If virtual worlds are segregated into adult and children's worlds, parents will no longer be interested in the same games as their children, and will no longer play alongside their children.²¹ Second, once responsible adults exit the worlds set aside for children, only those adults willing to lie to enter those worlds—predators—will remain in among the children.²²

Segregating virtual worlds will destroy much of the promise of virtual world technology. Some technologies, including virtual worlds, draw communities together.²³ Virtual worlds are in a serious sense the opposite of the cyberbalkanization process. They revolve around a shared simulated space and involve players in common goals and activities. The design of a virtual world is predominantly the design of spaces and activities for the population—including parents and children—to experience together.²⁴

19. See Berin Szoka & Adam Thierer, *COPPA 2.0: The New Battle over Privacy, Age Verification, Online Safety & Free Speech*, 16.11 PROGRESS ON POINT 1, 30 (2009), available at <http://www.pff.org/issues-pubs/pops/2009/pop16.11-COPPA-and-age-verification.pdf> ("Here, one must further ask if attempting to quarantine children from adults (however indirectly) actually advances, on net, a strong governmental interest in child protection.").

20. See PALFREY & GASSER, *supra* note 3, at 110 ("Parents and teachers need to become a much bigger part of the solution, and soon.").

21. See Szoka & Thierer, *supra* note 19, at 30 ("A substantial portion of those interactions involve parents talking to their own kids, older and younger siblings communicating with one another, teachers and mentors talking to their students, or even co-workers of different ages communicating. Even when adult-minor communications involve complete strangers, there is typically a socially-beneficial purpose."); see also JOHN D. AND CATHERINE T. MACARTHUR FOUNDATION, *LIVING AND LEARNING WITH NEW MEDIA: SUMMARY OF FINDINGS FROM THE DIGITAL YOUTH PROJECT 39* (2008), available at <http://digitalyouth.ischool.berkeley.edu/files/report/digitalyouth-WhitePaper.pdf> ("In contexts of peer-based learning, adults . . . have an important role to play Unlike instructors in formal educational settings, . . . these adults are passionate hobbyists and creators, and youth see them as experienced peers, not as people who have authority over them. These adults exert tremendous influence in setting communal norms").

22. See Szoka & Thierer, *supra* note 19, at 30 ("Such a quarantine is unlikely to stop adults with truly nefarious intentions from communicating with minors, as systems designed to exclude participation by adults in a 'kids-only' or 'adolescents-only' area can be easily circumvented.").

23. See SUNSTEIN, *supra* note 13, at 139–40 (suggesting an understanding of the blogosphere as a "huge market" and a "gigantic town meeting"); *id.* at 49 ("Of course the Internet can bring people together rather than drawing apart. Countless people are using the Internet to build larger and more diverse communities.").

24. See TOM BOELLSTORFF, *COMING OF AGE IN SECOND LIFE* 51 (2008) ("The essential

For example, the virtual *World of Warcraft* begins by introducing the concept of a quest—a task that can be performed for some in-world reward.²⁵ Higher level quests require more cooperation, and more people become involved in seeking the same goal.²⁶ The endgame of *World of Warcraft*, commonly called "raiding," involves large groups of people working together in a highly coordinated fashion to achieve complex goals.²⁷ Virtual worlds provide a forum for common discourse. In a virtual world, people from across the political, geographical, and financial spectrum cross paths.²⁸ Many quests or tasks are not possible without a larger group.²⁹ Entire guilds—or groups of groups—must focus on larger problems, such as how to organize a large group of people on a given task over a long period of time.³⁰

And of course, while people play, they talk.³¹ Like the workplace, virtual worlds have become a setting where citizens talk across the divide. What technology has wrought—separating neighborhoods out because of the low cost of driving to work, and family members from one another because of the search for jobs—technology can now undo. Virtual world technology reconstructs the social systems and the physical systems that were the rule for the majority of human existence.³² Conversation in a guild channel in *World of Warcraft*

lesson that we have abstracted from our experiences with [the virtual word] is that a cyberspace is defined more by the interactions among the actors within it than by the technology with which it is implemented."); *id.* at 180 (noting that virtual worlds constitute communities shaped by the residents within them); *see also* Szoka & Thierer, *supra* note 19, at 30.

25. *See* EDWARD CASTRONOVA, *SYNTHETIC WORLDS: THE BUSINESS AND CULTURE OF ONLINE GAMES* 106 (2005) (describing a quest).

26. *Id.*

27. *See* Joshua Fairfield & Edward Castronova, *Dragon Kill Points*, in *RATIONAL MODELS SEMINAR*, UNIV. OF CHI. 2006, at 1–3 (SSRN Working Paper Series No. 958945) [hereinafter *Dragon Kill Points*] (discussing the complicated organizational efforts that go into organizing a raid).

28. *See* Dmitri Williams et al., *Who Plays, How Much, and Why? Debunking the Stereotypical Gamer Profile*, 13 J. COMPUTER-MEDIATED COMM'C'N 993, 993–94 (2008), available at <http://www3.interscience.wiley.com/cgi-bin/fulltext/121394419/PDFSTART> (discussing the interactions between people who interact in a virtual world).

29. *See* *Dragon Kill Points*, *supra* note 27, at 2 ("[A] cohesive and persistent group structure . . . must be built and maintained over the course of many months if not years.").

30. *See id.* (discussing the coordination amongst players that is necessary to complete a successful raid); *see also* CASTRONOVA, *supra* note 25, at 121–22 (explaining briefly the formation of guilds within synthetic worlds).

31. *See* CASTRONOVA, *supra* note 25, at 67–68 (describing communicative aspects of virtual worlds).

32. *See id.* at 121–25 (discussing the effects of virtual technology on social systems); Nick Yee, *Playing with Someone*, in *THE DAEDALUS PROJECT* (2005), <http://www.nickyee.com/daedalus/archives/001468.php> (discussing a study that demonstrates that gamers often play with people they already know in real life, suggesting that gaming is not anti-social as critics

resembles nothing so much as conversation around a (slightly rowdy) kitchen table.³³

Virtual world relationships reflect real-world connections.³⁴ People do not enter virtual worlds purely anonymously. They do so in groups.³⁵ Groups join servers together, families play together, and (this is the important point) parents often play with children.³⁶ Children know many of the people with whom they interact from real life. Uncles and the occasional aunt are often in-world. Cousins abound. The distances that have dissected real-world families of course do not matter in a virtual world.

Virtual worlds present a compelling mix of fantasy and reality.³⁷ People enjoy content, but enjoy it more in the company of friends and family. Content draws people into virtual worlds, but a real sense of community is what causes people to remain in the world. Many players have no interest in a world that lacks their social network, and often players will return to a given world purely because of the social network that they left behind.

Children are protected by their own communities. Often children have a separate designation within the guild community that they join. For example, in the author's guild, children of members play alongside their parents, and receive a special guild designation that permits the guild to keep the chat channels that children can hear free of profanity.³⁸

At the same time, children are entering worlds in which rough speech and rough-and-tumble discourse are the norm. Profanity in virtual public spaces is

believe).

33. See CASTRONOVA, *supra* note 25, at 100–02 (drawing parallels between virtual world conversation and real-world conversation).

34. See *id.* at 121 (commenting on the similarities between real world and virtual world relationships); Williams et al., *supra* note 28, at 31 (suggesting "the displacement of previously existing relationships by new in-game ones").

35. See Nick Yee, *The Demographics of Guilds*, in THE DAEDALUS PROJECT (2008), <http://www.nickyee.com/daedalus/archives/001635.php> (last visited Sept. 29, 2009) (reviewing results in a study on the trends regarding virtual world guilds) (on file with the Washington and Lee Law Review).

36. See Nick Yee, *Kids and MMOs*, in THE DAEDALUS PROJECT 9 (2008), <http://www.nickyee.com/daedalus/archives/001627.php?page9> (last visited Sept. 29, 2009) (noting that "[a]s we've seen before, parents can play with kids productively," and discussing a survey that highlights the risks involved with gaming while stressing the importance that parents get involved and play with their children) (on file with the Washington and Lee Law Review).

37. See CASTRONOVA, *supra* note 25, at 107 ("The combination of these efforts produces a society with Earth-like richness and complexity, even though the objects about which this society dances are completely fantastical.").

38. See Hrafnwarband, Index, <http://www.hrafnwarband.com> (last visited Sept. 29, 2009) (serving as a forum for gamers) (on file with the Washington and Lee Law Review).

far more common than is the case in the real world.³⁹ Crude sexual or scatological references are quotidian.⁴⁰ Politics⁴¹ and religion⁴² are also common subjects—and the discussion is sure to cause a dispute with multiple parties chiming in. Political protests, analysis of legislation, party politics, and other subjects are routinely trotted out.⁴³ On the other hand, many people avoid such topics—as they do in real life—out of a sense that there are people in the same space who disagree with them. Since guild and group membership is at a premium, users of a space will often moderate their language or defuse conflict in order to get along.

The difficulty is that children may be exposed to rough-and-tumble discourse. Thus, we are presented with a choice between two alternatives: Ban offensive speakers when their speech reaches children's ears, through the application of criminal or other regulatory law, or improve filtering technology, so that children can share a world with their parents, but can only see and hear what their parents permit. This Article advocates the latter.

The Article develops the idea of this filtering technology below, but it is worth mentioning here that the existence of filtering technology does much to satisfy both the need to protect children and the need to preserve speech. Imagine that one simply enters the world with all other users turned "off." A parent would only permit the child to be able to speak with and hear another user that the parent truly knows. Thus, without one whit of regulation, the question of rough chat or of predators who seek to use online contacts to foster offline meetings can be resolved through parents' self-help. Those people simply cannot interact with—in fact would not even exist with reference to—the child.

39. See Jack Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043, 2058–59 (2004) (noting that one incentive a state may have for regulating virtual worlds is the "violent, offensive, or indecent" content); Peter Jenkins, *The Virtual World as a Company Town—Freedom of Speech in Massively Multiple Online Role Playing Games*, 8 J. INTERNET L. 1, 3–5 (2004) (discussing whether *Marsh v. Alabama*, 326 U.S. 501 (1946), allows for First Amendment protection in the virtual world context), available at SSRN ID No. 565181.

40. See BOELLSTORFF, *supra* note 24, at 151–65 (discussing the common use of sexual references in virtual worlds).

41. See SUNSTEIN, *supra* note 13, at 80 (noting that politics is a subject that often comes up in conversation in virtual worlds).

42. See BOELLSTORFF, *supra* note 24, at 185 (noting that religion is a common conversation topic in virtual worlds).

43. See SUNSTEIN, *supra* note 13, at 46–57 (discussing popular topics of conversation in virtual worlds); see also PETER LUDLOW & MARK WALLACE, *THE SECOND LIFE HERALD: THE VIRTUAL TABLOID THAT WITNESSED THE DAWN OF THE METAVERSE* 171–72 (2007) (recounting protest movements within the virtual world that "smacked of politics").

We are in very real danger of not following this path, and instead relying on the usual mix of laws to jail speakers who unwittingly transmit content to avatars that turn out to be run by children. The problem is that if speakers are liable for this content, free discourse within virtual worlds will be compromised. Rather than suffer the risk of being overheard, adults will either turn off the most promising technology for cooperation and discourse that we have seen in some time, or they will segregate children into separate worlds.

B. Speech and Child Protection Online

The usual argument is that we can protect either speech or children.⁴⁴ This Article argues that this is a false choice, and that free speech values are an integral part of any system that seeks to protect children in virtual worlds. At a minimum, people should be free to speak up about dangers to children in virtual worlds without fear of reprisal.

An example may clarify the problem. In 2003, Michigan philosophy professor Peter Ludlow published an account of teen virtual prostitution in the world *The Sims Online* (TSO).⁴⁵ Ludlow had developed an online journal, called the *Alphaville Herald*, which chronicled events within TSO.⁴⁶ Electronic Arts, the creator of TSO, subsequently banned Ludlow's avatar, wiping out the significant investment Ludlow had made in his reputation in that world.⁴⁷ The *Alphaville Herald* was forced to move to a different virtual world—*Second Life*—and ceased reporting on events within TSO.⁴⁸

From the Ludlow event we can see that game gods can use their power to banish users in order to suppress reports of situations that are dangerous to and exploitative of children.⁴⁹ And one can imagine a legislative response to the Ludlow banning—for example, a law that protects whistle blowing in virtual worlds—that would protect both speech and children. Such a law could be modeled on federal whistleblower statutes that forbid reprisals against those who reveal certain types of information.⁵⁰

44. See *Reno v. ACLU*, 521 U.S. 844, 849 (1997) (noting the tension between the protection of minors and the First Amendment guarantees of free speech).

45. See LUDLOW & WALLACE, *supra* note 43, at 127–43 (discussing teen virtual prostitution in the world TSO).

46. See *id.* at 5–8 (describing the establishment and works of the *Alphaville Herald*).

47. See *id.* at 12–14 (describing Ludlow's expulsion from TSO).

48. *Id.* at xv.

49. See *id.* at 13 (identifying a situation in which a person publishing questionable materials got banned from a virtual world).

50. See, e.g., 29 U.S.C. § 623(d) (2006) ("It shall be unlawful for an employer to

But the conflict between speech and child protection cannot be entirely assumed away. There are some things that adults should be able to say and do that children certainly should not hear or see. Working out rules that permit children and adults to safely interact, while protecting the maximum amount of speech possible is therefore a worthwhile goal.

A full treatment of First Amendment and child protection issues is beyond the scope of this Article. Instead, this subpart examines the First Amendment literature as applied to virtual worlds, and then looks at some Supreme Court cases that have encouraged technological filtering as a less restrictive means for blocking content to minors, while permitting adults to speak freely.

This Article is not the first time that the First Amendment has been invoked in discussions of virtual worlds. Jack Balkin, Eric Goldman, Peter Jenkins, and I have all talked about the First Amendment from a number of different perspectives.⁵¹ The initial difficulty with applying the First Amendment to virtual worlds has been that the most common censors—the game gods—are private parties. Game gods are not yet governments, although they trend heavily in that direction.⁵² As a result, most virtual world applications of the First Amendment founder on the state-action doctrine.

Therefore, it is worth noting that, for the purposes of this Article, little of the state-action debate matters. This Article considers the specter of real-world legislative action, not private censoring of speech. Real-world law and

discriminate against any of his employees or applicants . . . because such individual . . . has opposed any practice made unlawful by this section"); 42 U.S.C. § 12203(a) (2000 & Supp. V 2005) ("No person shall discriminate against any individual because such individual has opposed any act or practice made unlawful by this chapter or because such individual made a charge, testified, assisted, or participated in any manner in an investigation, proceeding, or hearing under this chapter."); *id.* § 300j-9(i)(1) (preventing discrimination against an employee for turning in an employer in violation of provisions of this section); 31 U.S.C. § 3730(h) (2000 & Supp. V 2005) (providing for relief for employees who are punished by an employer as a result of complying with the provisions of this section); 29 U.S.C. § 206(d) (prohibiting discrimination against whistleblowers in the sexual discrimination context).

51. See Balkin, *supra* note 39, at 2090–98 (discussing how real-world law is used to regulate freedom in virtual worlds); Joshua Fairfield, *The God Paradox*, 89 B.U. L. REV. 1017 (2009); Eric Goldman, *Speech Showdowns at the Virtual Corral*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 845, 850–54 (2005) (arguing that virtual worlds are not distinguishable from other online providers and therefore we should not create special speech rules for virtual worlds); Jenkins, *supra* note 39, at 18 ("[Massively Multiple Online Role Playing Games] are the leading edge of a coming virtual world that will eventually supersede the current structure of the Internet, providing a world-wide three-dimensional immersive platform in which we will shop, play, socialize, travel and work.").

52. Cf. Balkin, *supra* note 39, at 2043–44 (commenting that virtual worlds are developing into more than just gaming, replicating many aspects of the real world); Jenkins, *supra* note 39, at 1–3 (describing the similarities between a virtual world community and a real world community).

legislation that target online speech because of its content raise no difficulty of state-action.

The second common snag that First Amendment accounts encounter in virtual worlds is the speech/conduct dichotomy.⁵³ The fighting question is whether communications via virtual worlds are speech, expression, association, or conduct devoid of expressive content.⁵⁴ Every novel communications technology must surpass this hurdle. For example, the Court did not recognize that movies were protected expression until 1952.⁵⁵ Recognition that the First Amendment protects video games seems to be more quickly forthcoming.⁵⁶ Players in virtual worlds communicate using traditional modes of speech—voice and writing—but also can communicate via the shared three-dimensional virtual environment.⁵⁷ Thus, virtual world technology is an even richer medium of expression than traditional writing, speech, or movies.⁵⁸ There is, therefore, every chance that courts will seamlessly recognize that First Amendment protection applies to expression in a virtual world just as it does to an actor on stage.⁵⁹

53. See *United States v. O'Brien*, 391 U.S. 367, 376 (1968) ("[W]hen 'speech' and 'nonspeech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the nonspeech element can justify incidental limitations on First Amendment freedoms."); see also *Rice v. Paladin Entm't*, 128 F.3d 233, 243 (4th Cir. 1997) ("It is equally well established that speech which, in its effect, is tantamount to legitimately proscribable nonexpressive conduct may itself be legitimately proscribed, punished, or regulated incidentally to the constitutional enforcement of generally applicable statutes.").

54. *Rice*, 128 F.3d at 243.

55. See *Burstyn v. Wilson*, 343 U.S. 495, 502 (1952) (overturning its 1915 decision in *Mutual Film Corp. v. Industrial Commission of Ohio*, 236 U.S. 230 (1915), in which it had determined that movies were businesses, not speech).

56. See, e.g., *Interactive Digital Software Ass'n v. St. Louis County*, 329 F.3d 954, 957 (8th Cir. 2003). It states:

If the first amendment is versatile enough to shield [the] painting of Jackson Pollock, music of Arnold Schoenberg, or Jabberwocky verse of Lewis Carroll, we see no reason why the pictures, graphic design, concept art, sounds, music, stories, and narrative present in video games are not entitled to a similar protection. The mere fact that they appear in a novel medium is of no legal consequence.

Id. (citations and quotations omitted).

57. See Balkin, *supra* note 39, at 2046 ("Much of what goes on in virtual worlds should be protected against state regulation by the First Amendment rights of freedom of expression and association."); see also *id.* at 2053 ("If the state regulates virtual worlds because of the ideas expressed by the players and designers, the free speech principle is surely violated.").

58. See *id.* at 2054–55 ("[M]assively multiplayer games and virtual worlds are becoming recognized as media for the communication of ideas, including every sort of representation and recreation of human interaction Virtual worlds are a medium of expression, a medium in which you can say things and express things.").

59. See *id.* at 2056. Balkin states:

Even if players' interactions in virtual worlds were deemed mere conduct rather than speech—and they are not—it would merely beg the question of when conduct constitutes protected expression.⁶⁰ For example, erotic conduct—say, dance—is protected.⁶¹ If Congress wishes to target conduct due to its erotic content, it faces a quite high barrier.⁶² On the other hand, if a government rule is unrelated to the content of the expression and only imposes incidental burdens on expression, it is likely to be upheld.⁶³ Thus, Congress may instead seek a content-neutral approach by restricting only a nonexpressive component, that is, access by minors, but such an approach may not chill protected speech.⁶⁴

In addition, games, particularly massively multiplayer games and virtual worlds, have creative and interactive features that, in some ways, make them even more like speech than motion pictures. (Just as the ability to create games is part of the freedom to design, the ability to interact within games is part of the freedom to play.) With massively multiplayer games, it is even more obvious that what is going on is participatory. The most sophisticated multiplayer games allow you to tell your own stories and add things to the world in which you are playing. If movies are media for the communication of ideas, so too are massively multiplayer games.

Id.; see also *id.* at 2057 ("Thus, multiplayer games are not like boxing or hockey, whose claims to free speech protection are tenuous. A better analogy is improvisational theater.").

60. See *Texas v. Johnson*, 491 U.S. 397, 406–07 (1989) ("It is, in short, not simply verbal or non-verbal nature of the expression, but the government interest at stake, that helps to determine whether a restriction on that expression is valid.").

61. See, e.g., *Schad v. Borough of Mount Ephraim*, 452 U.S. 61, 66 (1981) ("Nor may an entertainment program be prohibited solely because it displays the nude human figure . . . nude dancing is not without its First Amendment protections from official regulation.").

62. See *Johnson*, 491 U.S. at 406. It states:

The Government generally has a freer hand in restricting expressive conduct that it has in restricting the written or spoken work. It may not, however, proscribe particular conduct *because* it has expressive elements. . . . A law *directed* at the communicative nature of conduct must, like a law directed at speech itself be justified by the substantial showing of need that the first amendment requires.

Id. (citations and quotations omitted).

63. See *Rice v. Paladin Entm't*, 128 F.3d 233, 243 (4th Cir. 1997); see also Robin Fretwell Wilson, *Sex Play in Virtual Worlds*, 66 WASH. & LEE L. REV. 1127, 1163 (2009) (citing RODNEY A. SMOLLA, LAW OF DEFAMATION § 4.63 (2d ed. 2008)).

64. See *Johnson*, 491 U.S. at 407. The Court stated:

Thus, although we have recognized that where 'speech' and 'non-speech' elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the non-speech element can justify incidental limitations on First Amendment freedoms, we have limited the applicability of *O'Brien's* relatively lenient standard to those cases in which the government interest is unrelated to the suppression of free expression.

Id. (citations and quotations omitted).

Claims that the government seeks to regulate conduct, not speech, will not avail if the regulation overly impacts the ability of adults to engage in constitutionally protected expression.⁶⁵ As the Court noted:

Here the Government wants to keep speech from children not to protect them from its content but to protect them from those who would commit other crimes. The principle, however, remains the same: The government cannot ban speech fit for adults, simply because it may fall into the hands of children The objective is to prohibit illegal conduct, but this restriction goes well beyond that interest by restricting the speech available to law-abiding adults.⁶⁶

There are two basic problems. First, adults may unwittingly interact with minors who hide behind internet anonymity.⁶⁷ If unwitting interactions are penalized, adults cannot speak with one another for fear that the person they are interacting with may be a hidden minor.⁶⁸ Avoiding liability would require all adults to limit every word and act to those fit for children.⁶⁹ Second, the imposition of age verification procedures, like credit card checks, would limit the ability of some adults to engage in protected expression.⁷⁰ As discussed below, where access restrictions for minors would functionally shut down protected expression among adults, courts seek less restrictive alternatives.⁷¹

Because of these considerations, the Supreme Court has long maintained that the Constitution bars legislators from functionally restricting adults to content "only . . . fit for children."⁷² "The precedents establish . . . that speech within the rights of adults to hear may not be silenced completely in an attempt to shield children from it."⁷³ In the internet context, this has meant that, where users of a service are anonymous, criminal liability cannot ride on the unwitting communication of harmful material to users who turn out to be children.⁷⁴ For

65. *Infra* note 82.

66. *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 252–53 (2002).

67. *Infra* note 74 and accompanying text.

68. *Infra* note 75 and accompanying text.

69. *Infra* note 72 and accompanying text.

70. *Infra* note 92.

71. *Infra* note 84.

72. *See, e.g., Butler v. Michigan*, 352 U.S. 380, 381–83 (1957) (determining legislative restriction on sale of books "tending to the corruption of the morals of youth" unconstitutional because "[t]he incidence of this enactment is to reduce the adult population . . . to reading only what is fit for children").

73. *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 252 (2002).

74. *See Reno v. ACLU*, 521 U.S. 844, 855 (1997) (holding sections of Communications Decency Act unconstitutional in part because "there is no effective way to determine the identity or age of a user").

example, "[k]nowledge that, for instance, one or more members of a 100-person chat group will be minor—and therefore that it would be a crime to send the group an indecent message—would surely burden communication among adults."⁷⁵ Thus, the Court held that the communication of pornographic material to a person that the content provider does not know to be a child cannot be grounds for criminal liability because to do so would "inevitably curtail a significant amount of adult communication on the internet."⁷⁶

Moreover, this principle is not curtailed by the characterization of a given statute as strict liability. The Court has repeatedly held that a criminal defendant must have some minimum chance to determine whether she is engaged in an activity subject to strict regulation in order for the imposition of criminal penalties to be constitutional.⁷⁷ With regard to expression, "the Court has held that punishment based on strict liability with regard to the elements that deprive the conduct of First Amendment protections is unconstitutional."⁷⁸ The difference between an adult who encounters a child in the real world and one who encounters an anonymous person who could or could not be a child in a virtual world is significant. Even if we hold the adult responsible for her real-world actions without considering her knowledge of the minor's age, we at least feel satisfied that she had some chance or opportunity to determine who she was dealing with. Not so in a virtual world.

Congress has had three bites at this apple. The Communications Decency Act (CDA),⁷⁹ the Children Online Protection Act (COPA),⁸⁰ and the Child

75. *Id.* at 876.

76. *See id.* (noting that it would be overly burdensome to First Amendment rights to make liable senders who do not know if the receiver is a minor).

77. *See Staples v. United States*, 511 U.S. 600, 619–20 (1994) (reversing conviction of unwitting owner of converted machine gun); *United States v. X-Citement Video*, 513 U.S. 64, 66 (1994) (finding an adult video vendor who unwittingly sold tapes that included an actress who was a minor not criminally liable). *See generally* Alan C. Michaels, *Constitutional Innocence*, 112 HARV. L. REV. 828 (1999) (detailing constitutional restraints on use of strict liability). Even where the Court has condoned strict liability, it has required at a minimum that the defendant have been in such a situation as to be aware of the danger that the activity would be strictly regulated. *See Staples*, 511 U.S. at 606 (noting that even public regulatory "strict liability" crimes require at a minimum that "a defendant know[] that he is dealing with a dangerous device of a character that places him in responsible relation to a public danger, [such that] he should be alerted to the probability of strict regulation") (citations omitted).

78. Michaels, *supra* note 77, at 868.

79. *See* Communications Decency Act of 1996, 47 U.S.C. §§ 230, 560–561 (2000 & Supp. V 2005) (providing restrictions on the transmission of information based on content).

80. *See* Children Online Protection Act, 47 U.S.C. § 231 (2000 & Supp. V 2005) (providing restrictions of access by minors to materials commercially distributed by means of the World Wide Web).

Pornography Prevention Act (CPPA)⁸¹ all had similar problems.⁸² Each was struck down. The reasoning was straightforward. Congress can only burden speech if it uses the least restrictive means available to it.⁸³ Traditionally, this has meant that if Congress could achieve its goal through a different regulation that restricted less speech, then the more restrictive legislation could not pass constitutional muster.⁸⁴

In internet cases, the Court has imported self-help filtering technologies of communities into this constitutional test. If filtering would protect children from smut, the Court reasoned, then a broad government law providing for liability to people who convey harmful material to minors is not necessary.⁸⁵ The hook to government action is that Congress could promote filtering through legislative means.⁸⁶ Further, the Court expressly welcomed the application of filtering technologies to keep children safe in many different forms of internet communication. Thus, the Court noted that "filters also may be more effective because they can be applied to all forms of internet communication . . . , not just the World Wide Web."⁸⁷

This is an invitation to apply filtering technologies to virtual worlds. To make the case concrete: It is possible to filter reality in a virtual world in the way that we can filter websites on the ordinary Internet.⁸⁸ A simple version of

81. See Child Pornography Prevention Act of 1996, 18 U.S.C. § 2252A (2006) (providing restrictions regarding activities relating to child pornography).

82. See *Ashcroft v. ACLU*, 542 U.S. 656, 670 (2004) (affirming the grant of a preliminary injunction prohibiting enforcement of COPA upon a finding that plaintiffs were likely to prevail on the claim that legislation violated the First Amendment by burdening adults' access to some protected speech); *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 251, 256 (2002) (finding that numerous provisions of CPPA violated the First Amendment); *Reno v. ACLU*, 521 U.S. 844, 870 (1997) (finding provisions of CDA prohibiting transmission of obscene or indecent communications to minors to be content-based blanket restrictions on speech and therefore violative of the First Amendment).

83. See *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 814 (2000) ("[T]he objective of shielding children does not suffice to support a blanket ban if the protection can be accomplished by a less restrictive alternative.").

84. See *id.* at 818 ("Technology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us."); see also *Ashcroft*, 542 U.S. at 666 ("[A court] asks what is the least restrictive alternative that can be used to achieve that goal The court should ask whether the challenged regulation is the least restrictive means among available, effective alternatives.").

85. See *Ashcroft*, 542 U.S. at 667–68 (finding that because the Government failed to introduce specific evidence proving that filtering technologies are less effective than the legislative restrictions, the legislative restrictions were enjoined).

86. *Id.* at 669.

87. *Id.* at 668.

88. See *infra* Part III (discussing filtering technology as an alternative to legislation).

this technology is already ubiquitous. A user who does not wish to interact with another user can enter the term "/ignore." As of that point, the two parties simply cannot speak with one another within the game. More advanced applications will be discussed below.

The speech/conduct distinction may yet yield hard cases in virtual worlds.⁸⁹ But it is not hard to discern that Congress's current apparent regulatory trajectory will run afoul of established case law. For example, in its consideration of virtual worlds regulation, Congress has again taken aim at content, not conduct, by directing the Federal Trade Commission (FTC) to report on the availability of explicit material to children in virtual worlds.⁹⁰ Moreover, commentators expect that the FTC will recommend requiring age verification by credit card to prevent children from accessing virtual worlds that adults use.⁹¹ Both the content-targeting and credit card verification elements have been previously rejected by the Court.⁹² The answer should not change merely because virtual worlds are a novel technology. A more measured legislative approach would promote the development and use of filtering and parental control technologies in virtual worlds, in lieu of either a blanket ban on certain content due to the risk of children accessing it, or of anonymity stripping measures such as mandatory credit card verification.

C. *The Effect of Isolation on Children*

It is not enough to note that adult discourse would be fundamentally threatened by the imposition of legal liability for unwitting interaction with avatars run by children. This Article also argues that internet segregation will render children vulnerable. Once all decent adults are driven away from children—by virtue of their fear of being overheard or duped—then only predators will remain among the children.⁹³ Predators, who of course have no

89. See Wilson, *supra* note 63, at 1164–71 (arguing that virtual sex may be sanctioned as conduct consistent with the First Amendment).

90. See *supra* note 1 (noting the existence of an urge to legislate).

91. *FTC May Urge Virtual Age Verification*, NAT'L J. ONLINE, July 27, 2009, <http://techdailydose.nationaljournal.com/2009/07/ftc-may-urge-virtual-age-verif.php> (last visited Sept. 29, 2009) (on file with the Washington and Lee Law Review).

92. See *Ashcroft v. ACLU*, 542 U.S. 656, 667 (2004) (determining that age verification via credit card did not save COPA, because "[u]nder a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves or provide their credit card information").

93. See Szoka & Thierer, *supra* note 19, at 30 ("The effect of age stratification on truly bad actors is likely to be marginal at best—or harmful at worst: Building walls around adolescents through age-verification might actually make it *easier* for predators to target

qualms about passing themselves off as children to access online spaces, will not be deterred.⁹⁴ This is hardly the state of affairs that the law ought to strive to create.

Predators desire to get children alone, and to generate separation and secrecy between the child and parents or other adults who might stop the abuse.⁹⁵ Internet predators are no different, seeking isolated corners of the Internet, generally overpopulated by children, for their abuse.⁹⁶ Isolation and secrecy are the predator's watchwords.⁹⁷ Driving adults and children apart in virtual worlds achieves both of the predator's ends: It gives the predator an adult-free zone in which to operate,⁹⁸ and it gives the predator a free hand to inculcate secrecy and attempt to arrange a real-world meeting with the child.⁹⁹

Finally, separating adults from children in online spaces will increase the risk and virulence of bullying or other adolescent-to-adolescent harm.¹⁰⁰ This

teens . . .").

94. See L. Alvin Malesky, Jr., *Predatory Online Behavior: Modus Operandi of Convicted Sex Offenders in Identifying Potential Victims and Contacting Minors over the Internet*, 16 J. CHILD SEXUAL ABUSE 23, 24 (2007) ("Because the Internet can provide anonymity for its users, adults can misrepresent their age and even present themselves as adolescents while interacting with actual minors online.").

95. Jon R. Conte et al., *What Sexual Offenders Tell Us About Prevention Strategies*, 13 CHILD ABUSE & NEGLECT 293, 293 (1989) (noting that predation "involved efforts to separate children from other adults who might protect them").

96. See Malesky, Jr., *supra* note 94, at 26 (noting that "[t]wenty-five individuals (81%) reported visiting chat rooms geared towards minors for the purpose of meeting children/adolescents").

97. See generally Conte et al., *supra* note 95 (describing the behavior of sexual predators and prevention strategies); Janis Wolak et al., *Online "Predators" and Their Victims*, 63 AM. PSYCHOLOGIST 111, 118 (2008) (commenting that risky behavior on the part of adolescents included chatting to unknown parties); Catherine D. Marcum, *Interpreting the Intentions of Internet Predators: An Examination of Online Predatory Behavior*, 16 J. CHILD SEX ABUSE 99 (2007) (discussing the increased amount of child sexual abuse on the Internet, the often blatant tactics used by online predators to pursue this abuse, and how they are continuing to successfully manipulate children with them).

98. See Conte et al., *supra* note 95, at 297 (noting that "isolation, closeness, [and] contact are more important than verbal seduction" for a sexual predator).

99. See generally Stefan C. Drombrowski et al., *Protecting Children from Online Sexual Predators: Technological, Psychoeducational, and Legal Considerations*, 35 PROF. PSYCHOL. RES. & PRAC. 65 (2004) (reviewing the general strategies of sexual perpetrators and their characteristics, as well as the online strategies and characteristics of the cyber sexual predator); Malesky, Jr., *supra* note 94 (discussing the online activity of thirty-one men who perpetrated or attempted to perpetrate contact sex offenses against minors with whom they communicated via the Internet).

100. See PALFREY & GASSER, *supra* note 3, at 95 ("The data that we do have demonstrate that inasmuch as we should be worrying about the danger of violence on the Internet, we should be worrying about kids hurting each other psychologically—and not as focused, as we seem to

risk is as serious a consideration as adult-to-child harm, if only because it is far more common.¹⁰¹ A major restraining force on child-to-child harm is the presence of responsible adults, who can de-escalate the behavior.¹⁰² Creating virtual playgrounds without adults will increase the incidence and severity of child-to-child harm.¹⁰³ Driving responsible adults—including parents—out of virtual worlds that parents had heretofore shared with children would achieve precisely this result.¹⁰⁴

Instead of segregating children from adults, legislators wishing to protect children should foster and promote the development of tools that parents and teachers can use to protect children in virtual worlds.¹⁰⁵ The best technology for doing this is unsurprisingly the same technology that the Court has previously turned to in its prior internet jurisprudence: Filtering.

III. Filtering and Virtual Worlds

Filtering technology presents a unique opportunity for virtual worlds: As noted in Part II.B, above, if virtual-world filtering technology is good enough, Congress must promote this technology rather than enact broad regulatory mandates that are intended to protect children, but inhibit speech. At the outset, it is worth distinguishing between filtering of virtual worlds and filtering within virtual worlds. Virtual worlds can be filtered just like websites. Many virtual worlds, like *Club Penguin* or *Webkinz*, are in fact websites. Thus, regular internet filters will work for parents who wish to filter their children's access to virtual worlds. This kind of filtering technology has been discussed at length in the case law.¹⁰⁶ This Article, therefore, focuses on filtering within virtual worlds. The question is whether the filtering technology available within virtual worlds is good enough to both provide the badly needed protection for children and stave off parentalism legislation. This Article submits that filtering technology in virtual worlds is impressive but still of

be, on adults hurting kids physically.").

101. *Id.*

102. *Id.*

103. *Id.*

104. See Malesky, Jr., *supra* note 94, at 29 ("[P]arents and/or guardians should be involved with their children's online activity. They should know who their children communicate with via the Internet as well as not allow them to spend inordinate amounts of time online.").

105. See PALFREY & GASSER, *supra* note 3, at 110 ("Parents and teachers need to become a much bigger part of the solution, and soon.").

106. *Supra* Part II.B.

limited availability to players, and that filtering could and should be made better still by the introduction of flagging and reputation systems.

A. Basic Chat Filtering

The state of the technology is changing rapidly, but as of the writing of this Article, there are some basic discernable trends. First, filtering of text, as regards sexual, scatological, or otherwise profane language, is already largely possible.¹⁰⁷ If players do not desire to hear coarse language, then they may simply turn on the language filter and the offensive language will be edited out.¹⁰⁸ Moreover, characters may filter one another by simply turning off the ability of another person to contact them via the ignore command.¹⁰⁹

But these simple filters will not be sufficient to fully protect children or fend off legislation. Current filters will not prevent work-arounds, such as the substitution of numbers for letters (in oft-mocked "Leetspeak") or other inventive use of characters to circumvent controls. Moreover, current filters do not do a good job of filtering inappropriate user-generated content.¹¹⁰ Thus, the following sections discuss not only the power to edit the text that a person sees in a computer-mediated environment but also the power to, in fact, edit that reality so that objectionable content is filtered out for one person, but not for others.

B. Filtering Reality: Instancing and Quest-Phasing

In a virtual world, reality itself can be edited on an individual basis. Instancing technology is especially promising. The largest advance in game play over the past several years has been the advance in the degree to which the

107. Cf. *World of Warcraft*, Community Site, <http://www.worldofwarcraft.com> (last visited Sept. 29, 2009) (providing basic filtering options for users).

108. Cf. *World of Warcraft*, Blizzard Support, <http://us.blizzard.com/support/article.xml?locale=en-US&articleId=20455> (last visited Sept. 29, 2009) (providing a language filter) (on file with the Washington and Lee Law Review).

109. Cf. *id.* (providing an ignore command filter).

110. Cf. *id.* (providing filtering options, but with limitations restricting the effectiveness of the filtering).

shared experience of a virtual world can be edited.¹¹¹ Players now do not share the same reality, they share overlapping experiences.¹¹²

The original problem that instances were meant to address was that of scarce resources. Imagine trying to kill Greg the Goblin to get his magical sword. If you must compete with everyone else in the virtual environment for the chance to kill Greg, you may suffer serious frustration. Other players are in line to kill Greg, too. Even if Greg "respawns," or reappears (to give another player a chance to enjoy the same content), other players may simply "spawn camp" or steal the kill.

To deal with problems of spawn camping and killstealing, game designers invented instances.¹¹³ If Greg lives in an instanced cave, when you enter the cave, you actually enter your own pocket universe. In your own "instance" of the cave, Greg is always there. Any other player who enters Greg's cave will encounter Greg—but not you.

How is this possible? Whenever you enter the cave, the game server generates a one-off copy—a single-player version of the content—of Greg's cave. Within that cave, you and your friends are the only ones who exist. Other people cannot disrupt your game experience. But this pocket universe is still connected to the larger game world. Once you defeat Greg and return to town, everyone can see the magical sword you won. In town, you have rejoined the rest of the shared experience.

However, in order to experience instanced content, players had to separate themselves from the rest of the shared experience for a while.¹¹⁴ The next challenge was to make it possible to "edit" reality so that people who shared a common space were actually experiencing different realities in some respects. This next step was called quest-phasing.

Quest-phasing permits a static world to appear to change.¹¹⁵ The original problem was this: Imagine, in a non-instanced, non-phased world, player *A* kills Greg the Goblin. Either the game server now considers Greg "dead," and thus no other player can experience that content, or the game server "respawns"

111. See CASTRONOVA, *supra* note 25, at 118–19 (explaining the mechanism of "instancing" content which "occurs when a player triggers the creation of content that is accessible to her and no one else").

112. See *supra* note 111 and accompanying text (describing instancing and its effects).

113. See CASTRONOVA, *supra* note 25, at 118–19 (describing instances and its purpose).

114. See *supra* notes 111, 113 and accompanying text (describing instances and discussing their affect on gaming).

115. See Interview with J. Allen Brack, Producer, *Wrath of the Lich King*, in Leipzig, F.R.G. (Aug. 22, 2008), http://www.eurogamer.net/articles/world-of-warcraft-wrath-of-the-lich-king_9 (last visited Sept. 29, 2009) (discussing the use of quest phasing rather than instancing in *Wrath of the Lich King*) (on file with the Washington and Lee Law Review).

Greg, leading to a disruption of the suspension of disbelief—"hey wait," says player *A*, "I just killed that guy. What's he doing still walking around, much less fighting player *B*?" Thus, if one player's act changed the world, that disrupted the experience of other players, who wished to perform the same quest. (Of course, the alternative—creating new quests for every player based on the prior actions of other players—is completely impossible from a design standard.)

Quest-phasing fixed this problem.¹¹⁶ If the quest to kill Greg the Goblin is phased, and if player *A* kills Greg, then for player *A*, Greg is indeed dead. But because player *B* has not killed Greg, then for player *B*, the goblin still lives. Note that for all other intents and purposes, player *A* and player *B* share a reality—each sees what the other sees, they can talk, go on other quests together. Their realities differ only when it comes to Greg.

Instancing and quest-phasing show that the technology exists to permit players to edit their realities without sacrificing the overlap, or shared experience, that makes virtual worlds so interesting. The technology filters the world based on the players' past experiences.¹¹⁷ It is not difficult to see how the technology might be extended in the direction of filtering other content. Just as the goblin might exist for player *B* but not player *A*, so grown-up content might exist for player *A*, an adult, but not player *B*, a child. This reality-editing function could extend to other players as well. A player *C* might well exist for *A*, but not for *A*'s child, *B*. (This is already the case with conversation—*B* can turn *C*'s ability to speak to *B* off.)¹¹⁸

These technologies do not exist in all virtual worlds, nor do they work the same way in every virtual world. But the theme—that filtering works in virtual worlds as well or even better than on the mainstream Internet—ought to give parentalist legislators pause. This opportunity also should give game designers food for thought. Filtering technology has a long way to go in virtual worlds. The most powerful technologies are not in the hands of the players—only the game god can spawn an instance or set up quest-phasing. Game gods ought to give players access to good filters if they wish to avoid regulation—especially when it comes to parents who are looking for ways to filter their children's in-game experiences. Further, game gods ought to make the filters that they have

116. See *id.* ("As you bring [the villagers] back to your quest hub, those villagers are there permanently for you, whereas if somebody who hasn't done the quest shows up, they don't see them.").

117. See *id.* (noting that people who complete certain quests will be able to see common things, but those that have not completed the quest will not be able to see those things).

118. See *supra* notes 107–10 and accompanying text (discussing the filtering technology normally available).

already developed even better—by combining filtering technology with flagging and reputation systems, as discussed below.

C. Making Filtering Better

Filtering can be made even more effective if one embraces its counterpart, flagging. Where filtering edits out content from existence, flagging permits creators of content, or speakers, to identify their content in order to receive a safe harbor and permit better filtering.¹¹⁹ Suppose one were to adopt a rule granting an absolute safe harbor to any speaker or creator of "adult" content (and by this I mean content fit for adult consumption, not merely or mostly sexual content) if that person "flags" the content, or identifies it as containing material for adults.

In turn, filtering software can more easily read the flag. Instead of having to guess whether content is safe or not, the filter can automatically identify and filter out self-identified adult content. In this way, violent imagery, strong language, and even boring academic articles could be flagged as "adult" to prevent damage to unwitting children. A safe harbor for flagged content thus makes filtering more effective.

People could even flag their own conversations. It is common practice in a virtual world to speak in several different "channels" simultaneously. A "say" command causes everyone in the local area to hear your comment. A "gu" command causes only your guild members to hear you speak, no matter where they are in the world. Other channels exist for specific purposes: A "trade channel" permits parties to hawk their virtual wares, while a "local defense channel" permits the organization of player-versus-player combat within the world.

The trick is that channels are a simple form of instancing: You can speak in multiple channels while sharing a simulated physical space with someone else, and the people you are near do not experience all the channels that you do. Thus, it is perfectly possible to have an adult conversation in one channel and a more "PG" conversation in another channel, without spillover. (Okay, there is the occasional spillover, called a "misstell," that is the stuff of internet hilarity, but the point remains a good one.)

119. Cf. What is Flagging? Parenthood.com, <http://www.community.parenthood.com/topic/4967> (last visited Sept. 29, 2009) (noting that when someone flags a site, a report is sent to a group of individuals who will then check out the site) (on file with the Washington and Lee Law Review).

People could thus flag their channels "PG" or "M," the way they currently select channels for other purposes. And it goes without saying that people who do not wish to hear the content would not be obliged to join the channel. Further, parents could set filters such that a child could not access such channels. In short, it is possible to protect adult speakers and child listeners without legislation that threatens to split up virtual worlds.

Once one embraces flagging as a way of enhancing filtering technology, there are all sorts of ways to make filters better. Players might flag not only their own content but also one another. One major system for self-regulation through e-commercial sites is a reputation system. eBay, for example, permits parties to rate one another based on prior commercial experience.¹²⁰ This technology is already readily apparent in forum bulletin boards. Many online fora are choked with random, irrelevant, or obnoxious posts. The forum host could opt to review each post, and remove offensive or irrelevant content.

Instead, many sites use a rating system. Posts are rated on their usefulness by the readers.¹²¹ If a post falls below a certain rating, it is not displayed. Thus, objectionable content is edited nearly out of existence by the player rating system. The content is still available, but special effort must be made to access low-rated content.

A reputation add-on to a filtering system could do much to increase the value of the underlying system.¹²² If player *A* encounters player *B*, who has a bad reputation, player *A* may already have filters in effect such that player *B* does not exist as far as *A* is concerned.

Of course reputation can be gamed, primarily through the practice of reanonymization, where a party who has an unsavory reputation creates a new online identity in order to escape her bad name. But reanonymization does not always—or even often—work because people refuse to deal with someone who has no reputation. For example, in the virtual world *Second Life*, avatars that have been created very recently are not permitted into many areas because they are likely to be reanonymized users who are attempting to "grief" (harass) other

120. See Feedback Forum, eBay, <http://pages.ebay.com/services/forum/feedback.html> (last visited Sept. 29, 2009) (providing an overview of eBay's user rating system) (on file with the Washington and Lee Law Review).

121. Cf. Internet Movie Database, <http://www.imdb.com> (last visited Sept. 29, 2009) (allowing users to rate the usefulness of other users' comments).

122. See BOELLSTORFF, *supra* note 24, at 228 (discussing the evolution of the user rating system in *Second Life*); CASTRONOVA, *supra* note 25, at 23 ("Human societies rely so much on reputation for their basic functioning that online anonymity seems unlikely to persist in any significant way.").

players on an "alt" (alternative character or identity) while preventing reputational harm to that player's "main" (primary identity).¹²³

D. Commerce, Anonymity, and Filtering

If anonymity is the shield of bad actors, commerce is the sword which pierces that shield. If real money is being exchanged, both companies and consumers must know with whom they are dealing. Thus, the oft-maligned intrusion of real-world economics into virtual worlds is a powerful source of trust and protection for players of all ages.

In COPA, described above, Congress attempted to mandate credit card numbers in an age-verification system for internet users.¹²⁴ This served two purposes. First, the credit card number provided pretty good evidence that the person was not a minor.¹²⁵ Second, the credit card number tied the customer to a real-world identity.¹²⁶ Because of this second factor, the Court found that requiring the disclosure of credit card information chilled legitimate speech, and that the credit card requirement was not the least restrictive means by which Congress could achieve its goals.¹²⁷

But there is nothing invasive or chilling about facilitating voluntary disclosure of information by a customer in order to improve filtering. For example, in the virtual world *Second Life*, if a customer uses a credit card in conjunction with an avatar, then that avatar's publicly-available profile discloses this fact and states: "[P]ayment information on file."¹²⁸

If a user is attempting to remain anonymous from the game god, of course no payment information will be used. But if payment information is on file, this means that the real-world identity behind the avatar may be subpoenaed from the game god.¹²⁹ An additional fact: Many game worlds record their

123. See BOELLSTORFF, *supra* note 24, at 235 ("[T]he ability to join Second Life without providing any identifying information made many residents concerned; they complained that the grid was being flooded with persons bent on grieving, and also that it would be easier for children to enter Second Life, raising issues of ethics and legal liability.").

124. See *Ashcroft v. ACLU*, 542 U.S. 656, 662 (2004) (providing the language of the statute).

125. See *id.* (noting that the statute allows for the establishment of an affirmative defense if a website seeks to identify users by requiring a credit card number).

126. *Id.*

127. See *id.* at 667 (finding filters to be less burdensome on First Amendment rights than restricting access online through legislation).

128. BOELLSTORFF, *supra* note 24, at 235.

129. See Tal Zarsky, *Privacy and Data Collection in Virtual Worlds*, in THE STATE OF PLAY: LAW, GAMES, AND VIRTUAL WORLDS 217, 221–22 (Jack M. Balkin & Beth Simone

players' conversations for customer service purposes.¹³⁰ Thus, revealing real-world information to the game god goes beyond a simple piercing of anonymity in the event that a player commits a bad act. In virtual worlds, the fact that another user has now disclosed her real-world identity to the game god is enormously useful in determining who to trust.

Online commerce is a powerful force for reducing online anonymity—and thus the threat of online bad acts—without government coercion.¹³¹ The elegance of this system is that it does not mandate disclosure of credit card information—as Congress attempted—but instead permits a user to self-identify as particularly worthy of trust.¹³² Those who wish to remain anonymous can do so. They will simply not be trusted as much, and may be subject to filtering, as discussed below.¹³³

This fits with norms in virtual worlds. "Alt" characters are often used, as noted above, to engage in bad acts, while "main" characters are much more rarely used for that sort of activity. A player who wishes to harass or grief another player will only rarely do so on her "main" character. And the more egregious the action, the more likely that a player will use an alternative account to commit the deed. Alts are, therefore, routinely distrusted in virtual worlds, since the chance of an alt being a reanonymized player is higher than the alt being simply a new player.

It is of course possible to combine these e-commercial identification techniques with filters. A child's filter could be set to edit out anyone who has not given their identity to the game god provider via a credit card number. In short, if a child can filter alts, they have removed a powerful tool used by griefers and harassers of all kinds.

IV. Necessary Law Enforcement in Virtual Worlds

Remember what this Article is not saying. This Article does not claim that virtual worlds should not ban sexual predators. They can and must. The KIDS

Noveck eds., 2006) (noting that the identity of a website user may be obtained through the use of the user's payment information).

130. See *id.* at 218, 221–22 (noting that conversation in virtual worlds can be stored and used for identification purposes).

131. BOELLSTORFF, *supra* note 24, at 234–35 (stating that government involvement is not necessary to obtain identification information from users if the users are involved with commercial activities).

132. *Id.*

133. See *id.* at 235 (commenting that the choice involved when deciding whether to identify oneself aids in separating the trustworthy from those not so trustworthy).

Act of 2008,¹³⁴ which provides social networking sites with access to the national sexual offender database, also provides civil immunity for suits based on using that database and excluding sex offenders from the social network.¹³⁵ Virtual world providers are social networks first and games second. Thus, virtual world game gods ought to have little difficulty claiming the civil immunity of the KIDS Act.

If the KIDS Act is the carrot, then state Attorneys General are the stick. State AGs have now sought, and received, settlements with Facebook and MySpace that require those sites to police their sites for predators and respond quickly to consumer complaints.¹³⁶ Although these site operators would be within their rights to stand on their CDA § 230 immunity¹³⁷ to claims premised on the bad acts of third parties, they have not chosen to take the risk, and have settled instead. Virtual world game gods would be wise to take notice: Improving filtering technology may affect specific attempts by Congress to legislate within virtual worlds, but good filters, as well as good procedures for responding to complaints, are also necessary to prevent claims from state AGs (as well as the negative publicity those claims generate).

Further, this Article does not argue that police ought not to enforce the law in virtual worlds. This Author has long argued that police and courts need no special adaptations to apply real-world law in virtual worlds. Certain applications of real-world law that do not take into account the unique nature of interactions in virtual worlds, however, run the risk of cyberbalkanization, as noted above.

For example, if police were to pursue claims of lewd and lascivious conduct toward virtual world denizens who had every reason to believe that they were engaged in conversations with other adults, this would first be a clear violation of the First Amendment principles set forth when the Supreme Court

134. See 42 U.S.C. § 16915a *et seq.* (2000 & Supp. V 2005) (stating requirements for sex offenders regarding websites).

135. See *id.* § 16915b(c)(5) ("A civil claim against a social networking website, including any director, officer, employee, parent, contractor, or agent of that social networking website, arising from the use by such website of the National Sex Offender Registry, may not be brought in any Federal or State court.").

136. See Nathan Olivarez-Giles, *Internet Social Sites Target Sex Offenders*, L.A. TIMES, Feb. 4, 2009, at C3 (stating that information on 90,000 sex offenders using MySpace was turned over to Connecticut Attorney General Richard Blumenthal's office in response to a subpoena); Jenna Wortham, *MySpace Turns over 90,000 Names of Registered Sex Offenders*, N.Y. TIMES, Feb. 4, 2009, at B4 (noting that MySpace was pressured into turning over the names of sex offenders in response to a subpoena); *Facebook Drops Sex Offenders*, *supra* note 6 (stating that Facebook has removed over 5,000 sex offenders from its site).

137. See 47 U.S.C. § 230 (2000 & Supp. V 2005) (noting protections and public policy rationale for providing some immunity to site operators).

struck down most of the CDA, COPA, and CPPA.¹³⁸ And, even if it were not, the enforcement of such rules against such parties would cause people either to abandon virtual worlds technology, or to balkanize the worlds.

Fortunately, police have been sensitive to online constitutional and cultural differences. Police in virtual worlds have followed the trend of chat room enforcement elsewhere. Police do not pursue virtual world denizens who honestly believe they are speaking to other adults, in the privacy of their own virtual homes or within adults-only clubs. Rather, police do the precise opposite: They pose as children, and target those who seek to turn virtual encounters with children into real-world encounters.¹³⁹

In sum, game gods can and should keep predators out of virtual worlds, and real-world police ought to find and arrest predators inside virtual worlds. But they ought to continue the practice of targeting those who seek out children for sex, rather than targeting anyone who unwittingly provides offensive content that is accessed by children.

V. Conclusion

Parents should play alongside their children. The law is no substitute for parental involvement and supervision. If the statutes that legislators enact, or the common law principles that courts deploy, place adults at risk for being in proximity with children, then adults will exit virtual worlds entirely or will move to separate worlds. This will increase the risk to children, both because responsible adults will not be present to blow the whistle on cultures of secrecy and isolation, and because parents will not be aware of the risks of their children's behavior since they will no longer share a context.

138. See *supra* notes 76–85 and accompanying text (discussing the cases that struck down most of the CDA, COPA, and CPPA as overly burdensome on First Amendment rights).

139. See Pat Kimbrough, *Sheriffs Ramp up Online Investigations*, HIGH POINT ENTERPRISE, Feb. 22, 2009, available at 2009 WLNR 3454063 (discussing the acts of the Piedmont Internet Crimes Against Children Task Force in trying to catch sexual predators); Todd South, *New Task Force Goes After Sex Predators*, CHATTANOOGA TIMES FREE PRESS, Aug. 12, 2008, <http://www.timesfreepress.com/news/2008/aug/12/catoosa-county-new-task-force-goes-after-sex-predator/> (last visited Sept. 29, 2009) ("A newly formed, multi-agency task force lets authorities go after online sex predators instead of waiting until they have a victim.") (on file with the Washington and Lee Law Review); *Eleven Arrested in Internet Sex Sting*, CINCINNATI POST, Apr. 17, 2007, at A2 (discussing the decision and results of the Kentucky Attorney General's choice to use impersonation to go after sexual predators). See generally Dateline NBC, *To Catch a Predator* (NBC television broadcast), available at <http://www.msnbc.msn.com/id/10912603> (detailing the efforts of task forces posing online in order to catch sexual predators).

Virtual worlds present a thrilling opportunity: They can put communities back together. Parents and children can and do play together in virtual worlds—not out of a sense of obligation by the parent, but because both parents and children find the games fun. Players from across the political spectrum achieve common goals and cooperate. Virtualization technology has a reverse balkanization effect, a regenerative effect on community. Laws that function to exile adults from these worlds both destroy the promise of the technology and actively decrease protection for children in virtual worlds.

