FREEDOM TO FILTER VERSUS USER CONTROL: LIMITING THE SCOPE OF § 230(C)(2) IMMUNITY

Nicholas Conlon†

Abstract

Section 230(c)(2) of the Communications Decency Act provides a safe harbor to Internet and software providers who use and/or distribute filtering technologies such as blocking software and search engines. Congress passed § 230 in order to incentivize the development of technologies that maximize users' control over what material they receive. But some courts have interpreted the language of § 230(c)(2) broadly enough to immunize providers who covertly and unilaterally block material to serve their own interests, as opposed to the interests of their users. This Article proposes an interpretation of § 230(c)(2) that is consistent with Congress's preference for user control technologies. Under my interpretation, a provider must satisfy one of two conditions in order to be immune from liability. First, the provider can show that its filtering technology exhibits user control. Alternatively, the provider can establish that it believed in good faith that the material it has filtered degraded the quality of its service for users.

TABLE OF CONTENTS

† J.D., 2012, Benjamin N. Cardozo School of Law. The author wishes to acknowledge the invaluable help of Felix Wu, Brett Frischmann, Eric Goldman, and Bill Jemas in the preparation of this Article.

I. INTRODUCTION

Section 230(c)(2) of the 1996 Communications Decency Act (CDA) provides a safe harbor to Internet and software providers who use and/or distribute filtering software.[1] Congress's objective in promoting the development of filtering software was to reduce children's access to pornography on the Internet.[2] During floor debates, Senator Feingold argued that voluntary use of filtering software by parents embodied the ideal of "user control"[3] because it would "empower[] people to make their own decisions,"[4] thereby obviating the need for Internet regulation that would reduce Internet communications "to the lowest common denominator—that which is appropriate for children."[5] The Supreme Court adopted this rationale in *Reno v. ACLU*,[6] where it invalidated a provision of the CDA that criminalized the "knowing" transmission of "obscene or indecent" messages over the Internet to a minor.[7] In holding that this provision violated the First Amendment, the Court reasoned that filtering software was a "less restrictive alternative" means of limiting children's exposure to Internet pornography.[8] Similarly, in the 2004 case *Ashcroft v. ACLU*,[9] the Court upheld an injunction against enforcement of the Child Online Protection Act (COPA)—Congress's revision of the CDA—on the basis that "[f]ilters . . . impose selective restrictions on speech at the receiving end, not universal restrictions at the source."[10]

In the years following the passage of § 230, filtering technology has

1. 47 U.S.C. § 230(c)(2) (2012).

2. Robert Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMM. L.J. 51, 53–57 (1996).

3. 141 CONG. REC. 16,015 (1995).

4. *Id.* at 16,016.

5. *Id.* at 16,014. For further analysis of this position, see Jerry Berman & Daniel J. Weitzner, *Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media*, 104 YALE L.J. 1619, 1629–37 (1995); Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 JURIMETRICS J. 629, 652–70 (1998); Christopher S. Yoo, *Technologies of Control and the Future of the First Amendment*, 53 WM. & MARY L. REV. 747 (2011).

6. Reno v. ACLU, 521 U.S. 844, 859–60 (1997).

7. *Id.* at 859–60 (quoting Telecommunications Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 133, *invalidated by* Reno v. ACLU, 521 U.S. 844 (1997)).

8. *Id.* at 874.

9. Ashcroft v. ACLU, 542 U.S. 656 (2004).

10. *Id.* at 667.

become more and more prevalent. Internet users rely on filtering software to block a wide variety of objectionable material besides pornography, such as spam e-mail, web page advertisements, viruses, and other harmful or unwanted material.[11] In many cases users rely on filters not to block any particular harmful material but to sift through the "avalanche" of material available on the Internet.[12] Search engines such as Google and Bing enable users to navigate through the voluminous Internet by filtering out all material that is irrelevant to a search term.[13] Web 2.0 providers, such as Facebook, Amazon, Flickr, and Yelp, integrate filtering tools into their platforms to help users select amongst vast amounts of user-generated content.[14] According to some commentators, the current diversity and sophistication of filtering technology vindicates § 230's policy of maximizing user control.[15]

But many critics question whether providers' filtering practices are consistent with their users' preferences. Jennifer Chandler recently argued that "selection intermediaries"—a term she uses to refer broadly to "search engines, software filters, Internet Service Providers (ISPs) that block or filter content, and spam blocklists"—"undermine the flow of information from speaker to listener . . . by censoring content and applying bases for discrimination that listeners would not have chosen."[16] Critics have provided several grounds in support of this position. First, filtering can enable an intermediary to further interests that are unrelated to users' preferences, such as improving its market position by filtering competitors' advertisements and services or by filtering

11. Eric Geier, *PC Security: Your Essential Software Toolbox*, PCWORLD (Nov. 6, 2012, 3:30 AM), http://www.pcworld.com/article/2013470/pc-security-your-essential-software-toolbox.html?page=3.

12. Christopher S. Yoo, *Free Speech and the Myth of the Internet as an Unintermediated Experience*, 78 GEO. WASH. L. REV. 697, 707 (2010) ("End users are unable to sift through the avalanche of new and existing content that appears on the Internet by themselves."); *February 2013 Web Server Survey*, NETCRAFT (Feb. 1, 2013), http://news.netcraft.com/archives/2013/02/01/february-2013-web-server-survey.html (estimating that the Internet has over 630 million web sites).

13. JACK M. BALKIN, BETH SIMONE NOVECK & KERMIT ROOSEVELT, INFO. SOC'Y PROJECT AT YALE LAW SCHOOL, FILTERING THE INTERNET: A BEST PRACTICES MODEL 4 (1999), *available at* http://www.yale.edu/lawweb/jbalkin/articles/Filters0208.pdf; NAT'L RESEARCH COUNCIL, YOUTH, PORNOGRAPHY, AND THE INTERNET 50 (Dick Thornburgh & Herbert S. Lin eds., 2002) ("Filtering systems . . . work like information retrieval systems in reverse; that is, they are concerned not with retrieving desirable information, but rather with making sure that undesirable information is not retrieved. However, their essential operations remain the same . . . .").

14. ERICA NEWLAND ET AL., ACCOUNT DEACTIVATION AND CONTENT REMOVAL: GUIDING PRINCIPLES AND PRACTICES FOR COMPANIES AND USERS 11 (2011), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf (describing Facebook's "individual blocking" tool); Yoo, *supra* note 12, at 707; *Frequently Asked Questions*, YELP, http://www.yelp.com/faq#review_remove (last visited Jan. 20, 2014) (describing Yelp's review filter, which directs users to the "most helpful and reliable reviews among the millions" that are submitted to the site).

15. 47 U.S.C. § 230(b)(3) (2012) ("It is the policy of the United States . . . to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services . . . ."); Jack M. Balkin, *Media Access*: *A Question of Design*, 76 GEO. WASH. L. REV. 933, 943–44 (2008); John B. Morris, Jr. & Cynthia M. Wong, *Revisiting User Control: The Emergence and Success of a First Amendment Theory for the Internet Age*, 8 FIRST AMEND. L. REV. 109, 132–136 (2009); Cecilia Ziniti, *The Optimal Liability System for Online Service Providers: How* Zeran v. America Online *Got it Right and Web 2.0 Proves It*, 23 BERKELEY TECH. L.J. 583, 610–14 (2008).

16. Jennifer A. Chandler, *A Right to Reach an Audience: An Approach to Intermediary Bias on the Internet*, 35 HOFSTRA L. REV. 1095, 1097–98 (2007).

negative reviews of its service.[17] Second, intermediaries' filtering practices often lack transparency, such that filtering can occur unbeknownst to a user.[18] For instance, critics allege that when Google significantly demotes a website's search result ranking as punishment for attempting to manipulate its search algorithm, it does not adequately notify users that a website has been omitted from their search results.[19] This is misleading, critics argue, because users believe that search results are only based on relevancy.[20] Finally, even if a user does know that filtering is occurring and disapproves of it, it is difficult to switch to a different selection intermediary because, at least in some contexts, there are few alternatives given the large market shares enjoyed by dominant intermediaries such as Comcast, Verizon, Google, and Facebook.[21]

Chandler's argument arises as part of a broader set of debates over how much discretion selection intermediaries should have over what material they transmit. The most prominent example is the net neutrality debate, which revolves around whether broadband providers and other ISPs should be allowed to discriminate against particular content or applications, such as by

17. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1179 (9th Cir. 2009) (Fisher, J., concurring); Search King, Inc. v. Google Tech., Inc., No. CIV-02-1457-M, 2003 WL 21464568, at *2 (W.D. Okla. May 27, 2003) (dismissing claims that Google decreased the PageRanks assigned to other search engine websites for anticompetitive motives); Preserving the Open Internet, 76 Fed. Reg. 59,192, 59,195 (Sept. 23, 2011) (to be codified at 47 C.F.R. pts. 0 and 8) ("The record in this proceeding reveals that [a] broadband provider[] . . . may have economic incentives to block or otherwise disadvantage specific edge providers or classes of edge providers . . . to benefit its own or affiliated offerings at the expense of unaffiliated offerings."); Reply Comments of Foundem, In the Matter of Preserving the Open Internet Broadband Industry Practices, GN Docket No. 09-191 (FCC), *available at* http://netcompetition.org/Universal_Search_Submission_To_FCC.pdf; Jack M. Balkin, *The Future of Free Expression in a Digital Age*, 36 PEPP. L. REV. 427, 431–32 (2009); Chandler, *supra* note 16, at 119–20; Thomas B. Nachbar, *Paradox and Structure: Relying on Government Regulation to Preserve the Internet's Unregulated Character*, 85 MINN. L. REV. 215, 265 (2000); Frank Pasquale, *Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries*, 104 NW. U. L. REV. 105, 119–24 (2010).

18. United States v. Am. Library Ass'n, Inc., 539 U.S. 194, 224 (2003) (Stevens, J., dissenting); *Zango*, 568 F.3d at 1179 (Fisher, J., concurring) ("If users are unaware of undesired blocking, they would not know to switch to different software or even to complain to the blocked provider that they are having trouble accessing its material . . . ."); BARBARA VAN SCHEWICK, NETWORK NEUTRALITY AND QUALITY OF SERVICE: WHAT A NON-DISCRIMINATION RULE SHOULD LOOK LIKE 14 (2012), *available at* http://cyberlaw.stanford.edu/files/publication/files/20120611-NetworkNeutrality_0.pdf; James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 194 (1997); Nicholas P. Dickerson, *What Makes the Internet So Special? And Why, Where, How, and by Whom Should Its Content Be Regulated?*, 46 HOUS. L. REV. 61, 76 (2009); Jonathan I. Ezor, *Busting Blocks: Revisiting 47 U.S.C. § 230 to Address the Lack of Effective Legal Recourse for Wrongful Inclusion in Spam Filters*, 17 RICH. J.L. & TECH. 7, 31 (2010).

19. Chandler, *supra* note 16, at 1116.

20. Letter from Gary Ruskin, Exec. Dir., Commercial Alert, to Donald Clark, Sec'y of the Comm'n, Fed. Trade Comm'n, Re: Deceptive Adver. Complaint Against AltaVista Co., AOL Time Warner Inc., Direct Hit Tech., iWon Inc., LookSmart Ltd., Microsoft Corp. & Terra Lycos S.A. (July 16, 2001), *available at* http://www.commercialalert.org/news/news-releases/2001/07/commercial-alert-files-complaint-against-search-engines-for-deceptive-ads.

21. Many have argued that scarcity in the ISP market diminishes the extent to which ISPs are susceptible to competitive pressure. Preserving the Open Internet, 76 Fed. Reg. at 59,197; VAN SCHEWICK, *supra* note 18, at 37; Balkin, *supra* note 17, at 430–31; John Blevins, *The New Scarcity: A First Amendment Framework for Regulating Access to Digital Media Platforms*, 79 TENN. L. REV. 353, 380–84 (2012); Susan P. Crawford, *Network Rules*, 70 LAW & CONTEMP. PROB. 51, 61 (2007); Dickerson, *supra* note 18, at 92. Several commentators have extended this argument to dominant search engines, like Google. Oren Bracha & Frank Pasquale, *Federal Search Commission: Access, Fairness, and Accountability in the Law of Speech*, 93 CORNELL L. REV. 1149, 1183–84 (2008); Chandler, *supra* note 16, at 1164.

blocking or slowing the packets in which they are transmitted, or by increasing service rates.[22] The net neutrality debate was ignited by several high-profile incidents of ISP filtering.[23] In 2005, the Canadian telecommunications company Telus blocked access to a website supporting the Telecommunications Workers Union.[24] In 2007, an FCC investigation concluded that Comcast had slowed traffic from users of file-sharing applications such as BitTorrent.[25] The FCC responded to these incidents in 2010 by adopting formal network neutrality regulations that prohibit broadband Internet providers from "block[ing] lawful content,"[26] and from "unreasonably discriminat[ing]" against "lawful network traffic."[27] While these regulations were recently invalidated by the D.C. Circuit as inconsistent with the FCC's statutory authority,[28] the FCC is currently assessing alternative approaches to regulating ISP filtering.[29]

Charges against other selection intermediaries' filtering have followed. Google has drawn criticism for its policy of refusing to host politically controversial advertisements,[30] and for significantly demoting search rankings of websites that attempt to manipulate its search algorithm.[31] A "search neutrality" movement has arisen, which calls for regulatory measures such as "disclosure requirements, prohibitions on discriminatory search result rankings, and limits on removals from search engine indexes."[32] Content-hosting platforms including Facebook and Live Journal have come under scrutiny for content-removal and account-termination decisions.[33] For instance, in 2010, Amazon deleted WikiLeaks's website from its cloud server in response to pressure from Senator Lieberman.[34] Drawing on this incident,

22. Daniel A. Lyons, *Net Neutrality and Nondiscrimination Norms in Telecommunications*, 54 ARIZ. L. REV. 1029, 1034–38 (2012).

23. VAN SCHEWICK, *supra* note 18, at 1; Lyons, *supra* note 22, at 1040–41.

24. Pasquale, *supra* note 17, at 122.

25. *In re* Comcast, 23 FCC Rcd. 13,028, 13,030–31 (Aug. 1, 2008).

26. *In re* Preserving the Open Internet: Broadband Industry Practices, 25 FCC Rcd. 17,905, 17,942 (Dec. 21, 2010).

27. *Id.* at 17,944.

28. Verizon v. FCC, 740 F.3d 623, 659 (D.C. Cir. 2014) (vacating the FCC's Preserving the Open Internet order).

29. Emma Woollacott, *FCC Readies New Network Neutrality Plan*, FORBES (Feb. 12, 2014, 11:24 AM), http://www.forbes.com/sites/emmawoollacott/2014/02/12/fcc-readies-new-network-neutrality-plan/.

30. Dawn C. Nunziato, *The Death of the Public Forum in Cyberspace*, 20 BERKELEY TECH. L.J. 1115, 1124 (2005) (discussing Google's policy regarding advertisements on "sensitive issues").

31. James Grimmelmann, *Some Skepticism About Search Neutrality*, *in* THE NEXT DIGITAL DECADE: ESSAYS ON THE FUTURE OF THE INTERNET 435–36 (Berin Szoka & Adam Marcus eds., 2010).

32. Blevins, *supra* note 21, at 363–64; Eric Goldman, *Search Engine Bias and the Demise of Search Engine Utopianism*, 8 YALE J.L. & TECH. 188, 194–95 (2006).

33. NEWLAND ET AL., *supra* note 14; Rebecca Tushnet, *Power Without Responsibility*: *Intermediaries and the First Amendment*, 76 GEO. WASH. L. REV. 986, 996–1001 (2008); Jake Levine, *It's Time for a Social Network Neutrality, Thinking, Reading, Writing About the Internet*, JAKE LEVINE (July 18, 2011), http://www.jakelevine.me/blog/2011/07/its-time-for-a-social-network-neutrality; Helen A.S. Popkin, *Facebook Calls Roger Ebert's Blog 'Abusive Content,'* NBC NEWS (Jan. 22, 2011, 1:46 PM), http://www.nbcnews.com/technology/technolog/facebook-calls-roger-eberts-blog-abusive-content-125626; Colleen Taylor, *Is This Censorship? Facebook Stops Users from Posting 'Irrelevant Or Inappropriate' Comments*, TECHCRUNCH (May 5, 2012), http://techcrunch.com/2012/05/05/facebooks-positive-comment-policy-irrelevant-inappropriate-censorship/.

34. Ewen MacAskill, *WikiLeaks Website Pulled by Amazon After US Political Pressure*, GUARDIAN

Yochai Benkler has argued that persons whose accounts are arbitrarily or improperly terminated should be able to sue the platform provider for breach of contract and/or tortious interference with prospective economic advantage.[35] Similar calls for economic tort remedies have been made in the context of filtering software.[36] Scholars have suggested that a provider whose filtering software blocks the display of advertisements on a website should be liable for tortious interference with contractual relations.[37] Claims of this sort have been the basis of several recent (and unsuccessful) lawsuits against providers of allegedly over-inclusive spam and spyware filters.[38]

Limits on intermediary discretion are necessary, critics argue, because filtering can limit the diversity of material available on the Internet and impose a severe burden on speakers whose material is filtered.[39] Under this account, the dominant audience-share enjoyed by popular intermediaries like Google, Facebook, and Twitter makes them "gatekeepers,"[40] or "core facilities"[41] for Internet expression. Being filtered by just one such intermediary can prevent a speaker from reaching a large portion of his or her intended audience.[42] Defenders of intermediary discretion respond by emphasizing the valuable role selection intermediaries play in helping Internet users avoid material they find offensive or irrelevant.[43] A user's interest in not receiving material, the argument goes, trumps the speaker's interest in disseminating in. This is why Chandler's argument about user control is significant. If intermediaries' filtering is not consistent with users' preferences, then the general justification for intermediary discretion is inapposite. In this respect, the issue of whether

(Dec. 1, 2010), http:// www.guardian.co.uk/media/2010/dec/01/wikileaks-website-cables-servers-amazon.

35. Yochai Benkler, *A Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate*, 46 HARV. C.R.-C.L. L. REV. 311, 367–70 (2011).

36. Ezor, *supra* note 18, at 36.

37. Andrew Saluke, *Ad-Blocking Software as Third-Party Tortious Interference with Advertising Contracts*, 7 FLA. ST. U. BUS. REV. 87, 119 (2008); Jordan L. Walbesser, *Blocking Advertisement Blocking; The War over Internet Advertising and the Effect on Intellectual Property*, 23 INTELL. PROP. & TECH. L.J., no. 1, 2011 at 19, 21. According to this argument, the "contractual relation" is the contract under which the advertiser pays the website operator to display its advertisements. By preventing the advertisements from displaying on a user's computer when he or she visits the website, the filtering software prevents the website operator from performing under the contract, and thus "interferes" with the contract between the advertiser and the website operator.

38. *E.g.*, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009); Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924 JF, 2011 WL 3740813 (N.D. Cal. Aug. 23, 2011); Holomaxx Techs. Corp. v. Yahoo!, Inc., No. 10-cv-04926 JF, 2011 WL 3740827 (N.D. Cal. Aug. 23, 2011); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2011 WL 900096 (D.N.J. Mar. 15, 2011); E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008).

39. Marvin Ammori, *First Amendment Architecture*, 2012 WIS. L. REV. 1, 45–46 ("[T]he First Amendment 'rests on the assumption that the widest possible dissemination of information from diverse and antagonistic sources is essential to the welfare of the public.'" (quoting Associated Press v. United States, 326 U.S. 1, 20 (1945))); John G. Palfrey, Jr. & Robert Rogoyski, *The Move to the Middle: The Enduring Threat of "Harmful Speech" to the End-to-End Principle*, 21 WASH. U. J.L. & POL'Y 31, 59–64 (2006); Jonathan Weinberg, *Rating the Net*, 19 HASTINGS COMM. & ENT. L.J. 453, 477 (1997).

40. Blevins, *supra* note 21, at 355.

41. Benkler, *supra* note 35, at 369–70, 390, 400–01.

42. NEWLAND ET AL., *supra* note 14, at 24; Chandler, *supra* note 16, at 1106–09; Dickerson, *supra* note 18, at 90–91; Ezor, *supra* note 18, at 32–37.

43. Goldman, *supra* note 32, at 195–98; Yoo, *supra* note 12, at 703–17 (describing not only the benefits of the practice, but also the role of intermediation in two-sided markets).

intermediary discretion is good policy turns largely on whether intermediaries' filtering practices are conducive to user control.

But there is also an important legal issue that turns on user control, which commentators have generally overlooked: whether the § 230(c)(2) safe harbor protects intermediaries from legal measures that would limit their discretion over filtering. Construed broadly, § 230(c)(2) would protect providers from measures directed against anticompetitive and/or deceptive filtering, such as the FCC's network neutrality regulations, proposed search neutrality regulations, and economic torts. Given that one of Congress's purposes in enacting § 230(c)(2) was to "encourage the development of technologies which maximize user control,"[44] the safe harbor should not cover filtering that is inconsistent with users' preferences. However, justifying this limitation poses a challenge, given the broad language of § 230(c)(2).

Section 230(c)(2) provides:

> (c) Protection for "Good Samaritan" blocking and screening of offensive material
>
> . . .
>
> (2) Civil liability
>
> No provider or user of an interactive computer service shall be held liable on account of—
>
> (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
>
> (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).[45]

The safe harbor protects Internet and software providers from being held liable for "restrict[ing] access" to material,[46] a phrase that has been found by courts to encompass the use of spam filters,[47] search engines,[48] and software designed to block spyware.[49] "[R]estrict access" may also encompass filtering by other selection intermediaries, such as ISP blocking (e.g., the Telus and Comcast incidents),[50] and account terminations by providers of user-generated content platforms (e.g., social networking sites), as Eric Goldman argued in a recent

---

44. 47 U.S.C. § 230(b)(3) (2012).

45. *Id.* § 230(c)(2). According to the United States Code Annotated, the use of "(1)" in § 230(c)(2)(B) is a typographical error and should be "(A)," as in "§ 230(c)(2)(A)." 47 U.S.C.A. § 230 (West 2014).

46. *Id.*

47. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2011 WL 900096 at *1, *4 (D.N.J. Mar. 15, 2011); Holomaxx Techs., Inc. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1098 (N.D. Cal. Mar. 11, 2011); E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008).

48. Langdon v. Google, 474 F. Supp. 2d 622, 634 (D. Del. 2007).

49. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1177–78 (9th Cir. 2009).

50. Several commentators have recognized that § 230(c)(2) is potentially applicable to ISP blocking. Dickerson, *supra* note 18, at 82–83; David Sohn, Comment to *Ask CDT: Internet Neutrality*, CENTER FOR DEMOCRACY & TECH. (Apr. 25, 2011, 3:11 PM), https://www.cdt.org/ask-internet-neutrality.

article.[51]

While the statute imposes an additional hurdle by requiring that the filtered material be "obscene, lewd, [etc.]," this requirement is not as strict as it appears at first glance.[52] It is sufficient for the provider to establish that the filtered material falls under the broad phrase "otherwise objectionable," which some courts have interpreted as being broader than the preceding terms.[53] Furthermore, the phrase "provider or user considers" indicates that whether material is "objectionable" may be assessed from the provider's subjective standpoint.[54] While the phrase "good faith" seems to preclude the provider from relying on a self-serving allegation that it found the material it filtered to be objectionable, good faith is only required under subsection (c)(2)(A), not (c)(2)(B).[55] As Judge Fisher explained in his concurrence to the recent Ninth Circuit case *Zango v. Kaspersky*, the lack of a good faith requirement in subsection (c)(2)(B) allows for "otherwise objectionable" to be construed as an "unbounded catchall phrase" that can apply to a provider who "block[s] content for anticompetitive purposes or merely at its malicious whim," and "without the user's knowledge or consent."[56] Moreover, even if a provider cannot satisfy (c)(2)(B), and thus must satisfy subsection (c)(2)(A), some courts have been heavily deferential to providers' allegations of good faith, out of reluctance to subject providers to a fact-sensitive inquiry and the resulting litigation costs that the § 230 safe harbor is designed to avoid.[57]

Courts should reject these broad interpretations of § 230. Allowing providers to claim the safe harbor with respect to filtering that does not comport with users' preferences is inconsistent with Congress's policy of "encourag[ing] the development of technologies which maximize user

51. Eric Goldman, *Online User Account Termination and 47 U.S.C. § 230(c)(2)*, 2 SANTA CLARA L. REV. 659 (2011).

52. 47 U.S.C. § 230(c)(2)(A) (2012).

53. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2010 WL 1799456, at *6 (D.N.J. May 4, 2010) ("Congress included the phrase 'or otherwise objectionable' in its list of restrictable materials, and nothing about the context before or after that phrase limits it to just patently offensive items."); *Langdon*, 474 F. Supp. 2d at 631–32 (finding that even if politically controversial advertisements did not qualify as "obscene" or "harassing," they fell within the meaning of "objectionable").

54. Several courts have read § 230(c)(2) as only requiring that the provider subjectively deem material to be "otherwise objectionable." Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. Mar. 11, 2011); *Smith*, 2010 WL 1799456, at *6; E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 608 (N.D. Ill. 2008).

55. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1177 (9th Cir. 2009) (noting that subsection (c)(2)(B) "has no good faith language" and declining to decide whether it "should be construed implicitly to have a good faith component").

56. *Id.* at 1178 (Fisher, J., concurring).

57. Holomaxx Techs. v. Yahoo!, Inc., No. 10-cv-04926 JF, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 22, 2011) ("[A]ll doubts 'must be resolved in favor of immunity.' . . . To permit Holomaxx to proceed solely on the basis of a conclusory allegation that Yahoo! acted in bad faith essentially would rewrite the CDA." (quoting Goddard v. Google, No. C 08-2738 JF, 2008 WL 5245490, at *2 (N.D. Cal. 2008))); *Holomaxx*, 783 F. Supp. 2d at 1104 (reading *E360Insight* for the proposition that "virtually total deference to provider's subjective determination is appropriate"); *E360Insight*, 546 F. Supp. 2d at 609 ("To force a provider . . . to litigate the question of whether what it blocked was or was not spam would render § 230(c)(2) nearly meaningless."); *see also* Goldman, *supra* note 51, at 671 ("Section 230(c)(2) provides substantial legal certainty to online providers who police their premises and ensure the community's stability when intervention is necessary.").

control."[58] The "good faith" and "obscene, lewd, [etc.]" requirements indicate that Congress intended there to be limits on the safe harbor.[59] Moreover, the fact that the "good faith" requirement only applies in cases where the provider has restricted access, as opposed to giving users the technical means to do so, indicates that Congress intended the contrast between subsections (c)(2)(A) and (c)(2)(B) to be a trade-off between power and responsibility. In other words, when the provider cedes power to users (i.e., by employing filtering technology that maximizes user control), the filtering should be governed under subsection (c)(2)(B), in which event the absence of a "good faith" requirement means the provider should commensurately bear less responsibility to ensure that the filtered material is objectionable. However, when the provider's filtering technology does not exhibit user control, subsection (c)(2)(A) requires that the provider has acted with a good faith belief that its filtering accommodated users' preferences.

The balance of this Article proceeds as follows: Part I discusses the legislative history of § 230(c)(2) and subsequent case law. Part II argues that Congress's policy in favor of user control technologies should inform courts' application of § 230(c)(2). Part III explains how courts should construe subsection (c)(2)(B) so as to limit it to technologies that exhibit user control. Part IV discusses how courts should resolve the ambiguities in the phrases "good faith" and "otherwise objectionable."

II. BACKGROUND

Section 230(c)(2) is an immunity law. It regulates conduct not by imposing liability, but by preempting it with respect to certain proscribed activities: "restrict[ing] access to . . . obscene, lewd, [etc.]" material by any provider of an interactive computer service (ICS),[60] which in practice means any provider of Internet-based services, from an ISP to an e-mail spam filter.[61] Section 230(c)(2) encourages providers to filter by giving them assurance that they cannot be held liable for doing so.[62] If a cause of action is predicated on some act of filtering by the defendant, such as where an online advertiser brings suit for tortious interference against the provider of a spyware filter, it falls within the scope of § 230(c)(2).[63] Section 230 contains a separate immunity provision—subsection (c)(1)—which applies to claims arising out of

58. 47 U.S.C. § 230(b)(3) (2012).

59. *Id.* § 230(c)(2)(A).

60. *Id.* § 230(c)(2).

61. Courts have found that a diverse array of services qualify as an ICS. *See, e.g.*, Doe v. MySpace, Inc., 528 F.3d 413 (5th Cir. 2008) (social networking site); Chicago Lawyers Committee v. Craigslist, 519 F.3d 666 (7th Cir. 2008) (classified-advertisement listing services); Universal Communication System, Inc. v. Lycos, Inc., 478 F.3d 413 (1st Cir. 2007) (online discussion forum); Carafano v. Metrosplash.com, 339 F.3d 1119 (9th Cir. 2003) (dating sites); Batzel v. Smith, 333 F.3d 1018 (9th Cir. 2003) (e-mail listserv operators); *E360Insight*, 546 F. Supp. 2d 605 (web-based consumer complaint services); Murawski v. Pataki, 514 F. Supp. 2d 577 (S.D.N.Y. 2007) (search engines).

62. 47 U.S.C. § 230(c)(2)(B).

63. Zango, Inc. v. Kaspersky, Lab Inc., 568 F.3d 1169, 1173 (9th Cir. 2009); *see also Batzel*, 333 F.3d at 1030 n.14 ("[Section 230(c)(2)] insulates service providers from claims premised on the taking down of a customer's posting such as breach of contract or unfair business practices . . . .").

the publication and dissemination of material created by third parties,[64] such as defamation.[65] Subsection (c)(1) has been the subject of far more litigation than subsection (c)(2),[66] which reflects the fact that causes of action that hinge on filtering generally fail on the merits and are thus not commonly asserted.[67] But the growing criticism of dominant intermediaries' filtering practices suggests that such claims will become increasingly viable. Indeed, the number of defendants asserting § 230(c)(2) defenses has increased significantly in the past several years.[68]

A. Legislative History

Section 230 originated as the Online Family Empowerment Act (OFEA), a bill proposed by Representatives Cox and Wyden.[69] Cox and Wyden proposed OFEA as an alternative to the proposed Exon-Coats amendment to 47 U.S.C. § 223, which made it a crime for any person to "make . . . and initiate the transmission of . . . any . . . communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age."[70] Whereas OFEA targeted pornography at the receiving end by encouraging filtering, the Exon-Coats amendment targeted pornography at the source by prohibiting its dissemination.[71]

The contrast between OFEA and the Exon-Coats amendment reflected the disagreement amongst Congress on how to make Internet pornography inaccessible to children. A divisive issue was whether parents could effectively control their children's online activity.[72] In arguing "no," proponents of the Exon-Coats amendment claimed that filters were under-inclusive in that they did not detect and block all pornography, and parents were not technologically sophisticated enough to implement them.[73] Thus, it was argued, it was necessary for the government to prohibit Internet

64. 47 U.S.C. § 230(c)(1) ("No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.").

65. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (holding that America Online is not liable for not taking down inflammatory content).

66. Goldman, *supra* note 51, at 660.

67. In *E360Insight*, the court expressed doubt that a provider of a spam filter could be held liable for tortious interference with prospective economic advantage, stating:

> I have found no cases in which refusal to allow a plaintiff to run an advertisement in a medium with wide circulation (and thus reducing sales) of plaintiff's products or those from whom he is selling constitutes such tortious interference. Usually the prospective economic advantage is far more concrete than selling to public which consists of people on a very, very long opt-in list. It is illegal to interfere with a fair number of prospects, but usually they are a class of easily identified individuals and usually the interference is that of the defendant interacting directly with the prospective buyers.

E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 n.3 (N.D. Ill. 2008).

68. *See generally* Melissa A. Troiano, *The New Journalism? Why Traditional Defamation Laws Should Apply to Internet Blogs*, 55 AM. U. L. REV. 1447, 1453–63 (2006) (speaking to the expansive use of the § 230(c)(2) defense).

69. 141 CONG. REC. 22,044 (1995).

70. *Id.* at 16,068.

71. *Id.*

72. *Id.* at 16,009 (statement of Sen. Exon).

73. *Id.*

pornography at the source.[74] Opponents of the Exon-Coats amendment countered that filtering software was quickly becoming more sophisticated and accessible to parents.[75] This made the Exon-Coats amendment not only unnecessary, they argued, but unconstitutional as well given the Supreme Court's approach of applying heightened First Amendment protection to technologies exhibiting user control.[76]

Recognizing the significance that filtering software played in the larger debate, Representatives Cox and Wyden proposed OFEA.[77] To Cox and Wyden, the alleged inefficacies of filtering software stemmed from over-regulation, not limited technology.[78] To illustrate this point, Representative Cox referred to *Stratton Oakmont, Inc. v. Prodigy Services Co.*, in which a New York trial court held Prodigy (an online service provider) liable for a defamatory comment that had been posted to its online forum by an anonymous user.[79] The court found that since Prodigy had made efforts to filter offensive content off of its network, it assumed responsibility for any offensive content that it failed to filter, even if it lacked actual or constructive knowledge of such content.[80] According to Representative Cox, the *Stratton Oakmont* court's approach of premising liability on efforts to filter would deter software companies from providing filtering software.[81] OFEA was designed to eliminate this deterrent effect by specifically overruling *Stratton Oakmont* and by immunizing providers like Prodigy from liability in future cases.[82]

Congress supported OFEA and voted to enact it as § 230 of the CDA, which was a part of the Telecommunications Act of 1996.[83] The Exon-Coats amendment was also enacted as part of the CDA and codified at 47 U.S.C. § 223, but was invalidated by the Supreme Court a year later in *Reno v. ACLU*.[84] While the *Reno* court did not discuss § 230, it did state that filtering software was a less restrictive means of limiting children's access to pornography than the Exon-Coats amendment.[85]

---

74. *Id.*

75. *Id.* at 16,013 (statement of Sen. Feingold).

76. *Id.*

77. *Id.* at 22,044.

78. *Id.* at 22,045.

79. *Id.*; *see also* Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute,* Telecommunications Act of 1996, Pub. L. No. 104-104, 110 Stat. 137, *as recognized in* Shiamili v. Real Estate Grp. of N.Y., 952 N.E.2d 1011 (N.Y. 2011).

80. *See Stratton Oakmont*, 1995 WL 323710, at *5 ("PRODIGY's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than CompuServe and other computer networks that make no such choice.").

81. 141 CONG. REC. 22,045 (1995) (statement of Rep. Cox).

82. H.R. CONF. REP. NO. 104-879, at 194 (1996) ("One of the specific purposes of this section is to overrule *Stratton-Oakmont v. Prodigy* and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that [*Stratton Oakmont*] create[s] serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.").

83. Telecommunications Act of 1996, Pub. L. No. 104-104, § 509, 110 Stat. 56, 137–39.

84. Reno v. ACLU, 521 U.S. 844, 877–79 (1997).

85. *Id.*

B. Text

The operative provision of § 230 is subsection (c), which, as discussed above, provides immunity for disseminating material created by third parties and for restricting access to material the user or provider considers to be "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[86] As the language "excessively violent, harassing, or otherwise objectionable" indicates, immunity under subsection (c)(2) is not limited to the filtering of pornography.

In addition to subsection (c), § 230 contains several other provisions. Subsection (a) includes a list of Congressional findings relevant to § 230.[87] Subsection (b) includes a list of policies underlying § 230.[88] Under § 230(d), a provider that "enter[s] an agreement with a customer for the provision of interactive computer service" shall "notify such customer that parental control protections . . . are commercially available."[89] Section 230(e) provides that immunity does not apply to federal criminal laws, intellectual property laws, electronic privacy laws, and state laws that are consistent with § 230.[90] Finally, § 230(f) defines the terms "Internet," "interactive computer service," "information content provider," and "access software provider."[91]

C. Application

Most of the § 230 case law has focused on subsection (c)(1), which protects a provider from liability for disseminating material created by a third party.[92] By contrast, subsection (c)(2), the focus of this Article, governs cases where the plaintiff's complaint is that a defendant has prevented the dissemination of material.[93] For example, in *E360Insight*, Comcast was sued by a company whose marketing e-mails were blocked by the spam filter Comcast provided to users of its e-mail service.[94] The court held that Comcast was entitled to immunity because E360Insight's claims were premised on the fact that the spam filter had restricted Comcast subscribers' access to E360Insight's e-mails within the meaning of subsection (c)(2).[95] As *E360Insight* illustrates, the "restrict access" language applies where the provider takes some action that prevents the plaintiff's intended audience from accessing material that the plaintiff is seeking to disseminate.[96] In addition to employing filtering technologies, "restricting access" could also include other

86. 47 U.S.C. § 230(c) (2012).
87. *Id.* § 230(a).
88. *Id.* § 230(b).
89. *Id.* § 230(d).
90. *Id.* § 230(c).
91. *Id.* § 230(f).
92. *See, e.g.*, Zeran v. Am. Online, Inc., 129 F.3d 327, 332 (4th Cir. 1997) (discussing how to define "provider").
93. *E.g.*, Stratton Oakmont, Inc. v. Prodigy Servs. Co., 1995 WL 323710, at *3 (N.Y. Sup. Ct. May 24, 1995).
94. E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 606 (N.D. Ill. 2008).
95. *Id.* at 609.
96. *Id.*

measures a provider might take to make it more difficult for a speaker to reach his or her intended audience, such as charging a speaker fees for his or her use of an (ICS), or terminating his or her account.[97]

In addition to restricting access, § 230(c)(2) requires that a defendant qualify as an ICS.[98] Subsection 230(f)(2) defines an ICS as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[99] Courts have construed the term ICS broadly.[100] In the context of § 230(c)(2) it has been held applicable to e-mail spam filters,[101] spyware filtering software,[102] eBay,[103] and Google's search engine.[104]

Once a defendant qualifies as a provider of an ICS, it must satisfy either subsection (c)(2)(A) or (c)(2)(B) for each claim that it defends on immunity grounds.[105] Subsection (c)(2)(A) preempts any cause of action premised on "[a]ction voluntarily taken in good faith to restrict access to or availability of material that the provider . . . considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable . . . ."[106] Subsection (c)(2)(B), on the other hand, preempts "any action taken to enable or make available to information content providers or others the technical means to restrict access to material" that the provider considers to be obscene, lewd, etc.[107] A claim is preempted so long as the facts on which it is premised fall within one of the two prongs.[108] Claims preempted under § 230(c)(2) have included tortious interference,[109] breach of contract,[110] trade libel,[111] and various alleged violations of state antitrust and consumer protection statutes.[112]

---

97. *Id.* at 607.

98. 47 U.S.C. § 230(c)(2) (2012).

99. *Id.* § 230(f)(2).

100. See *supra* note 61.

101. Holomaxx Techs. Corp. v. Yahoo!, Inc., No. 10-cv-04926 JF, 2011 WL 3740827, at *4 (N.D. Cal. Aug. 23, 2011); Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924 JF, 2011 WL 3740813, at *7 (N.D. Cal. Aug. 23, 2011); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2011 WL 900096, at *18 (D.N.J. May 4, 2010); *E360Insight*, 546 F. Supp. 2d at 609.

102. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1173 (9th Cir. 2009).

103. National Numismatic Certification, LLC. v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *23–25 (M.D. Fla. July 8, 2008).

104. Langdon v. Google, 474 F. Supp. 2d 622, 631 (D. Del. 2007).

105. 47 U.S.C. §§ 230(c)(2)(A)–(B) (2012).

106. *Id.* § 230(c)(2)(A).

107. *Id.* § 230(c)(2)(B).

108. *See id*. § 230(c)(2) ("No provider or user of an interactive computer service shall be held liable on account of (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; *or* (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1)." (emphasis added)).

109. E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008).

110. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2010 WL 1799456, at *4–6 (D.N.J. May 4, 2010).

111. National Numismatic Certification, LLC v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *23–25 (M.D. Fla. July 8, 2008).

112. *Smith*, 2010 WL 1799456, at *2–4; *see* Google, Inc. v. MyTriggers.com, Inc., No. 09CVH10-14836, 2011 WL 3850286, at *5–7 (Ohio Com. Pl. Aug. 1, 2011) (discussing whether § 230 preempted state antitrust statute).

While § 230(c)(2) case law has illustrated what it means for a provider of an ICS to restrict access to material, several ambiguities remain. For instance, courts have reached inconsistent interpretations of the "good faith" requirement in subsection (c)(2)(A). In *Holomaxx Technologies v. Yahoo!*, the court rejected the plaintiff's allegations of bad faith because it found that § 230 did not specifically impose any duties on providers, such as responding to or complying with requests to unblock material.[113] But in *Smith v. Trusted Universal Standards in Electronic Communication*, the court assessed the defendant ISP's good faith by reviewing a wide-ranging array of circumstantial evidence, such as the plaintiff's allegation that the ISP failed to explain why it blocked his outgoing e-mails and told him "he would not have to worry about any e-mail blocking if [he] subscribed to a higher level of service."[114] Courts have also disagreed over how specific and well-supported a plaintiff's allegations of bad faith must be in order to survive a motion to dismiss on the pleadings.[115] As Eric Goldman has argued, allowing plaintiffs to conduct discovery in search of a wide range of circumstantial evidence of bad faith "[i]mposes additional advocacy and discovery costs on the defendant"[116] and undermines Congress' policy of "remov[ing] disincentives for the development and utilization of blocking and filtering technologies. . . ."[117] But Goldman's proposed prescription—allowing a provider's justification for filtering to satisfy the "good faith" requirement "even if that justification is ultimately pretextual"[118]—goes too far. The fact that Congress included the "good faith" requirement in subsection (c)(2)(A) indicates that it intended for that requirement to be more than a mere formality.

Courts have also disagreed over how to interpret the phrase "otherwise objectionable."[119] In *E360Insight*, the court noted that § 230(c)(2) "only requires that the provider subjectively deems the blocked material objectionable,"[120] and concluded that "there is no question that Comcast, through the use of its numerous programs, software, and technologies,

113. Holomaxx Techs. v. Yahoo!, Inc., 783 F. Supp. 2d 1097, 1105 (N.D. Cal. Mar. 11, 2011).

114. *Smith*, 2010 WL 1799456, at *7 (quoting Plaintiff's Complaint) (alterations in original).

115. *Compare* Holomaxx Techs. v. Yahoo!, Inc., No. 10-cv-04926 JF, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) (granting Yahoo!'s motion to dismiss under Fed. R. Civ. P. 12(b)(6) because denying the motion "solely on the basis of a conclusory allegation that Yahoo! acted in bad faith essentially would rewrite the CDA"), *and* E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 610 (N.D. Ill. 2008) (granting Comcast's motion for judgment on the pleadings because E360Insight's affidavit did not attest to its allegation that Comcast imposed a stricter filtering policy on E360Insight than other senders of marketing e-mails), *with* Nat'l Numismatic Certification v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *24 (M.D. Fla. July 8, 2008) ("With allegations in the Amended Complaint that eBay acted in bad faith, the Court should not grant dismissal under Federal Rule of Civil Procedure 12(b)(6)."), *and* Sabbato v. Hardy, No. 2000CA00136, 2000 WL 33594542, at *3 (Ohio Ct. App. Dec. 18, 2000) (holding that the trial court erred by granting defendant's motion to dismiss on the basis of § 230 because "the 'good faith' language presupposes some evidence of that 'good faith' which" the court found that the defendant had not adequately pled).

116. Goldman, *supra* note 51, at 666.

117. 47 U.S.C. § 230(b)(4) (2012).

118. Goldman, *supra* note 51, at 666.

119. Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. Mar. 11, 2011) ("No court has articulated specific, objective criteria to be used in assessing whether a provider's subjective determination of what is 'objectionable' is protected by § 230(c)(2).").

120. *E360Insight*, 546 F. Supp. 2d at 608 (citing Zango, Inc. v Kaspersky Lab, Inc., No. 07-0807, 2007 WL 5189857, at *4 (W.D. Wash. Aug. 28, 2007)).

considers the material sent by e360 via e-mail objectionable."[121] Furthermore, in *Langdon v. Google*, the court held that a website accusing the North Carolina Attorney General of fraud was "objectionable" and that Google was thus immune from liability for removing the website from its search results.[122]

However, several courts have read "objectionable" more narrowly. In *National Numismatic Certification v. eBay*, the court held that § 230(c)(2) did not immunize eBay from liability for removing auction listings for potentially counterfeit coins.[123] The court relied on the principle of *ejusdem generis*, which holds that "[w]hen a general term follows specific terms, courts presume that the general term is limited by the preceding terms."[124] Applying this principle, the court stated:

> One may find an array of items objectionable; for instance, a sports fan may find the auction of a rival team's jersey objectionable. However, Congress provided guidance on the term "objectionable" by providing a list of seven examples and a statement of the policy behind section 230. Accordingly, the Court concludes that "objectionable" content must, at a minimum, involve or be similar to pornography, graphic violence, obscenity, or harassment.[125]

While several courts have adopted this approach,[126] the court in *Smith v. Trusted Universal Standards in Electronic Transactions* rejected the "[p]laintiff's argument that the blocked material must be 'obscene, lewd, filthy, excessively violent, or harassing'"[127] and stated that "Congress included the phrase 'or otherwise objectionable' in its list of restrictable materials, and nothing about the context before or after that phrase limits it to just patently offensive items."[128] Moreover, the principle of *ejusdem generis* does not necessarily limit the breadth of § 230 immunity because courts have also interpreted the preceding term "harassing" broadly. In *National Numismatic Certification*, the court stated that its interpretation was consistent with the outcome in *Langdon* because the material at issue in *Langdon*—a web site accusing the North Carolina Attorney of fraud—qualified as "harassing."[129] However, if courts read "objectionable" in conjunction with "good faith," as Judge Fisher suggested in his concurrence to *Zango v. Kaspersky*,[130] then a

121. *Id.*

122. Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007).

123. Nat'l Numismatic Certification, LLC. v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *23–26 (M.D. Fla. July 8, 2008).

124. *Id.* at *25.

125. *Id.*

126. *See* Goddard v. Google, Inc., No. C 08-2738 JF (PVT), 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008) (holding that the fact that advertisements for mobile services violated Google AdWords's requirement that such services provide pricing and cancellation information did not render advertisements objectionable because the "requirements relate to business norms of fair play and transparency and are beyond the scope of § 230(c)(2)"); Google, Inc. v. MyTriggers.com, Inc., No. 09CVH10-14836, 2011 WL 3850286, at *5–7 (Ohio Com. Pl. Aug. 1, 2011) (holding that advertisements for a search engine were not objectionable).

127. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2010 WL 1799456, at *6 (D.N.J. May 4, 2010) (quoting Plaintiff's Brief).

128. *Id.*

129. *Nat'l Numismatic Certification*, 2008 WL 2704404, at *25, n.35.

130. Zango Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178, n.1 (9th Cir. 2009) (Fisher, J., concurring).

provider's self-serving allegation that it deems material objectionable should be insufficient to satisfy subsection (c)(2)(A).

If courts do read "good faith" as limiting the scope of "objectionable," then defendants may instead rely on subsection (c)(2)(B), which does not require good faith.[131] Subsection (c)(2)(B) presents an opportunity for any provider who cannot satisfy the "good faith" requirement in subsection (c)(2)(A) to nonetheless obtain immunity.[132] This would render the "good faith" requirement obsolete, which Congress presumably did not intend.

In *Zango v. Kaspersky*, the Ninth Circuit held that subsection (c)(2)(B) immunized a software developer, Kasperky Lab, from claims arising out of the use of Kaspersky Internet Security (KIS),[133] a malware-blocking program that Kaspersky developed and distributed.[134] Once installed on a user's computer, KIS would block any material included in a database that was maintained and updated by Kaspersky.[135] KIS blocked software distributed by Zango, which led Zango to sue Kaspersky for injunctive relief and damages for claims including tortious interference and trade libel.[136] In an attempt to defeat Kaspersky's subsection (c)(2)(B) defense, Zango alleged that KIS did not enable users to override the blocking of its software[137] and argued on this basis that "Kaspersky, rather than the customer, determines that Zango is malware such that it overrides the customer's desire to use Zango."[138] The Court responded:

> Users choose to purchase, install, and utilize the Kaspersky software. Regardless of whether Zango is correct in its allegation that Kaspersky does not provide users of Kaspersky products a choice to override the security software and download and use Zango, there is no question that Kaspersky has "made available" for its users the technical means to restrict access to items that Kaspersky has defined as malware.[139]

The Court went on to find that Zango had "waived any argument on appeal that Kaspersky does not consider Zango's software to be 'otherwise objectionable'"[140] and concluded that Kasperky was entitled to immunity under subsection (c)(2)(B).[141]

In his concurring opinion, Judge Fisher argued that the majority's interpretation of subsection (c)(2)(B) appeared to give providers "free license

131. 47 U.S.C. § 230(c)(2)(B) (2012).
132. *Id.*
133. *Zango*, 568 F.3d at 1176–78 (majority opinion).
134. *Id.* at 1170–71 ("Malware works by, for example, compromising a user's privacy, damaging computer files, stealing identities, or spontaneously opening Internet links to unwanted websites, including pornography sites.").
135. *Id.* at 1171.
136. *Id.* at 1172.
137. *Id.* at 1171–72.
138. *Id.* at 1176.
139. *Id.*
140. *Id.* at 1176–77.
141. *Id.* at 1175.

to *unilaterally* block the dissemination of material,"[142] which could prove to be problematic in future cases. While KIS provided a warning to users when it was blocking content, Judge Fisher stated:

> Other blocking software might be less accommodating to the user's preferences, either not providing an override option or making it difficult to use. Consider, for example, a web browser configured by its provider to filter third-party search engine results so they would never yield websites critical of the browser company or favorable to its competitors. Such covert, anti-competitive blocking arguably fits into the statutory category of immune actions—those taken by an access software provider to provide the technical means to block content the *provider* deems objectionable.[143]

Judge Fisher further noted that the provider's lack of good faith in this example would not preclude it from satisfying subsection (c)(2)(B) because subsection (c)(2)(B), unlike subsection (c)(2)(A), does not explicitly require good faith.[144]

Indeed, if unilateral blocking by the provider can satisfy subsection (c)(2)(B), then it is difficult to see why any of the services that courts have analyzed under subsection (c)(2)(A)—Google's search engine,[145] eBay's auction listings,[146] and various e-mail spam filters[147]—could not have also satisfied subsection (c)(2)(B). One might argue that such services do not fall within the meaning of "access software provider,"[148] which the *Zango* court found applicable to KIS.[149] But subsection (c)(2)(B), by its terms, applies to all ICSs, and being an access software provider is not necessary for qualifying as an ICS.[150] Moreover, all of the aforementioned services arguably do qualify

142. *Id.* at 1178 (Fisher, J., concurring).

143. *Id.* at 1179.

144. *Id.*

145. *See* Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007) ("Section 230 provides Google, Yahoo, and Microsoft immunity for their editorial decisions regarding screening and deletion from their network."). *But see* Google v. MyTriggers.com, Inc., No. 09CVH10-14836, 2011 WL 3850286, at *5–7 (Ohio Com. Pl. Aug. 1, 2011) (finding that MyTriggers's ads "do not fall within the same class of objectionable content that is listed in § 230(c)(2)" as in *Langdon*).

146. *See* Nat'l Numismatic Certification, LLC. v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *25 (M.D. Fla. July 8, 2008) (finding, in part, that § 230(c)(2) does not "encompass an auction of potentially-counterfeit coins when the word [objectionable] is preceded by seven other words that describe pornography, graphic violence, obscenity, and harassment").

147. *See* Holomaxx Techs. v. Microsoft Corp., Case No. 10-cv-04924 JF, 2011 WL 3740813, at *3 (N.D. Cal. Aug. 23, 2011) ("While Microsoft stopped blocking Holomaxx's emails in April 2010, that fact alone is insufficient to support a reasonable inference that Microsoft acted in bad faith when it decided to resume blocking Holomaxx's emails in June 2010."); Holomaxx Techs. v. Yahoo!, Inc., Case No. 10-cv-04926 JF, 2011 WL 3740827, at *2 (N.D. Cal. Aug. 23, 2011) ("While Yahoo! delivered at least some emails prior to June 2010, that fact alone is not sufficient to support a reasonable inference that Yahoo! acted in bad faith when it decided to block Holomaxx's emails."); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2011 WL 900096, at *8 (D.N.J. Mar. 15, 2011) (finding that Cisco's and Microsoft's activity of restricting access to unwanted spam email falls "within the realm of conduct protected by the CDA"); E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008) ("To force a provider like Comcast to litigate the question of whether what it blocked was or was not spam would render § 230(c)(2) nearly meaningless.").

148. 47 U.S.C. § 230(f)(4) (2012).

149. *Zango*, 568 F.3d at 1176.

150. 47 U.S.C. § 230(f)(2) ("The term 'interactive computer service' means any information service, system, *or access software provider* . . . ." (emphasis added)).

as access software providers given that they are "enabling tools that . . . pick, choose, analyze, or digest content."[151] Thus, as interpreted by courts thus far, subsection (c)(2)(B) presents an opportunity for any provider who cannot satisfy subsection (c)(2)(A)'s "good faith" requirement[152] to nonetheless obtain immunity.

III. THE NEED FOR LIMITS ON § 230(C)(2) IMMUNITY

In determining the proper scope of § 230 immunity, courts must draw a difficult balance. On the one hand, legal limits on intermediary discretion can serve important policy ends, such as promoting the diversity of material on the Internet and preventing dominant intermediaries like Comcast, Verizon, and Google from behaving anticompetitively.[153] On the other hand, the potential for liability burdens all Internet intermediaries, even those who filter consistently with users' preferences. Faced with the prospect of having to defend against unmeritorious claims, with resulting litigation costs, intermediaries may hesitate to provide new services. This concern is reflected in the text of § 230(b)(4), which provides that one of the policies underlying § 230 was "to remove disincentives for the development and utilization of blocking and filtering technologies . . . ."[154]

But in expressing its support for intermediary discretion, Congress added an important qualification: an additional purpose of § 230 was "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services."[155] Read in conjunction, the "user control" and "remove disincentives" policies indicate that Congress did not intend for § 230 to represent a wholesale preference of intermediary interests over speaker interests. Rather, Congress only intended to subordinate speaker interests as against intermediaries whose filtering allows users to control what information they receive.

Indeed, Congress's focus on user control technologies is evident in the text of § 230(c)(2). As discussed above, "good faith" is only required under subsection (c)(2)(A), which preempts claims alleging that the provider has unlawfully restricted access to material.[156] Cases where the provider restricts access do not exemplify what Congress meant by "user control," as indicated by the fact that § 230 distinguishes providers from users.[157] In contrast, subsection (c)(2)(B) applies where a provider enables "others"—which presumably includes users[158]—to restrict access, a manner of filtering that

151. *Id.* § 230(f)(4).
152. *Id.* § 230(c)(2)(A).
153. *See supra* p. 106 (discussing Congressional goals of the CDA).
154. 47 U.S.C. § 230(b)(4).
155. *Id.* § 230(b)(3).
156. *Id.* § 230(c)(2)(A). While subsection (c)(2)(A) applies where the "provider or user" has restricted access, the "or user" language only applies where the defendant is a user. To this author's knowledge, all § 230(c)(2) cases to date have characterized the defendant as a provider.
157. *Id.* §§ 230(c)(1)–(2) (using the phrase "provider or user").
158. The *Zango* court's analysis repeatedly used the term "user" to refer to Kaspersky's customers (i.e.

exemplifies user control. Thus, the particular way in which Congress carried out its objective of "encourag[ing] the development of technologies which maximize user control" was to allow providers who utilize such technologies to obtain immunity without having to litigate the "good faith" requirement.[159] To effectuate Congress' objective, courts should limit subsection (c)(2)(B) to technologies that exhibit user control. Furthermore, if a technology does exhibit sufficient user control to satisfy subsection (c)(2)(B), the absence of a "good faith" requirement in subsection (c)(2)(B) means that the court should be more deferential to the provider's allegation that it considered the filtered material to be objectionable than under subsection (c)(2)(A).

IV. LIMITING THE SCOPE OF SUBSECTION (C)(2)(B)

To satisfy subsection (c)(2)(B), a provider should have to establish that its ICS exhibits user control, such that the filtering at issue has been performed by a user rather than the provider. This inquiry is roughly analogous to the Ninth Circuit's *Roommates* analysis,[160] which holds that while subsection (c)(1) does protect a provider who has disseminated material created by a user, it does not protect a provider who has materially contributed to the alleged illegality of the material.[161] Under the *Roommates* analysis, the fact that the "the user pushes the last button or takes the last act before publication" does not negate a finding of material contribution by the provider.[162] As Judge Kozinski stated, "[t]he projectionist in the theater may push the last button before a film is displayed on the screen, but surely this doesn't make him the sole producer of the movie."[163] While *Roommates* is not directly applicable to subsection (c)(2)(B), it does suggest that courts should avoid formalism in determining whether an action is attributable to a user or a provider.[164]

In fleshing out the concept of "user control," it is helpful to consider the body of Supreme Court case law that influenced Congress to adopt the "user control" policy. In *FCC v. Pacifica Foundation*,[165] the Court upheld

---

the "others" to whom KIS has been "made available"). *See, e.g.*, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1176 (9th Cir. 2009) ("[T]here is no question that Kaspersky has 'made available' for its *users* the technical means to restrict access to items that Kaspersky has defined as malware.") (emphasis added)*; see also* Brief for Center for Democracy and Technology et al. as Amici Curiae Supporting Appellee at 24, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1179 (9th Cir. 2009) (No. 07-35800) [hereinafter CDT *Zango* Brief] ("Section 230(c)(2)(B) only protects entities that provide the tools and services to enable *others* to block access to content—in other words, to empower users to control access to Internet content.").

159. 47 U.S.C. § 230(b)(3).

160. Fair Hous. Council v. Roommates.com, 521 F.3d 1157, 1161–65 (9th Cir. 2008) (en banc) (holding that a matching service for apartment-seekers did not satisfy subsection (c)(1) for user profiles indicating preferences regarding a roommate's "sex, sexual orientation and whether they will bring children to the household," because the preferences were elicited by questions that the user was required to answer in order to register for the service).

161. *Id.* at 1167−68.

162. *Id.* at 1166.

163. *Id.* at 1166−67.

164. Preserving the Open Internet, 76 Fed. Reg. 59,192, 59,206 (Sept. 23, 2011) (codified in C.F.R pt. 0, 8) ("[T]here is not a binary distinction between end-user controlled and broadband-provider controlled practices, but rather a spectrum of practices ranging from more end-user controlled to more broadband provider-controlled.").

165. FCC v. Pacifica Found., 438 U.S. 726 (1978).

restrictions prohibiting a radio station from broadcasting "indecent" speech in part because "the broadcast audience is constantly tuning in and out, [and as such] prior warnings cannot completely protect the listener or viewer from unexpected program content."[166] However, in *Sable Communications of California v. FCC*,[167] the Court invalidated a ban on "indecent" prerecorded telephone messages.[168] In distinguishing *Pacifica*, the *Sable* Court noted that "the dial-it medium requires the listener to take affirmative steps to receive the communication,"[169] and that "[p]lacing a telephone call . . . is not the same as turning on a radio and being taken by surprise by an indecent message."[170] Referring to these cases during a floor debate, Senator Feingold stated, "[t]he Supreme Court has taken into consideration . . . the ability of the user to control the material he or she might view over the medium,"[171] and argued that restrictions on Internet speech like the Exon-Coats amendment were unconstitutional because "[t]here is a greater ability on computer networks to avoid materials end users do not wish to receive than exists for either broadcast media or telephony . . . ."[172] This is precisely the position the Supreme Court subsequently took in invalidating the Exon-Coats amendment in *Reno*[173] as well as Congress's revision of the Exon-Coats amendment, COPA, in *Ashcroft*.[174]

A. Identifying Potential User Control Factors

To illustrate the factors that courts might consider in assessing user control, it is helpful to draw a contrast from the *Zango* court's analysis. The *Zango* court did not construe the "user control" policy in connection with any of the language that is unique to subsection (c)(2)(B).[175] The court's only discussion of the "user control" policy was that it militated in favor of allowing KIS to qualify as an ICS, a requirement that applies to both subsection (c)(2)(A) and (c)(2)(B).[176] Furthermore, the court did not contest Zango's argument that "Kaspersky, rather than the customer, determine[d] that Zango [was] malware such that it override[d] the customer's desire to use Zango[,]"[177] but instead stated that Kaspersky satisfied subsection (c)(2)(B) "[r]egardless of whether Zango [was] correct in its allegation that Kaspersky does not provide users of Kaspersky products a choice to override the security software . . . ."[178] Given that § 230(c)(2) distinguishes between providers and

166. *Id.* at 748.
167. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115 (1989).
168. *Id.* at 116.
169. *Id.* at 128.
170. *Id.*
171. 141 CONG. REC. 16,015 (1995) (statement of Sen. Feingold).
172. *Id.*
173. Reno v. ACLU, 521 U.S. 844, 868–70 (1997).
174. Ashcroft v. ACLU, 542 U.S. 656, 666–68 (2004).
175. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1176–77 (9th Cir. 2009).
176. *Id.* at 1174.
177. *Id.* at 1176.
178. *Id.*

users,[179] the premise that the provider was controlling KIS should have led the court to question whether KIS really exhibited user control.

However, in some respects, the *Zango* court's analysis is consistent with a user control approach to subsection (c)(2)(B). For instance, the legislative history of the CDA indicates that Congress considered software programs to be a form of filtering that was performed by users.[180] In a floor debate, Senator Feingold noted that "[t]here is currently software available *which allows parents and employers to screen out objectionable services* or newsgroups on the Internet. On-line service providers also have the ability to provide parents with a choice of what types of information their children should access."[181] Similarly, when Representatives Cox and Wyden introduced OFEA to the House, Representative Goodlatte stated:

> The Cox-Wyden amendment removes the liability of providers such as Prodigy who currently make a good faith effort to edit the smut from their systems. It also encourages the online services industry to develop new technology, such as blocking software, *to empower parents to monitor and control* the information their kids can access.[182]

As these statements demonstrate, Congress contemplated two categories of filtering: filtering by online service providers, such as Prodigy, America Online, and CompuServe,[183] and filtering by software programs, which it referred to as performed by users. The fact that § 230(c)(2) refers to two categories of filtering, one performed by providers (subsection (c)(2)(A)), and one performed by users (subsection (c)(2)(B)), suggests that Congress intended for subsection (c)(2)(B) to apply to filtering by software programs. While the *Zango* court did not refer to these statements, the fact that KIS is a software program is a factor that arguably supports the court's conclusion that Kaspersky satisfied subsection (c)(2)(B).

Furthermore, the *Zango* court's subsection (c)(2)(B) analysis described the users' involvement in the operation of KIS. The Court stated that "[u]sers choose to purchase, install, and utilize the Kaspersky software[,]"[184] and that "[i]f a Kaspersky user . . . is unhappy with the Kaspersky software's performance, he can uninstall Kaspersky and buy blocking software from another company . . . ."[185] Based on these facts, one could plausibly conclude that KIS exhibited user control.

To explain why this is the correct conclusion, it is necessary to introduce two additional user control factors: notice and adjustability. Notice refers to the user's knowledge of the material that is being filtered.[186] Adjustability is

179. 47 U.S.C. § 230(c)(2) (2012).

180. 141 CONG. REC. 16,015 (1995) (statement of Sen. Feingold).

181. *Id.* (emphasis added).

182. *Id.* at 22,047 (emphasis added) (statement of Rep. Goodlatte).

183. *Id.* at 16,015 (statement of Sen. Feingold) (referring to Prodigy, America Online, and Compuserve as examples of "[o]n-line service providers").

184. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1176 (9th Cir. 2009).

185. *Id.* at 1177.

186. BALKIN ET AL., *supra* note 13, at 7–8; Berman & Weitzner, *supra* note 5, at 1632 ("User control . . .

the extent to which the ICS is capable of conforming to the users' preferences of what material to filter.[187] The importance of notice is evident from the *Pacifica* court's conclusion that radio lacks user control because listeners do not receive "prior warnings" of "program content."[188] Moreover, in explaining why the Internet is conducive to user control, Senator Feingold noted during a floor debate that "[m]ost newsgroups or bulletin boards that have sexually explicit materials are named such that there can be little doubt what types of materials one might encounter if you try to get into that area."[189] Focusing on adjustability is consistent with statements during the introduction of OFEA that filtering technologies would enable "every one of us . . . to tailor what we see to our own tastes"[190] and would "allow a parent to sit down and program the Internet to provide just the kind of materials that they want their child to see."[191]

KIS afforded users some degree of notice. The fact that users chose to purchase KIS indicates that they had general, ex ante notice that the installation of KIS would cause some material to be filtered.[192] "General" because all that users knew about the to-be-filtered material at the time of purchase and installation was that it would fall within the general category of "malware;" "ex ante" because the notice arose before the actual filtering of material. The *Zango* court also noted that "[w]hen a user attempted to download Zango software, KIS displayed a 'Web Anti–Virus Warning' that advised the user to block the Zango download."[193] In contrast with the general, ex ante notice users had when purchasing Zango, the notice provided by KIS's warnings was specific in that it identified the filtered material as Zango's software and contemporaneous because it was delivered at the time of filtering.[194]

Under the adjustability factor, there was a weaker case for finding that KIS exhibited user control because the override feature did not work.[195] To be sure, KIS did exhibit some adjustability in that once a user received a warning that KIS was blocking Zango's software, he or she had the option of uninstalling KIS. In this sense, users' continued use of KIS amounted to a

---

requires two functional attributes in a new medium: [1] the means of identifying the content being transmitted, and [2] the ability of the user to screen out certain kinds of content."); Palfrey, Jr. & Rogoyski, *supra* note 39, at 61.

187. BALKIN ET AL., *supra* note 13, at 8 ("[E]nd-users should have a choice about whether and what to filter."); Berman & Weitzner, *supra* note 5, at 1632 ("User control . . . requires two functional attributes in a new medium: [1] the means of identifying the content being transmitted, and [2] the ability of the user to screen out certain kinds of content.").

188. FCC v. Pacifica Found., 438 U.S. 726, 748 (1978).

189. 141 CONG. REC. 16,015 (1995) (statement of Sen. Feingold).

190. *Id.* at 22,045 (statement of Rep. Cox).

191. *Id.* at 22,046 (statement of Rep. White).

192. CDT *Zango* Brief, *supra* note 158, at 27 ("By installing anti-spyware software, the user is asking to be protected from spyware even if the user does not immediately recognize certain downloaded software as spyware.").

193. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1171 (9th Cir. 2009).

194. *See id.* ("When a user attempted to download Zango software, KIS displayed a 'Web Anti–Virus Warning' that advised the user to block the Zango download.").

195. *See id.* at 1171–72 ("The [KIS] 'Web Anti–Virus Warning' permitted the user to click 'Allow' to override the warning . . .; however, once the user clicked 'Allow,' a new 'File Anti–Virus Warning' appeared, stating . . . 'write access is denied.' [I]nstallation of Zango software was made impossible as a consequence.").

ratification of KIS's blocking of Zango's software. But a user's decision to refrain from uninstalling KIS does not necessarily indicate that the user preferred to not receive Zango's material and may instead indicate the user's adversity to other consequences that uninstallation would entail, such as leaving all material unblocked or having to purchase new filtering software. KIS would have been more adjustable had its override feature functioned properly, thus allowing users to unblock Zango's material while blocking other material. But the *Zango* court rejected the argument that such a feature is required under subsection (c)(2)(B).[196]

A final user control factor that courts should consider is the user's engagement (i.e. the level of activity the user exercises in the filtering process).[197] Focusing on engagement is consistent with the *Sable* court's conclusion that the "dial-it medium" exhibits user control because it "requires the listener to take affirmative steps to receive the communication."[198] Relying on *Sable*, Senator Feingold argued during floor debates that the Internet exhibits user control because users "typically do not stumble across information, but go out surfing for materials on a particular subject."[199] While the *Zango* court's subsection (c)(2)(B) analysis did not describe the specific activities involved in a user's operation of KIS, in discussing the facts of the case the court did mention that "KIS's warning include[d] an 'apply to all' checkbox that presumably is meant to stop the repeated warnings if the user opts to 'skip' and selects 'apply to all . . . .'"[200] The fact that users had to take the affirmative step of selecting "apply to all" in order to filter material weighs towards user control under the engagement factor. The engagement factor would have weighed less towards user control if, for example, the warning had disappeared automatically after a few seconds without any action by the user. Conversely, the engagement factor would have tilted even further towards user control had KIS required the user to take action every time he or she wanted to block Zango's material, as opposed to utilizing the "apply to all" function that resulted in KIS automatically blocking Zango's software on all future occasions after the user's initial selection.

To summarize, there are four factors that are prima facie applicable to a user control inquiry: (1) the status of the ICS as software as opposed to an online service provider; (2) notice; (3) adjustability; and (4) engagement. One might object that a factor-based approach to subsection (c)(2)(B), as opposed to a bright-line approach, undermines § 230's policy of reducing litigation costs. This criticism is especially pertinent given that subsection (c)(2)(B) should spare providers the costs and uncertainty of litigating the "good faith" requirement under subsection (c)(2)(A). But a factor-based approach need not be open-ended in every case. Factors can be useful when courts are addressing types of ICSs that have not been previously analyzed under subsection

196. *Id.* at 1176.

197. BALKIN ET AL., *supra* note 13, at 6 (arguing that a filtering system should "feature a user-friendly interface that encourages actual use of its features . . . .").

198. Sable Commc'ns of Cal., Inc. v. FCC, 492 U.S. 115, 127–28 (1989).

199. 141 CONG. REC. 16,015 (1995) (statement of Sen. Feingold).

200. *Zango*, 568 F.3d at 1171.

(c)(2)(B). Once application of the factors leads a court to find that a particular type of ICS exhibits user control, subsequent courts can foster certainty by presuming that that ICS qualifies for subsection (c)(2)(B) immunity. The remainder of this Part examines the factors more closely and illustrates how they might apply with respect to other ICSs like search engines and social networking sites.

B. Critiquing the Factors

1. The Software/Online Service Provider Distinction

As discussed above, the legislative history of the CDA suggests that Congress contemplated two categories of filtering: (1) filtering by software programs, which it referred to as performed by users, and (2) filtering by online service providers such as Prodigy, America Online, and CompuServe.[201] This suggests that ICSs that are more like software programs should satisfy subsection (c)(2)(B), whereas technologies that are more like Prodigy and America Online should fail subsection (c)(2)(B) and thus have to establish "good faith" under subsection (c)(2)(A). But determining what any given ICS is "more like" is difficult because Congress did not explain its basis for distinguishing between software programs and online service providers.

The distinction that Congress may have had in mind was that online service providers and software programs filtered material at different levels or, to borrow Jonathan Zittrain's terminology, different "point[s] of presence" on "the technical path between two points of communication on the Internet" from sender to receiver.[202] As one scholar notes:

> The process of filtering can take place at different levels on the Internet, though there are three major points: (1) at the sender's level, also referred to as the server-level, which is the place of origination of the speech (the web site containing the objectionable speech); (2) at the Internet Service Provider's level (ISP); or (3) at the receiver's or end user's level.[203]

Online service providers such as America Online and Prodigy provided subscribers with dial-up Internet access and also functioned as "walled garden[s]," which "direct[ed] subscribers to proprietary online forums or third-party content that [could not] be accessed by non-subscribers . . . ."[204] Thus, such providers were capable of employing server-level filtering of their proprietary content as well as ISP-level filtering in their capacity as providers of dial-up internet access. Describing the filtering capacities of online service providers during a floor debate, Senator Feingold stated that providers like

---

201. *See supra* notes 181–84 and accompanying text.

202. Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 655–56 (2003).

203. Otilio Gonzalez, *Regulating Objectionable Content in Multimedia Platforms: Will Convergence Require a Balance of Responsibilities Between Senders and Receivers?*, 20 SANTA CLARA COMPUTER & HIGH TECH L.J. 609, 630 (2004).

204. Anthony Ciolli, *Chilling Effects: The Communications Decency Act and the Online Marketplace of Ideas*, 63 U. MIAMI L. REV. 137, 166 (2008).

America Online and Prodigy "act[ed] as . . . intermediar[ies] between the user and the Internet," thus enabling them to "eliminate access to certain services."[205]

Software programs, on the other hand, imposed filtering at the end-user level.[206] In concluding that "blocking and filtering software" was more consistent with the First Amendment than source-based restrictions like COPA, the Supreme Court noted in *Ashcroft* that filters "impose selective restrictions on speech at the receiving end, not universal restrictions at the source."[207] Furthermore, several influential Internet law scholars of the 1990s argued that filtering imposed at the end-user level was more consistent with user control than filtering imposed at the server level or ISP level.[208] For instance, in explaining why PICS, a rating system for filters, "enable[d] user control,"[209] Lawrence Lessig stated:

> PICS is an application level filtering protocol. Its use is end-to-end. The filter gets invoked in a user's application. The filtering is not designed to interfere with the flow of the network itself. No system between the sender and the receiver need make a judgment about whether to deliver content based on the content of message.[210]

Lessig proceeded to cite "the use of PICS by a search engine . . . [to] filter the results of a search" as an example of "upstream filtering," which he argued did not exhibit user control.[211] It is plausible that Congress's basis for distinguishing between software programs and online service providers was that the former utilized filtering at the end-user level whereas the latter utilized "upstream" filtering at the server level and/or ISP level. One might argue on this basis that filtering should satisfy subsection (c)(2)(B) if and only if it is imposed at the end-user level.

But courts should disregard the "levels" analysis in applying subsection (c)(2)(B). It is difficult to identify modern analogues to the "walled garden" ISPs of the mid-nineties, like America Online and Prodigy. The use of "walled garden" providers declined sharply throughout the late '90s and early 2000s.[212] The modern ISP market is dominated by broadband access providers which "provide[] subscribers with unfettered access to the Internet" and do not offer proprietary content.[213] As a result of this disaffiliation between access providers and content providers, a court is unlikely to encounter a defendant provider that is capable of filtering at both the server level and the ISP level, as

---

205. 141 CONG. REC. 16,015 (1995) (statement of Sen. Feingold).

206. *See* Gonzalez, *supra* note 203, at 631 (noting that filtering at end-user level takes place through filtering software).

207. Ashcroft v. ACLU, 542 U.S. 656, 667 (2004).

208. *See, e.g.*, BALKIN ET AL., *supra* note 13, at 6 ("[M]eaningful choice by end-users requires a variety of filtering options that reflect different cultural values and ideologies"); Jerry Berman & Daniel J. Weitzner, *Developments in the Law—The Law of Cyberspace*, 112 HARV. L. REV. 1634, 1642–43 (1999) (finding that other types of filtering "may impose an externality on individuals who want unfiltered Internet activity.").

209. Lessig, *supra* note 5, at 661.

210. *Id.* at 660.

211. *Id.* at 661.

212. Ciolli, *supra* note 204, at 169–73.

213. *Id.* at 173.

the "walled garden" providers were. In order to assess whether a provider that filters at only one of the levels is analogous to a "walled garden" provider for purposes of the "levels" analysis, a court would have to determine whether Congress's basis for distinguishing such providers from software providers was their capacity for server-level filtering, for ISP-level filtering, or the combination of both. But the legislative history of the CDA does not answer this question. Thus, the fact that a provider does not utilize end-user level filtering should not disqualify it from subsection (c)(2)(B).

Nor should the use of end-user-level filtering be sufficient for a technology to satisfy subsection (c)(2)(B). Even where filtering is imposed at the end-user level, inasmuch as it is implemented by software installed on the end user's computer, it may nonetheless be subject to more control by the provider than Congress envisioned in 1996. As Zittrain notes:

> [T]he rise of always-on, broadband-connected PCs means that software or operating systems need not follow a factory-produces, consumer-inherits sequence. Software can become service, tuned and re-tuned near-instantly by its author, like a child who leaves home but finds the parents not only constantly in touch, but able to set and adjust curfews from afar.[214]

Indeed, KIS was exemplary of this trend in that it was "designed to be updated regularly in order to keep malware definitions current" and could be configured by the user "to communicate automatically with [Kaspersky's] online update servers."[215] Just as a projectionist is not the sole producer of a movie merely because he or she pushes the last button, it would be too formalistic to conclude that a KIS user was the party who had filtered Zango's material just because the filtering was imposed at the end-user level.

The broader point is that the user control inquiry should focus on who is responsible for a filtering decision, not on where in the network it is implemented. This is consistent with *United States v. Playboy*, in which the Supreme Court invalidated a provision of the CDA that required cable TV operators to fully scramble or fully block premium channels carrying sexually oriented programming.[216] Following the *Sable* Court's user control approach, the Court found that the requirement was unnecessary given "the feasibility of a technological approach to controlling minors' access" to the sexually oriented programming.[217] Specifically, the Court noted that "viewers could order signal blocking on a household-by-household basis."[218] Even though the blocking was implemented by the cable provider, the fact that it was ordered by the viewer made it a form of user control. Similarly, in cases where a provider imposes filtering at the server level or ISP level, the provider should still be able to satisfy subsection (c)(2)(B) if the filtering is traceable to an end user's exercise of control, as assessed under the other factors.

---

214. Jonathan Zittrain, *A History of Online Gatekeeping*, 19 HARV. J.L. & TECH. 253, 296 (2006).
215. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1171 (9th Cir. 2009).
216. United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 807 (2000).
217. *Id.* at 814.
218. *Id.* at 807.

2. Notice

In applying the notice factor, courts should consider both the content and the timing of the notice. The notice should provide specific information about what material is being filtered. In general, the notice should identify the sender attempting to disseminate the material. In the case of a browser filter, the notice should state the URL of the blocked web site. An e-mail spam filter should state the e-mail address of the sender of the alleged spam.

However, in some contexts, an identification of the sender of material may result in the user having little information about the content of the filtered material. For example, on an anonymous message board, notice that posts from a particular moniker have been deleted may not inform other users about the content of the deleted posts. However, if a user receives notice contemporaneously with his or her attempt to access material, he or she is in a better position to infer the content of the filtered material. Seeing the notice of deletion placed within a thread topic, for instance, may allow the user to infer the content of the deleted post from the topic and the surrounding posts. Such contextual cues would not be available, however, if the user were to merely receive periodical updates of deleted posts listed by moniker.

Where notice is neither specific nor contemporaneous, the filtering should fail subsection (c)(2)(B) barring an especially strong showing under the other factors. An example of notice that is neither specific nor contemporaneous to filtering is an ICS's terms of service. YouTube, for instance, has removed content from its hosting service for violation of its policy against "speech which attacks or demeans a group based on race or ethnic origin, religion, disability, gender, age, veteran status, and sexual orientation/gender identity."[219] This is insufficient under the notice factor to establish user control over a search result that fails to yield such content. Similarly, general statements in the licensing agreement for a filtering software program are insufficient to establish user control under the notice factor.[220]

3. Adjustability

As *Zango* illustrates, a user generally has two methods of adjusting an ICS to make it conform to his or her preferences. First, a user can stop using the ICS. In focusing on the user's ability to "uninstall [KIS] and buy blocking software from another company," the court noted that "[r]ecourse to competition is consistent with the statute's express policy of relying on the market for the development of interactive computer services."[221] Second, a user can adjust the settings of the ICS. As Judge Fisher noted, filtering

219. *YouTube Community Guidelines*, YOUTUBE, https://www.youtube.com/t/community_guidelines (last visited Feb. 24, 2014).

220. *See* NATHANIEL GOOD ET AL., STOPPING SPYWARE AT THE GATE: A USER STUDY OF PRIVACY, NOTICE AND SPYWARE 2 (2005), *available at* http://homepages.uconn.edu/~dbt12001/papers/SpywarePaperFinal.pdf ("[T]here is a general perception that these notices [licensing agreements] are ineffective. One software provider included a $1000 cash prize offer in the EULA that was displayed during each software installation, yet the prize was only claimed after 4 months and 3,000 downloads of the software.").

221. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1177 (9th Cir. 2009).

software might fail to "accommodat[e] . . . the user's preference, either not providing an override option or making it difficult to use."[222] Either method can weigh towards user control, depending on how much it enables the user to effectuate his or her preferences for what material to filter and receive.

Several examples illustrate how ceasing to use an ICS may or may not enable a user to effectuate his or her preferences. A KIS user who preferred to use Zango's software could have achieved this end by uninstalling KIS. In other cases, however, ceasing to use the ICS will not result in access to the blocked material. For instance, if an ISP has blocked material, unsubscribing from the ISP will not enable a user to access the material because he or she will be left without an Internet connection on his or her computer. To view the blocked material, the user would have to find an alternative ISP that does not block the same material, which may be difficult given concentration in the market for broadband services.[223] Similarly, if Facebook terminates a member's account, his or her posts and profile are unavailable not only to Facebook users, but users of any other social networking site as well. Thus, the extent to which a user's ability to stop using an ICS weighs towards user control depends on whether the user can acquire the blocked material from alternative sources.

Even if an ICS has an override feature which enables the user to view filtered material without having to rely on alternative sources, it may nonetheless not exhibit sufficient adjustability. Consider, for instance, a filter that allows users to select amongst broad categories of material such as "pornography," "violence," or "hate speech." If material falling within one of the categories is blocked, the user can view it by adjusting the filter to stop blocking that category. However, turning off a category of filtering will expose the user to all other material falling within that category. Thus, an overbroad override feature may expose the user to more objectionable material than he or she wishes to receive and thus fail to effectuate the user's preferences. As with the notice factor, the assessment of whether an override feature weighs towards user control should depend on specificity. The more specifically a user can issue commands for the ICS to stop filtering material, the more heavily the ICS weighs towards user control under the adjustability factor.

4. Engagement

Engagement is the user's level of activity in the filtering process. A user is active in the filtering process to the extent that the ICS's filtering is the immediate result of the user's inputs to the ICS's interface. For example, a search engine weighs towards user control under the engagement factor because it filters out irrelevant results immediately upon the user's input to the search engine's interface (i.e. clicking of the "search" button). In contrast,

222. *Id.* at 1179 (Fisher, J., concurring).

223. *See supra* note 21 and accompanying text (arguing that scarcity in the ISP market diminishes the extent to which ISPs are susceptible to competitive pressure).

standalone filtering software, such as KIS, generally involves a low level of user activity. The user periodically selects material to block or unblock, but the actual filtering occurs when the user gives inputs to the interface of a different ICS such as an Internet browser. In order for a user's activity to weigh towards user control under the engagement factor, the activity must be directed at the ICS that is performing the filtering.

C. Overview: Tying Together the Factors

In determining whether an ICS exhibits sufficient user control to satisfy subsection (c)(2)(B), courts should apply the notice, adjustability, and engagement factors. Courts should not assess whether the ICS is more like filtering software or online service providers like America Online or Prodigy. An ICS does not have to weigh heavily toward user control under all of the factors. A search engine, for example, may fail to provide adequate notice of the vast amount of material that it filters out of search results. But a search engine still may satisfy subsection (c)(2)(B) under the adjustment and engagement factors because users have the ability to access omitted websites from alternative sources and because search results are the immediate result of a user's inputs to the search engine's interface. On the other hand, ISP filtering should fail subsection (c)(2)(B) because ceasing to use an ISP does not result in access to the filtered material and because generally an ISP does not have an interface into which a user enters inputs.

V. INTERPRETING SUBSECTION (C)(2)(A)

If a provider has not ceded a sufficient level of control to the user to satisfy subsection (c)(2)(B), the provider can alternatively attempt to satisfy subsection (c)(2)(A). In order for the prospect of immunity under subsection (c)(2)(B) to encourage providers to develop technologies that maximize user control, courts must construe "good faith" in a way that makes immunity under subsection (c)(2)(A) more than a mere formality. Otherwise providers would be indifferent between the two provisions and would not be encouraged to develop technologies that satisfy subsection (c)(2)(B). However, if courts were to make immunity under subsection (c)(2)(A) too difficult to obtain, they would be failing to "remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[224] This Part proposes an interpretation of subsection (c)(2)(A) that balances these competing concerns.

A. Otherwise Objectionable

When assessing a provider's subsection (c)(2)(A) defense, a court should assess whether the provider has a good faith subjective belief that the material

224. 47 U.S.C. § 230(b)(4) (2012).

at issue (i.e. the material that the plaintiff is seeking to hold the provider liable for blocking) is obscene, lewd, etc. Courts have generally construed the term "considers" as imposing a subjective standard.[225] Thus, even if a reasonable person would not find the filtered material to be obscene, lewd, etc., the provider can nonetheless satisfy subsection (c)(2)(A) so long as it subjectively deems the filtered material to be obscene, lewd, etc. The provider's subjective belief that material is obscene, lewd, etc. must be genuine, similar to how an obligor to a contract with a satisfaction clause cannot feign dissatisfaction in order to avoid performance.[226] Furthermore, because of subsection (c)(2)(A)'s "good faith" requirement, the level of deference that courts accord to providers' allegations as to considering material obscene, lewd, etc. should be lower than in the (c)(2)(B) context, where there is no good faith requirement.

However, the fact that a provider must subjectively consider material to be objectionable does not mean that the provider must review material on an individualized basis prior to filtering it. In many cases, a provider will filter without having any specific knowledge of the material it is filtering. For example, a provider might filter material by means of an algorithm that operates according to generally defined criteria. Or, alternatively, a provider's adoption of a policy against certain categories of material may preemptively filter material falling within the categories by deterring users from attempting to disseminate such material. The filtering in these examples are instances of "action . . . taken . . . to restrict access" and would thus be prima facie eligible for § 230(c)(2) immunity. But the analysis of the obscene, lewd, etc. would be slightly different from a case where a provider filters material based on specifically reviewing it. Instead of focusing on the provider's good faith belief with respect to the actual material that has been filtered, the inquiry would assess whether the provider has a good faith, subjective belief that the general category of material is obscene, lewd, etc. and whether the provider has made a good faith attempt to limit the filtering material falling within the category.

In determining whether a provider has a good faith belief that material (or a category of material) is obscene, lewd, etc., a court first has to identify the

225. *See* Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. Mar. 11, 2011) ("No court has articulated specific, objective criteria to be used in assessing whether a provider's subjective determination of what is ''objectionable'' is protected by § 230(c)(2)."); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567, 2010 WL 1799456, at *6 (D.N.J. May 4, 2010) ("[A] party is entitled to immunity for causes of action arising out of its efforts to restrict or block material when the party . . . subjectively believed that the material blocked or restricted was a) obscene, b) lewd, c) lascivious, d) filthy, e) excessively violent, f) harassing, or g) otherwise objectionable."); E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 608 (N.D. Ill. 2008) ("[S]ection 230 imposes a subjective element into the determination of whether a provider or user is immune from liability."). *But see* Google, Inc. v. MyTriggers.com, Inc., No. 09CVH10-14836, 2011 WL 3850286, at *5 (Oh. Com. Pl. Aug. 31, 2011) ("[T]he CDA provides immunity to any 'interactive computer service' which restricts access to content *that is* 'obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable.'" (emphasis added)).

226. Hill v. Perrone, 42 P.3d 210, 213 (Kan. Ct. App. 2002) ("[If] [p]arties to a contract . . . stipulate that performance by one of them shall be to the satisfaction of the other . . . the party to be satisfied is the judge of his own satisfaction, subject to the limitation that he must act in good faith. He should fairly and candidly investigate and consider the matter, reach a genuine conclusion, and express the true state of his mind. He can not act arbitrarily or capriciously, or merely feign dissatisfaction." (quoting Hollingsworth v. Colthurst, 96 P. 851, 851 (Kan. 1908))).

term that comes closest to describing the material at issue. Then, the court must determine, based on how close the applicable term comes to describing the material, whether it is plausible that the provider could consider the term to be descriptive of the material. The main challenge in this inquiry is the term "otherwise objectionable."[227] In cases where the material at issue has not been easily classifiable as obscene, lewd, lascivious, filthy, excessively violent, or harassing, providers have asserted that "otherwise objectionable" is, to use Judge Fisher's phrase, an "unbounded catchall phrase."[228] While some courts have suggested that this broad reading of "otherwise objectionable" is appropriate,[229] other courts have applied the canon of interpretation *ejusdem generis* to limit the scope of "otherwise objectionable" to material that is similar to the preceding terms.[230]

The problem with the broad reading of "objectionable" is that the text of subsection (c)(2)(A) suggests that Congress intended for courts to construe the term more narrowly than the term's literal definition.[231] Had Congress intended subsection (c)(2)(A) to apply to material that is objectionable in a literal sense—in addition to material that is obscene, lewd, lascivious, filthy, excessively violent, or harassing—it could have simply used the term "objectionable" without all of the preceding terms. Stated that way, the statute would still apply to material that is obscene, lewd, lascivious, filthy, excessively violent, or harassing because any material possessing those qualities is also objectionable in a literal sense. Thus, consistently with the principle of *ejusdem generis*, courts should construe "objectionable" as having a similar meaning to "obscene," "lewd," "lascivious," "filthy," "excessively violent," or "harassing."

But in applying *ejusdem generis*, courts face the difficult task of determining how similar material must be to the preceding terms in order to qualify as "objectionable." It will not suffice to say that "objectionable" must be the *same* as any or all of the preceding terms, because that would make "objectionable" superfluous. One might suppose, based on the terms "obscene, lewd, lascivious, filthy, [and] excessively violent," that in order for material to be otherwise objectionable, it must implicate Congress's policy of "empower[ing] parents to restrict their children's access to objectionable or

227. *Holomaxx*, 783 F. Supp. 2d at 1104 ("No court has articulated specific, objective criteria to be used in assessing whether a provider's subjective determination of what is 'objectionable' is protected by § 230(c)(2) . . . .").

228. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178 (9th Cir. 2009) (Fisher, J., concurring). The broadest reading of "objectionable" that I am aware of was made by Google: "Google argues that the phrase 'otherwise objectionable' contained within § 230(c)(2) must be read to include any type of editorial discretion it uses when selecting which ads to include in its search results." *MyTriggers.com*, 2011 WL 3850286, at *5–6.

229. *Smith*, 2010 WL 1799456, at *6–7; Langdon v. Google, Inc., 474 F. Supp. 2d 622, 631 (D. Del. 2007).

230. *MyTriggers.com*, 2011 WL 3850286, at *5–6; Goddard v. Google, Inc., No. C 08-2738 JF, 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008); Nat'l Numismatic Certification, LLC v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *25 (M.D. Fla. July 8, 2008).

231. OXFORD ENGLISH DICTIONARY 643 (2d ed. 1989) (defining "objectionable" as "[o]pen to objection; that may be objected to; against which an adverse reason may be urged; now often in a weakened sense: [e]xciting disapproval or dislike, unacceptable, disagreeable, unpleasant.").

inappropriate online material."[232] But the problem with this construal is the term "harassing," which several courts have used in reference to material that is not any more unsuitable for children than it is to adults, such as spam e-mail.[233] Indeed, the term "harass" also appears elsewhere in the 1996 Telecommunications Act—namely 47 U.S.C. § 223(a)—which contains separate provisions governing obscenity (§ 223(a)(1)(B)) and harassment (§§ 223(a)(1)(A), (C), (D), and (E)), with only the former being limited to material directed at children under 18.[234] So, "objectionable" cannot be limited to material that is unsuitable for children.

Instead, courts should require that material be similar to the preceding terms in the respect that all of the preceding terms are characteristics that degrade the quality of the ICS for users. In other words, to qualify as "objectionable," material must degrade the quality of the ICS for users. This is a broader construal of "objectionable" than courts have reached under the principle of *ejusdem generis*.[235] For instance, eBay could have established that counterfeit coins had the tendency to degrade the quality of an eBay user's online shopping.[236] However, this interpretation is not broad enough to cover cases of anticompetitive blocking that concerned Judge Fisher.[237] From the provider's standpoint, exluding materials that it finds "otherwise objectionable" is consistent with the fact that subsection (c) is entitled "[p]rotection for 'good samaritan' blocking and screening of offensive material."[238] The term "good Samaritan"[239] indicates that Congress intended for subsection (c)(2)(A) to protect providers who block material for the benefit of their users, not for their own personal or financial benefit.

Of course, anticompetitive blocking is not the only potential policy drawback of immunity for filtering. Construing "objectionable" as including any material that degrades the quality of a provider's ICS for users encourages providers to filter significantly more material than a more narrow construal would. This is especially so if providers can claim immunity for filtering performed on a generalized basis, such as where a provider preemptively excludes certain generally-defined categories of material. Some critics would object to such widespread filtering on the ground that it would greatly reduce the diversity of material to which Internet users are exposed.

However, there are several indications that in enacting § 230(c)(2),

232. 47 U.S.C. § 230(b)(4) (2012).

233. *Holomaxx*, 783 F. Supp. 2d at 1104; *MyTriggers.com*, 2011 WL 3850286, at *7 (stating in dicta that spam e-mail would fall under the term "harassing"); *Nat'l Numismatic Certification,* 2008 WL 2704404, at *25 n.35 (stating in dicta that the political commentary at issue in *Langdon* could be characterized as harassing because it advocated "against a group").

234. 47 U.S.C. § 223(a).

235. *Nat'l Numismatic Certification*, 2008 WL 2704404, at *25 ("Under [the cannon of ejusdem generis], when a statute sets out a series of specific items ending with a general term, that general term is confined to covering subjects comparable to the specifics it follows." (citing Hall Street Assocs., L.L.C. v. Mattel, Inc., 552 U.S. 576, 586 (2008))).

236. *Id.*

237. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178–80 (9th Cir. 2009) (Fisher, J., concurring).

238. 47 U.S.C. § 230(c).

239. *Luke* 10:30–37 (expressing that a Good Samaritan is a person who gratuitously gives help or sympathy to those in distress).

Congress was willing to tolerate this reduction in diversity for the sake of improving users' ability to avoid unwanted material. First, § 230(b)(3) provides that "user control" should be over "what information is received."[240] Congress's focus on the control exercised by recipients on speech, as opposed to speakers, indicates its agreement with the proposition that an audience's interest in avoiding speech trumps the speaker's interest in disseminating it. Second, Rep. Cox stated during the introduction of OFEA, that "[w]e can go much further . . . than blocking obscenity or indecency, whatever that means in its loose interpretations. We can keep away from our children things not only prohibited by law, but prohibited by parents."[241] This indicates that Congress contemplated a wide variety of contexts in which users would rely on filtering software to avoid unwanted material. Deferring to users' preferences as to what constitutes objectionable material is also consistent with the user control doctrine the Supreme Court relied on in *Sable* and *Pacifica*, which is based on the principle that each "householder [is] the exclusive and final judge of what will cross his threshold."[242]

Others might argue that denying immunity in cases where only the provider deems material objectionable conflicts with the premise that a provider's subjective belief that filtered material is objectionable should satisfy subsection (c)(2)(A). However, there is no inconsistency in holding, on the one hand, that subsection (c)(2)(A) can be satisfied by the provider's subjective belief and, on the other hand, that the *content* of the provider's subjective belief must pertain to users' experiences with the ICS.

A similar objection is that cases where material degrades the quality of the ICS for users are covered in the phrase "user considers"[243] and that by requiring that the "provider or user considers" material be objectionable, subsection (c)(2)(A) makes establishing that the "user considers" material is objectionable a disjunctive requirement. By making "user considers" a disjunctive requirement, the argument goes, Congress expressly indicated that courts should not treat it as a necessary requirement. Finally, the argument continues, requiring that the material degrades the quality of the ICS for users—even in cases where the provider seeks to rely on "provider . . . considers" rather than "user considers" and treats "user considers" as a necessary requirement—runs contrary to the express indication in the text that it should only be a disjunctive requirement.

The problem with this argument is that "provider or user considers" is not a disjunctive requirement. That is, a provider cannot satisfy subsection (c)(2)(A) by relying on the "user considers" language. Subsection (c)(2)(A) refers to "the provider or user" with "the" indicating that "user" refers to a specific user—namely, the user who has filtered material. Thus, the "user considers" language is only relevant in cases where the defendant is a user that has filtered material. In cases where the defendant is a provider, the "user

240. 47 U.S.C. § 230(b)(3).
241. 141 CONG. REC. 22,045 (1995) (statement of Rep. Cox).
242. Rowan v. U.S. Post Office Dep't, 397 U.S. 728, 736 (1970).
243. 47 U.S.C. § 230(c)(2)(A).

considers" language is obsolete. Therefore, it is not the case that subsection (c)(2)(A) expressly indicates that "user considers" is a disjunctive requirement. In the absence of such an express indication, incorporating a "quality of the ICS for users" component into the requirement that the provider consider material to be objectionable does not contravene the language of the statute.

B. Inadvertent Blocking

In addition to filtering of material that the provider considers in good faith to be obscene, lewd, etc., subsection (c)(2)(A) should also apply in cases where the provider inadvertently blocks material even if the provider does not consider such material to be obscene, lewd, etc. For example, a filtering algorithm may yield false positives by filtering material that does not fall within the general categories the algorithm was programmed to filter. In such a scenario, the provider should satisfy subsection (c)(2)(A) so long as the blocking of the material at issue was an inadvertent mistake resulting from the provider's good faith attempt to block material that the provider considered to be obscene, lewd, etc. While no defendant has attempted to argue that subsection (c)(2)(A) should cover inadvertent blocking, providing immunity for such blocking is consistent with the language of subsection (c)(2)(A).

The language that supports subsection (c)(2)(A) applying to inadvertent blocking is "action . . . taken . . . to restrict access . . . ."[244] The phrase "taken . . . to" indicates that the action subsection (c)(2)(A) immunizes is the provider's attempt to block material, not the completed act of blocking material. Thus, the material that the provider must consider obscene, lewd, etc. is the material it has attempted—or taken action—to block, as opposed to the material it may inadvertently block as a result. In a scenario where a provider's good faith attempt to block material that it considers to be obscene, lewd, etc. results in the blocking of material that the provider does not consider to be obscene, lewd, etc., then the provider should satisfy subsection (c)(2)(A). Liability for the blocking of material that resulted from the provider's attempt would be tantamount to liability on account of action taken to restrict access and, thus, contrary to the text of subsection (c)(2)(A).

Providing immunity for inadvertent blocking of non-objectionable material "remove[s] disincentives for the development and utilization of blocking and filtering technologies."[245] If the provider could not establish immunity from liability for a mistaken attempt to block material that it considered objectionable, then it might refrain from making any attempts to block such material. The need for immunity in cases of good faith mistakes is especially apparent in light of the fact that many filtering technologies that providers utilize involve automated assessments of large volumes of material.[246] Utilization of such filtering technology is bound to result in the

244. *Id.*

245. *Id.* § 230(b)(4).

246. NAT'L RESEARCH COUNCIL, *supra* note 13, at 53 ("[T]he sheer size of the Web means that the screening process involved must involve a mix of automated and human process.").

inadvertent blocking of non-objectionable material. Subsection (c)(2)(A) should thus be construed to give the provider a margin for error.

Determining whether material was blocked as the result of an attempt to block other material poses evidentiary difficulties. Presumably, it will frequently be the case that the provider engages in efforts to block material it believes in good faith to be obscene, lewd, etc. It will be difficult to determine whether the filtering of the material at issue arose out of such efforts or whether the provider intentionally targeted the material at issue despite lacking a good faith belief that it was obscene, lewd, etc. As a technological matter, it is unclear whether a computer forensics expert could distinguish between these two types of cases by inspecting the way a provider has programmed its filter. Similarly unclear is whether the expenses necessary for such an inspection would substantially raise the litigation costs involved in establishing immunity. Thus, like the issue of whether the provider considers the material it has blocked to be obscene, lewd, etc., the issue of whether material has been blocked by mistake will depend on circumstantial evidence pertaining to good faith.

C. Good Faith

Whether a provider seeks to establish that it considered the material it has filtered to be obscene, lewd, etc. or that it blocked material by mistake, subsection (c)(2)(A) requires good faith. Assuming that direct evidence is not available, courts will have to rely on circumstantial evidence.[247] In analyzing the good faith requirement, courts have discussed indicia including: (1) whether the provider has filtered material by one sender while not filtering similar material from other senders;[248] (2) whether the provider's filtering techniques conformed to an industry standard;[249] (3) whether the provider was seeking to derive a payment in order to unblock material;[250] (4) whether the provider has put forth a credible explanation of why it blocked the material at issue;[251] and (5) whether the provider has complied with users' requests to stop blocking particular non-objectionable material.[252] Thus, there are a variety of

247. *Cf.* Sullivan v. Solimini (*In re* Sullivan), 326 B.R. 204, 211 (B.A.P. 1st Cir. 2005) (applying a "totality of the circumstances test to determine whether a debtor lacked good faith in filing a Chapter 13 petition for purposes of [11 U.S.C.] § 1307(c)").

248. E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008) ("[E360Insight] argues that . . . 'Comcast has not acted in good faith. Comcast allows numerous other companies to send bulk emails in greater volume and with greater frequency . . . singling out Plaintiff when others behaving in a like manner are not treated in a like fashion.'" (quoting Plaintiff's Brief)).

249. Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1105 (N.D. Cal. 2011) ("Holomaxx alleges no facts in support of its conclusory claim that Microsoft's filtering program is faulty, nor does it identify an objective industry standard that Microsoft fails to meet.").

250. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2010 WL 1799456, at *6–7 (D.N.J. May 4, 2010).

251. Smith v. Trusted Universal Standards in Elec. Transactions, Inc., Civil No. 09-4567, 2011 WL 900096, at *9 (D.N.J. Mar. 15, 2011) ("The Court finds that a reasonable jury could conclude that Comcast acted in bad faith when it failed to respond to Plaintiff's repeated requests for an explanation why it continually blocked Plaintiff's outgoing email.").

252. *Holomaxx*, 783 F. Supp. 2d at 1097 ("Nor does Holomaxx cite any legal authority for its claim that Microsoft Corp. has a duty to discuss in detail its reasons for blocking Holomaxx's communications or to

factual issues a provider may have to litigate under the good faith requirement.

Requiring the provider to litigate a variety of factual issues in order to establish good faith is at odds with § 230's policy of "remov[ing] disincentives for the development and utilization of blocking and filtering technologies." Litigating a broad range of circumstantial evidence is costly, even in cases where the evidence does not lead to a finding of bad faith. Because a good faith defense can be costly to litigate even if it is meritorious, the prospect of having to litigate such a defense has a deterrent effect on all filtering, not just filtering that is inconsistent with users' preferences. Furthermore, if courts construe "good faith" as an open-ended phrase that encompasses many different factors, providers will be uncertain about what filtering procedures they must adopt in order to avail themselves of subsection (c)(2)(A) immunity. However, it is difficult to see how courts could apply the "good faith" requirement without reviewing circumstantial evidence of good faith. To disregard such evidence would effectively read "good faith" out of the statute.

To reconcile the tension between the "good faith" requirement and the policy to remove disincentives for filtering, courts should articulate what evidence is and is not relevant under the good faith inquiry. Specifically, courts should assess two factors: (1) communications amongst the provider and the users who the provider filters material from and (2) the extent to which market forces constrain the provider's filtering decisions. While these factors are broad enough to be costly to litigate in some cases, they are narrow enough to exclude evidence that courts have alluded to, such as the provider's response to a sender's request to unblock material and whether the provider's filtering practices comply with an industry standard.

1. Provider-User Communications

Communications between the provider and its users can support the provider's claim that it considered the material it has filtered to be objectionable. This is true of communications from the provider to its users as well as communications from users to the provider. For instance, the fact that the provider has communicated a general filtering policy to users serves as evidence that the provider believes that its users are amenable to the filtering of material encompassed within the policy. Thus, although general, ex ante notice of this sort would not enable the provider to satisfy subsection (c)(2)(B), it can help demonstrate that the provider believed in good faith that certain material would degrade the quality of its ICS for users.

Of course, communications from the provider to users should only support a finding of good faith if the filtering at issue is consistent with the provider's communications. For example, a provider's representation that its filtering software is directed at Nazi propaganda would demonstrate that the provider believed its users are amenable to filtering of Nazi propaganda but

---

provide a remedy for such blocking. Indeed, imposing such a duty would be inconsistent with the intent of Congress to 'remove disincentives for the development and utilization of blocking and filtering technologies.'" (citing 47 U.S.C. § 230(b)(4) (2006))).

would not demonstrate that users of the provider's software are also amenable to the filtering of pop-up advertisements. Similarly, if a provider fails to communicate a filtering policy to its users, such as where a search engine acts contrary to the FTC's directive for search engines to ensure that "the use of paid inclusion is clearly and conspicuously explained and disclosed,"[253] a court may infer that the provider believed its users are not amenable to such filtering, which should weigh against a finding of good faith.

Communications from users to the provider should also be relevant. Requests to remove material support a finding that the provider had a good faith belief that the requested material degraded the quality of the ICS for users and was thus objectionable. In assessing communications from a user to the provider, courts must be careful to distinguish between senders and recipients of material. While requests from recipients for the provider to block material are relevant under the good faith inquiry, requests from senders to unblock material generally should not be relevant. Although senders in many cases are users of an ICS's service, § 230(c)(2) is intended to protect receivers from viewing unwanted material. This is evident from the fact that § 230(b)(3) provides that "user control" should be control "over what information is received," not over what material is disseminated. Thus, contrary to *Smith*, the good faith requirement does not impose a duty on providers to respond to a sender's request to unblock e-mails, either by complying with the sender's request or by explaining the basis for its refusal.[254] The fact that a sender does not believe that his or her e-mails are objectionable has little bearing on whether recipients of the e-mails would find them objectionable.

However, in cases where the provider is alleging that material was blocked inadvertently, communications from the sender to the provider may be relevant. If a provider receives notice from a sender that it has blocked non-spam e-mail and continues to block it anyway, then it is difficult to characterize the provider's continued blocking as inadvertent. In this scenario, there are several arguments that a provider can make to preserve an inadvertent blocking argument under subsection (c)(2)(A). First, the provider can argue that it was unable to verify the accuracy of the sender's assertion that the blocked material was not objectionable. Maintaining a protocol for receiving and verifying requests to unblock can be costly,[255] so in many cases it is plausible that notice from a sender will be an insufficient basis on which to impute knowledge of the mistake to the provider. Second, even if the provider has verified the accuracy of the sender's request to unblock, the provider may lack the technical ability to comply with the sender's request. For instance, if a

253. Letter from Heather Hippsley, Acting Assoc. Dir., Div. of Adver. Practices, Fed. Trade Comm'n, to Gary Ruskin, Executive Dir., Commercial Alert (June 27, 2002), *available at* https://web.archive.org/web/20130723064344/http://www.ftc.gov/os/closings/staff/commercialalertletter.shtm (original webpage has been removed, can be accessed using archive.org).

254. *Smith*, 2011 WL 900096, at *8–9.

255. David S. Ardia, *Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act*, 43 LOY. L.A. L. REV. 373, 391 (2010) ("It is costly for intermediaries to offer dispute resolution procedures to their users. It is far less costly to simply remove speech at the first sign of trouble or to decline to carry controversial speech in the first place.").

provider uses an algorithm to filter material, then it may be difficult for the provider to adjust the algorithm so as to unblock the sender's non-objectionable material while not also unblocking a lot of objectionable material in the process. In such cases, the provider's continued blocking of the sender's material would be the result of "action . . . taken . . . to" block objectionable material, within the meaning of subsection (c)(2)(A).

2. Market Forces

Even in the absence of any evidence of provider-user communications, it is still plausible to infer that the provider has filtered consistently with users' preferences. This is because providers depend on users for revenue, and users will cease to use a provider's service if it filters against their preferences.[256] As such, the fact that a provider utilizes a certain filtering practice suggests that its users are amenable to that practice and hence that the provider should satisfy the good faith requirement. For example, the allegation that a provider has utilized faulty filtering technology should not negate the good faith requirement because the provider's widespread use of the particular technology suggests that users are amenable to its faults. It is plausible that users would be amenable to a faulty filtering technology because the alternative—a more sophisticated filtering technology—may require costs that the provider would pass along to the user, either through subscription fees or by displaying more advertisements.

However, in relying on market forces as an indicator of good faith, courts should be sensitive to characteristics that limit a provider's susceptibility to such forces. For instance, if a provider filters in a way that is difficult to detect, then it is unlikely that users will respond by ceasing to use the provider's service. In addition to failing to notify users that filtering is taking place, providers can also make filtering difficult to detect by only filtering a small class of material. As Jonathan Ezor notes in the context of spam filters, "where a single, legitimate sender's messages (or even Web site) are blocked, unless a large number of users expect to receive the messages, the impact an incorrect block listing has on the community as a whole will be minimal, thereby making any resulting market forces negligible."[257] In this respect, E360Insight's allegation that Comcast "single[d] out" its e-mails as spam while "allow[ing] numerous other companies to send bulk emails in greater volume and with greater frequency" supported its position that Comcast did not satisfy the good faith requirement.[258]

Additional characteristics that should limit a court's reliance on market forces include market concentration and switching costs. These characteristics are exemplified by broadband ISPs. In promulgating the network neutrality rules, the FCC stated that a broadband provider's "incentive to favor affiliated

256. Goldman, *supra* note 51, at 672 ("Thus, marketplace incentives work unexpectedly well to discipline online providers from capriciously wielding their termination power.").

257. Ezor, *supra* note 18, at 47.

258. E360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008).

content" and "block . . . traffic . . . will . . . be greater if end users are less able to respond by switching to rival broadband providers," and that this was indeed the case because "most residential end users today have only one or two choices for wireline broadband Internet access service."[259] In further concluding that "customers may incur significant costs in switching broadband providers," the FCC cited factors including:

> early termination fees; the inconvenience of ordering, installation, and set-up, and associated deposits or fees; possible difficulty returning the earlier broadband provider's equipment and the cost of replacing incompatible customer-owned equipment; the risk of temporarily losing service; the risk of problems learning how to use the new service; and the possible loss of a provider-specific e-mail address or Web site.[260]

Thus, assuming that an ISP can satisfy subsection (c)(2)(A), it should not be on the basis that it is susceptible to market forces. Conversely, John Blevins argues that "[c]onsumers who are unhappy with their search engine or social networking site can generally switch products simply with a few keystrokes."[261] Assessing such factors as part of a market forces analysis is the best way to harmonize Congress's policies of "preserv[ing] a . . . competitive free market . . . for the Internet," "maximiz[ing] user control,"[262] and "remov[ing] disincentives for the development and utilization of blocking and filtering technologies . . . ."[263]

VI. CONCLUSION

Section 230 is broad enough to immunize a broad range of intermediaries from liability. While such immunity furthers Congressional objectives of incentivizing the development and utilization of filtering technologies, it can also contravene Congress's objective of maximizing user control. The text of § 230(c)(2) demonstrates how Congress intended for courts to reconcile these competing objectives. The fact that the "good faith" requirement only applies in cases where the provider has restricted access, as opposed to giving users the technical means to do so, indicates that Congress intended the contrast between subsections (c)(2)(A) and (c)(2)(B) to be a trade-off between power and responsibility. When the provider cedes power to users (i.e., by employing filtering technology that maximizes user control), the filtering should be governed under subsection (c)(2)(B), in which event the absence of a "good faith" requirement means the provider should commensurately bear less responsibility to ensure that the filtered material is objectionable. However, when the provider's filtering technology does not exhibit user control, subsection (c)(2)(A) requires that the provider has acted with a good faith belief that its filtering accommodated users' preferences.

259. Preserving the Open Internet, 76 Fed. Reg. 59,192, 59,198 (Sept. 23, 2011).
260. *Id.*
261. Blevins, *supra* note 21, at 392.
262. 47 U.S.C. §§ 230(b)(2), (b)(3) (2012).
263. *Id.* § 230(b)(4).