Online User Account Termination and 47 U.S.C. § 230(c)(2)

By Eric Goldman*

INTRODUCTION

An online provider's termination of user accounts that facilitate user-generated content[1] can be a major—and potentially even life-changing—event for users.[2] Termination of these types of accounts exile the user from a virtual place

* Associate Professor and Director, High Tech Law Institute, Santa Clara University School of Law. E-mail: egoldman@gmail.com. Website: http://www.ericgoldman.org. This paper was prepared in connection with the "Governing the Magic Circle: Regulation of Virtual Worlds" symposium at the UC Irvine Center for Computer Games and Virtual Worlds, April 2011. I appreciate comments from the symposium participants and Ethan Ackerman, Venkat Balasubramani, James Grimmelmann, Nancy Kim, and John Ottaviani on earlier drafts.

1. This Essay addresses only online accounts that enable user-generated content. It does not address Internet access termination, which has brewed substantial discussion about the human rights implications of such terminations. *See, e.g.*, FRANK LA RUE, REPORT OF THE SPECIAL RAPPORTEUR ON THE PROMOTION AND PROTECTION OF THE RIGHT TO FREEDOM OF OPINION AND EXPRESSION (2011), *available at* http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. It also does not address accounts enabling users to transact with an online vendor.

2. *See generally* ERICA NEWLAND ET AL., ACCOUNT DEACTIVATION AND CONTENT REMOVAL (2011), *available at* http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final

where the user wants to be, disrupts any social network relationship ties in that venue, and prevents the user from sending or receiving messages there. The user loses any virtual assets in the account, which could include anything from archived e-mails to accumulated game assets. The effects of account termination are especially acute in virtual worlds[3] where dedicated users may spend a majority of their waking hours or accumulate substantial in-game wealth. However, the problem arises in all online environments (including e-mail, social networking, and web hosting) where account termination disrupts investments made by users.[4]

Because of the potentially significant consequences of online user account termination, user-rights scholars and advocates, especially in the virtual world context, have sought legal restrictions on online providers' discretion to terminate users.[5] However, these efforts are largely misdirected because of 47 U.S.C. § 230(c)(2), which grants federal statutory immunity to online providers. This Essay explains § 230(c)(2)'s role in immunizing online providers' decisions to terminate user accounts. It also explains why this immunity is sound policy.

AN INTRODUCTION TO § 230(C)(2)

Congress enacted § 230 in 1996 as part of the Communications Decency Act (CDA),[6] itself part of the Telecommunications Act of 1996.[7] Section 230 contains two immunities for qualifying service providers.

Section 230(c)(1) generally immunizes websites and other online actors from liability for third party content or actions,[8] subject to three statutory exclusions.[9]

Section 230(c)(2) immunizes certain activities related to online content filtering. Section 230(c)(2)(A) generally immunizes websites from liability for their decisions to filter content. Section 230(c)(2)(B) generally immunizes an enterprise that provides filtering instructions to others, such as publication of a list of e-mail addresses or websites that should be blocked (a "blocklist").[10] Compared to § 230(c)(1), § 230(c)(2) is litigated much less frequently.[11]

_Report_on_Account_Deactivation_and_Content_Removal.pdf, (trying to ameliorate possible human rights consequences of unmeritorious account terminations).

3. Eric Goldman, *Termination of Accounts in Virtual Worlds*, TECH. & MARKETING L. BLOG (Feb. 13, 2005), http://blog.ericgoldman.org/archives/2005/02/termination_of.htm.

4. For simplicity, this Essay focuses on account termination, but generally applies to lesser disruptions of the user's account, such as account suspension, functionality restrictions, or deprivations of specific virtual assets.

5. *See, e.g.*, Jack M. Balkin, *Virtual Liberty: Freedom to Design and Freedom to Play in Virtual Worlds*, 90 VA. L. REV. 2043 (2004); Joshua Fairfield, *The God Paradox*, 89 B.U. L. REV. 1017 (2009).

6. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 56. Section 230 was § 509 of that Act.

7. *Id.*

8. *See* Eric Goldman, *Unregulating Online Harassment*, 87 DENV. U. L. REV. 59 (2010).

9. The exclusions are intellectual property claims, federal criminal prosecutions, and violations of the Electronic Communications Privacy Act or related state laws. 47 U.S.C. § 230(e) (2006).

10. Websites relying on third-party-supplied filtering instructions may be immunized under

This Essay focuses on § 230(c)(2)(A), which reads:

> No provider or user of an interactive computer service shall be held liable on account of 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.

Breaking this clause into components, a successful § 230(c)(2)(A) immunity defense has three elements:

1. *The defendant provides or uses an interactive computer service.* Although the statutory definition of "interactive computer service" is not especially clear,[12] every service available through the Internet should qualify as a provider of an interactive computer service.[13]

2. *The defendant took a voluntary action in good faith.* As discussed below, what qualifies as "good faith" is a contested area in § 230(c)(2) jurisprudence.

3. *That action restricted "objectionable" material.* The statute applies when the material qualifies as one of seven specifically enumerated adjectives or is "otherwise objectionable." As discussed below, whether the statute meant "otherwise objectionable" to be a broad or narrow catchall is another contested area in § 230(c)(2) jurisprudence.

Section 230(c)(2) (including both subparts (A) and (B)) is subject to three statutory exclusions: federal criminal prosecutions, intellectual property claims,[14] and claims under the Electronic Communications Privacy Act or analogous state laws.[15] Although § 230(c)(1) cases often explore these exceptions, they are less likely to arise with § 230(c)(2).[16] Therefore, this Essay does not consider the statutory exclusions further.

---

§ 230(c)(1), § 230(c)(2)(A), or both.

11. 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, 412 n.194 (2010).

12. 47 U.S.C. § 230(f)(2) defines the term as a system "that provides or enables computer access by multiple users to a computer server," not exactly a logical description of websites.

13. *See, e.g.*, Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 521 F.3d 1157, 1162 n.6 (9th Cir. 2008) ("Today, the most common interactive computer services are websites."); Universal Comm. Sys. v. Lycos, Inc., 478 F.3d 413, 419 (1st Cir. 2007) ("[W]eb site operators, such as Lycos, are providers of interactive computer services within the meaning of Section 230."); *see also* IAN C. BALLON, E-COMMERCE AND INTERNET LAW: TREATISE WITH FORMS § 37.05[2] (2d ed. 2009) ("[A]lmost any networked computer would qualify as an interactive computer service . . . ."); Dylan M. Spaduzzi, Note, *Publicity Enemy Number One: Federal Immunity for a Virtual World*, 40 U. MEM. L. REV. 603, 629 (2010) (arguing that Second Life qualifies as a provider of an interactive computer service).

14. In the Ninth Circuit, only federal IP claims are excluded from § 230's immunity; state IP claims are preempted. *See* Perfect 10, Inc. v. CCBill LLC, 488 F.3d 1102 (9th Cir. 2007).

15. 47 U.S.C. § 230(e) (2006).

16. For example, it is difficult, if not impossible, to conceive of how an account termination could lead to an IP claim by the user against the online provider. *See* Williams v. Life's Rad, No. C-10-

Section 230(c)(2)(A) does not expressly reference third-party content—in contrast to § 230(c)(1), which immunizes only "information provided by another information content provider." Therefore, § 230(c)(2)(A) does not seek to protect service providers solely from liability for third-party content. Instead, the provision immunizes "first party" filtering decisions; that is, a service provider's self-made editorial decisions to screen out content it deems objectionable.[17] In this sense, as one leading commentator has described, § 230(c)(2)(A) "inverts the common law rules on distributor and publisher liability by immunizing conduct undertaken to monitor or screen content."[18]

Numerous cases reinforce that § 230(c)(2)(A) protects an online provider's content-screening and related editorial decisions.[19] For example, in *Green v. America Online* the Third Circuit immunized AOL from liability for a virus that a user released in an AOL chatroom.[20] The circuit court upheld § 230(c)(2) from a First Amendment challenge, saying, "Section 230(c)(2) does not require AOL to restrict speech; rather it allows AOL to establish standards of decency without risking liability for doing so."[21] In *Langdon v. Google*, the plaintiff sued several search engines for not accepting his paid ads.[22] In upholding the search engines' § 230(c)(2) defense, the court said, "Section 230 provides Google, Yahoo, and Microsoft immunity for their editorial decisions regarding screening and deletion from their network."[23] And *e360Insight, LLC v. Comcast Corp.* involved Comcast's decision (acting as an e-mail service provider) to block e360's incoming e-mails because Comcast determined they were spam.[24] The court immunized Comcast's blocking decision, noting that § 230(c)(2) "does provide fairly absolute protection to those who choose to block . . . [and] a mistaken choice to block, if made in good faith, cannot be the basis for liability under federal or state law."[25] However,

---

0086 SBA, 2010 WL 5481762, at *4 (N.D. Cal. May 11, 2010) ("Plaintiff has not identified (nor has the Court been able to identify) any provision of the Lanham Act that restricts an Internet service provider's discretion to remove items from its website as a result of any third party claim of trademark infringement."). Further, § 230(c)(2) applies to terminations based on the online provider's receipt of third-party IP infringement complaints about the user's activity; in those circumstances, the user would not be advancing an IP claim against the online provider. However, in situations involving private messaging, the Electronic Communications Privacy Act exclusion can apply. *See, e.g.*, Holomaxx Techs. Corp. v. Yahoo!, Inc., No. 10-cv-04926 JF (PSG), 2011 WL 3740827 (N.D. Cal. Aug. 23, 2011); Holomaxx Techs. Corp. v. Microsoft Corp., No. 10-cv-04924 JF (HRL), 2011 WL 3740813 (N.D. Cal. Aug. 23, 2011); *see also* Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

17. Judge Easterbrook's opinion in *GTE Corp.*, 347 F.3d at 659–60, offers some alternative readings of § 230(c)(2) in dictum, but his musings have not found much traction among other judges.

18. BALLON, *supra* note 13, § 37.05[1][A].

19. As discussed below, § 230(c)(1) may also apply to some or all of these circumstances.

20. Green v. Am. Online, 318 F.3d 465 (3d Cir. 2003).

21. *Id.* at 472.

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

23. *Id.* at 631.

24. e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008).

25. *Id.* at 609.

as discussed in a moment, not all courts have read § 230(c)(2) as broadly as in these cases.

SECTION 230(C)(2) AND ACCOUNT TERMINATION

The prior Section sketched the potential breadth of immunity Congress granted online providers for their filtering decisions. This Section applies those principles to online account terminations. It argues that § 230(c)(2) provides a statutory immunity against most legal challenges by terminated users. It then looks at various ways that users try to get around § 230(c)(2)'s immunity.

Section 230(c)(2)'s Prima Facie Application to Account Terminations

As an application of the general principle that § 230(c)(2) immunizes filtering decisions, the statute presumptively immunizes an online provider's termination of user accounts. The specific language of § 230(c)(2) protects decisions to restrict access to "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" material. Where the user has done something obscene, lewd, lascivious, filthy, excessively violent or harassing, § 230(c)(2) clearly immunizes account termination as a method to prevent the user from continuing those activities. If the "otherwise objectionable" catchall is read broadly, the online provider can say it objected to the user's behavior—even if that behavior does not fit within one of the other statutory categories—and its termination of the user account should be immunized. But unless the online provider is terminating a specific user for the user's failure to pay, or offline activity, or the online provider has a technological glitch, account terminations by the online provider invariably will be based on some objection to the user's onsite activity or content.[26] As a result, § 230(c)(2) should presumptively immunize almost every user account termination.

Section 230 preempts all other federal and state legislation and common law (excluding the three statutorily enumerated exclusions).[27] Thus, unless a disgruntled terminated user can fit within one of those exclusions, § 230(c)(2) should effectively end most of the discussion about the online provider's liability for the termination.

The Role of § 230(c)(1)

This Essay principally focuses on § 230(c)(2)'s preemptive effect, but § 230(c)(1) can immunize account terminations in numerous circumstances as well. First, courts have a difficult time distinguishing between § 230(c)(1) and

26. BALLON, *supra* note 13, § 37.05[4][A] ("[T]he nature of networked computers is such that *conduct* that occurs online frequently is manifested in the form of *content*.").

27. *See, e.g.*, 47 U.S.C. § 230(e)(3) ("No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.").

§ 230(c)(2), so some opinions citing to § 230 generally, or § 230(c)(1) specifically, may have meant to cite § 230(c)(2). As Internet law expert Ian Ballon notes, "In ruling on CDA defenses, some courts have conflated subparts (c)(1) and (c)(2)(A) or simply cited § 230(c) without specifically explaining the basis for a decision or the interrelationship between the subparts."[28] Second, § 230(c)(1) applies (in addition to § 230(c)(2)) when the online operator filters third-party content that triggers the plaintiff's claim. Third, to the extent that the account termination is effectuated by a third party—such as where the online provider relies on a third-party filtering report—then § 230(c)(1) should apply as well.[29] Fourth, courts could treat the user's own content as the "third party" content that triggers § 230(c)(1)'s immunity for account termination. As one court said, "Given that both claims for negligence are based on the deletion of Plaintiff's profiles, a decision by MySpace to effectively 'remove content' created by Plaintiff from its website, MySpace's actions are immune from liability under § 230(c)(1) of the CDA."[30]

Workaround: The Constitution and State Action

Where they conflict, the U.S. Constitution will trump § 230(c)(2)'s statutory immunity and any other legal doctrines giving managerial discretion to online providers. Thus, some user advocates have asserted that online providers are state actors and are therefore subject to constitutional restrictions such as the First Amendment.[31]

These constitutional arguments have gone nowhere in the courts. A standard commercial online provider is clearly not a state actor under any of the prevailing tests.[32] As a result, although in theory the Constitution could trump § 230(c)(2), in practice the constitutional considerations are irrelevant for commercial online providers.[33]

---

28. BALLON, *supra* note 13, § 37.05[1][C].

29. *See, e.g.*, Optinrealbig.com, LLC v. Ironport Sys., Inc., 323 F. Supp. 2d 1037 (N.D. Cal. 2004).

30. Riggs v. MySpace, Inc., 2:09-cv-03073-GHK-CT (C.D. Cal. Sept. 17, 2009), *rev'd on other grounds*, 444 F. App'x. 986 (9th Cir. 2011) (affirming the § 230(c)(1) dismissal).

31. *See, e.g.*, Fairfield, *supra* note 5, at 1058–62; Peter S. Jenkins, *The Virtual World as Company Town—Freedom of Speech in Massively Multiple On-Line Role Playing Games*, 8 J. INTERNET L. 1, 17 (July 2004).

32. *See* Buza v. Yahoo!, Inc., No. C 11-4422 RS, 2011 WL 5041174, at *1 (N.D. Cal. Oct. 24, 2011) (finding that Yahoo!'s GeoCities is not a state actor); Kamango v. Facebook, No. 3:11-CV-0435 (GTS/ATB), 2011 WL 1899277, at *2 (N.D.N.Y. May 19, 2011) (finding that Facebook is not a state actor); Young v. Facebook, No. 5:10-cv-03579-JF/PVT, 2010 WL 4269304, at *3 (N.D. Cal. Oct. 25, 2010) (same); Estavillo v. Sony Computer Entm't Am., No. C-09-03007 RMW, 2009 WL 3072887, at *2 (N.D. Cal. Sept. 2, 2009) (finding that Sony's PS3 online network is not a state actor); *see also* Jayne v. Google Internet Search Engine Founders, No. 07-4083, 263 F. App'x 268 (3rd Cir. Feb. 7, 2008); KinderStart v. Google, No. C 06-2057 JF (RS), 2006 WL 3246596, at *4 (N.D. Cal. July 13, 2006) (dismissing plaintiff's First Amendment claims because Google is not a state actor).

33. *Compare* White Buffalo Ventures, LLC v. Univ. of Tex. at Austin, 420 F.3d 366 (5th Cir.

Workaround: The Statutory References to "Good Faith" and "Otherwise Objectionable"

Plaintiffs can attack a § 230(c)(2) immunity claim by challenging the online provider's reason for terminating a user, either because the online provider did not terminate in good faith or because the provider's reason falls outside the statute.

As far as I know, no online provider has lost § 230(c)(2) immunity because it did not make a good faith filtering decision. Nevertheless, a few cases have given examples of some provider actions that may not be in good faith. For example, anticompetitive motivations might disqualify an online provider from § 230(c)(2). In *Zango v. Kaspersky*, Ninth Circuit Judge Fisher wrote the following in his concurring opinion:

> [U]nder the generous coverage of § 230(c)(2)(B)'s immunity language, a blocking software provider might abuse that immunity to block content for anticompetitive purposes or merely at its malicious whim, under the cover of considering such material "otherwise objectionable."
>
> . . . Unless § 230(c)(2)(B) imposes some good faith limitation on what a blocking software provider can consider "otherwise objectionable," or some requirement that blocking be consistent with user choice, immunity might stretch to cover conduct Congress very likely did not intend to immunize.[34]

In *Smith v. Trusted Universal Standards in Electronic Transactions*, the judge found that an online provider's failure to articulate a reason for its blocking decision could be bad faith:

> [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 e-mail . . . the Court is not convinced that an internet service provider acts in good faith when it simply ignores a subscriber's request for information concerning an allegedly improper e-mail blockage . . . there is no reason why Comcast could not articulate its immunity (or provide another rationale for the blockage) when asked to do so by a paying customer.[35]

As these examples illustrate, the statute's "good faith" reference invites judges to introduce their own normative values into the consideration.[36] This may be the inevitable consequence of any good faith legal element.[37]

2005) (holding that state action applies to e-mail services offered by a public university), *with* Kathleen R. v. City of Livermore, 104 Cal. Rptr. 2d 772 (Ct. App. 2001) (holding that a public library offering Internet access to its patrons was eligible for § 230).

34. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009) (Fisher, J., concurring); *see also* BFS Fin. v. My Triggers Co., No. 09CV-14836 (Franklin Cnty. Ct. Com. Pl. Aug. 31, 2011) (refusing to apply § 230(c)(2) to an antitrust claim).

35. Smith v. Trusted Universal Standards in Elec. Transactions, No. 09-4567 (RBK/KMW), 2011 WL 900096, at *25–26 (D.N.J. Mar. 15, 2011).

36. *See, e.g.*, Mail Abuse Prevention Sys. LLC v. Black Ice Software, Inc., No. CV 788630, 2000 WL 34016435, at *9 (Cal. Super. Ct. Oct. 13, 2000) (labeling of defendant's errors as not in good

Fortunately, most judges do not introduce their own normative values into the statutory inquiry. Several § 230(c)(2) cases have held that good faith is determined subjectively, not objectively.[38] In that circumstance, courts should accept any justification for account termination proffered by the online provider, even if that justification is ultimately pretextual.[39] Furthermore, if plaintiffs have the obligation to show subjective bad faith, they are unlikely to do so. They would need to find convincing evidence of bad faith,[40] an unlikely situation in most cases.

Even if good faith is interpreted subjectively, defendants may not be enthusiastic about the good faith statutory reference. Deferential courts may refuse to grant § 230(c)(2) immunity on a motion to dismiss if the plaintiff alleges a lack of good faith,[41] which gives plaintiffs the chance to hunt for evidence and imposes additional advocacy and discovery costs on the defendant.

As Judge Fisher's concurrence in the *Zango* case indicates, judges may interpret the "good faith" and "otherwise objectionable" language in conjunction with each other. Alternatively, even if a provider makes a filtering judgment in good faith, the filtered content may not be covered by the statutorily enumerated justifications. This requires courts to resolve the breadth of the "otherwise

---

faith, without further explanation).

37. A similar problem with "good faith" arises in contract interpretation cases, including limits on a contracting party's termination rights. In the online context see, for example, *Young v. Facebook, Inc.*, No. 5:10-cv-03579-JF/PVT, 2010 WL 4269304, at *4 (N.D. Cal. Oct. 25, 2010) ("It is at least conceivable that arbitrary or bad faith termination of user accounts, or even termination of user accounts with no explanation at all, could implicate the implied covenant of good faith and fair dealing."); *Cranford v. Consumer Depot, Inc.*, No. 05C-3242 (Tenn. Ct. App. Dec. 8, 2009) (holding that eBay's contractual right to terminate users for threatening site integrity was definite enough to survive the plaintiffs' claim that the termination provision enabled eBay to make arbitrary terminations if the court read a good faith reasonableness requirement into the provision).

38. *See, e.g.*, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009); e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605 (N.D. Ill. 2008). *But see* Nat'l Numismatic Certification, LLC. v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404 (M.D. Fla. July 8, 2008).

39. *Cf.* Donato v. Moldow, 865 A.2d 711, 727 (N.J. Super. Ct. App. Div. 2005) ("If the conduct falls within the scope of the traditional publisher's functions, it cannot constitute, within the context of § 230(c)(2)(A), bad faith. . . . To raise an issue of an absence of good faith, an allegation of conduct outside the scope of the traditional publisher's function would be required.").

40. *But see* Sabbato v. Hardy, No. 2000CA00136, 2000 WL 33594542, at *3 (Ohio Ct. App. Dec. 18, 2000) (effectively putting the burden on the defense to show evidence of good faith: "the 'good faith' language presupposes some evidence of that 'good faith'").

41. *Nat'l Numismatic Certification*, 2008 WL 2704404; *Sabbato*, 2000 WL 33594542; *see also* BALLON, *supra* note 13, § 37.05[7] ("Where a claim of immunity is based on subpart 230(c)(2)(A), it may be more difficult to establish entitlement short of summary judgment because, unlike § 230(c)(1) which is self-executing, subpart 230(c)(2)(A) requires a showing of voluntary action undertaken in good faith to benefit from the exemption.") (footnotes omitted); *see also* Levitt v. Yelp! Inc., Nos. C-10-1321 EMC, C-10-2351 EMC, 2011 WL 5079526, at *7 (N.D Cal. Oct. 26, 2011) (acknowledging that plaintiffs cannot plead provider scienter to get around § 230(c)(1) because only § 230(c)(2) relies on provider good faith).

objectionable" reference in the statute, and courts have reached different interpretations.

The statutory construction principle of *ejusdem generis* indicates that catchall words should be interpreted by the company they keep.[42] Under that principle, "otherwise objectionable" material should relate to pornographic, violent, or harassing content.[43] Any other basis for an online provider's account termination, even if reasonable, would drop out of § 230(c)(2)'s statutory immunity.[44]

On the other hand, courts have generally read the statute more broadly, treating the "otherwise objectionable" language as merely requiring that the online provider deems the filtered content "objectionable."[45] Given that Congress chose a very general catchall word ("objectionable") and did not limit or qualify the word in any way, this is a defensible statutory reading. Alternatively, even if courts read the catchall narrowly, they could reach the same basic outcome by expansively interpreting what constitutes "harassing" behavior.

If judges read "objectionable" as a general catchall and measure "good faith" subjectively, then the statute immunizes any online provider's efforts to restrict materials that it subjectively believes are objectionable. Thus, if an online provider subjectively feels that a user is degrading its environment in any way, § 230(c)(2) appears to protect the online provider from liability for terminating that user.

This still leaves open the question of whether an online provider could terminate a user for provably capricious or even malicious reasons and still claim § 230(c)(2) immunity. In this situation, judges should find that the online provider lacked the requisite subjective good faith. However, if an online provider can offer a plausible excuse (even if pretextual) for its actions, § 230(c)(2) immunity could still be available.

Workaround: Provider Promises

Promise-based theories are another potential workaround to § 230. This argument applies when online providers, whose discretion is otherwise immunized

---

42. *See, e.g.*, Hall St. Assocs., L.L.C. v. Mattel, Inc., 552 U.S. 576, 586 (2008) ("Under [the *ejusdem generis*] rule, 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.").

43. *See, e.g.*, *Nat'l Numismatic Certification*, 2008 WL 2704404, at *25 ("'[O]bjectionable' content must, at a minimum, involve or be similar to pornography, graphic violence, obscenity, or harassment."); BFS Fin. v. My Triggers Co., No. 09CV-14836 (Franklin Cnty. Ct. Com. Pl., Aug. 31, 2011).

44. As another example, see *Goddard v. Google, Inc.*, No. C 08-2738 JF (PVT), 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008), which (citing the *National Numismatic* case) rejected § 230(c)(2) immunity for an advertising network's disclosure requirements for advertisers, which the court said "relate to business norms of fair play and transparency and are beyond the scope of § 230(c)(2)."

45. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009); Langdon v. Google, Inc., 474 F. Supp. 2d 622 (D. Del. 2007); Pallorium, Inc. v. Jared, No. G036124, 2007 WL 80955 (Cal. Ct. App. Jan. 11, 2007).

by § 230(c)(2), make promises to users that conflict with or apparently waive their discretion. Those promises could come from marketing representations, contract provisions, and non-contract promises (such as individualized responses to specific user inquiries). When an online provider fails to honor its promises, users may have claims under false advertising, fraud, breach of contract, promissory estoppel, and other doctrines.[46]

With respect to account termination, user agreements often specify that the online provider, in its sole discretion, can terminate the user (a "termination-for-convenience" clause).[47] Courts typically honor termination-for-convenience clauses on their face. Because termination-for-convenience clauses are so legally powerful, many cases involving user account terminations never reach § 230(c)(2) defenses; the court resolves the dispute on the contract.[48]

Nevertheless, an online provider can void the user agreement's termination-for-convenience clause by making inconsistent promises elsewhere. The remainder of this Section assumes that the online provider either did not include a termination-for-convenience clause in its user agreement (an unlikely scenario) or has made inconsistent promises elsewhere.

In this narrowed situation, it may seem odd to even consider that § 230(c)(2) plays any role. Of course an online provider should stand behind the promises it voluntarily makes; why would § 230 disrupt that? Shouldn't online providers be allowed to opt for a more user-friendly regime than the immunity provides?[49] As a recent case said, "Claims of misrepresentation, false advertising, or other causes of action based . . . on [Yelp's] representations regarding such conduct, would not be immunized under § [230(a)(1)]."[50]

Yet, as surprising as it may be, the legislative background suggests that § 230 can trump online providers' voluntarily made promises in some circumstances. Section 230 was enacted as a response to *Stratton Oakmont v. Prodigy*, where a user allegedly defamed the plaintiff on a Prodigy message board.[51] The court imposed liability on Prodigy, in part because Prodigy advertised that it provided a family-friendly service. In effect, in *Stratton Oakmont* the plaintiff asserted that an online

46. For examples of such lawsuits, see *Bragg v. Linden Research, Inc.*, 487 F. Supp. 2d 593 (E.D. Pa. 2007), and *Evans v. Linden Research, Inc.*, No. 10-cv-01679 (E.D. Pa. Feb. 3, 2011). In both cases, Second Life "took back" land that users had purchased in-game, and the users argued that the land should be treated as real property due to Linden's marketing representations.

47. *See* Andrew Jankowich, *EULAw: The Complex Web of Corporate Rule-Making in Virtual Worlds*, 8 TUL. J. TECH. & INTELL. PROP. 1 (2006).

48. *Cf.* Mehmet v. Add2Net, Inc., 886 N.Y.S.2d 397 (App. Div. 2009) (dismissing a lawsuit against a web host for terminating a user based on a contract restriction against abusing the web host's customer support representatives).

49. *Cf.* Andrew E. Jankowich, *Property and Democracy in Virtual Worlds*, 11 B.U. J. SCI. & TECH. L. 173 (2005) (discussing why a virtual world provider might want to voluntarily restrict its discretion).

50. Levitt v. Yelp! Inc., Nos. C-10-1321 EMC, C-10-2351 EMC, 2011 WL 5079526, at *9 (N.D Cal. Oct. 26, 2011) (dicta).

51. Stratton Oakmont v. Prodigy, No. 031063/94, 1995 WL 323710 (N.Y. 1995).

provider's marketing representations should increase the online provider's liability for user-supplied content. By overturning *Stratton Oakmont*, arguably Congress sought to prevent plaintiffs from doing that.[52]

Indeed, some cases have interpreted § 230(c)(1) as preempting claims against online providers for their first-party marketing representations. For example, in *Milo v. Martin*, a website's marketing collateral claimed that the website "contains facts believed to be totally accurate by sources with character and truthfulness as their primary attributes."[53] The plaintiffs argued that the site, in fact, contained false statements posted by third parties. The court held that, despite the falsity of its marketing collateral, the website was immunized by § 230(c)(1).[54]

In another case, *Mazur v. eBay*, eBay promoted its live bidding service, which eBay outsourced to third-party auction houses, using allegedly false marketing representations.[55] Section 230(c)(1) immunized eBay's representation that it screened the third-party auction houses because screening is an editorial function protected by § 230. However, § 230(c)(1) did not immunize eBay's claims that live bidding is "safe," is conducted against "floor bidders," and involves "international" auction houses.

In contrast, *Barnes v. Yahoo!, Inc.* held that promissory estoppel could serve as a § 230 workaround when the online provider made a user-specific promise, even though § 230(c)(1) preempted related claims such as negligent failure to remove.[56] As a practical matter, online providers try to avoid making definitive promises to individual users,[57] so the promissory estoppel workaround may arise infrequently.

As the *Barnes* holding and the split ruling in *Mazur* indicate, courts may be reluctant to apply § 230 to an online provider's promises, especially if they can

52. H.R. Rep. No. 104-458, at 194 (1996) ("One of the specific purposes of [§ 230] 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.").

53. Milo v. Martin, 311 S.W.3d 210, 216 (Tex. Ct. App. 2010).

54. *Id.* Another case in this genre is *Hopkins v. Doe #1*, No. 2:11-CV-100-RWS, 2011 WL 5921446 (N.D. Ga. Nov. 28, 2011), which applied § 230 to a fraud claim based on the website's announced policies.

55. Mazur v. eBay Inc., No. C 07-03967 MHP, 2008 WL 618988 (N.D. Cal. 2008).

56. Barnes v. Yahoo!, Inc., 570 F.3d 1096 (9th Cir. 2009); *see also* Scott P. v. Craigslist, Inc., No. CGC-10-496687 (Cal. Super. Ct. June 2, 2010), *available at* http://www.sfsuperiorcourt.org/online-services (follow "Case Number Query" hyperlink for civil cases; enter "CGC10496687" into case number field; open docket item dated July 6, 2010, titled "ORDER SUSTAINING IN PART AND OVERRULING IN PART CRAIGSLIST, INC'S DEMURRER") (finding a promissory estoppel workaround to § 230). In addition to *Barnes*, see, for example, *Murawski v. Pataki*, 514 F. Supp. 2d 577, 591 (S.D.N.Y. 2007), and *Schneider v. Amazon.com, Inc.*, 31 P.3d 37 (Wash. Ct. App. 2001).

57. Eric Goldman, *47 USC 230 Retrospective Conference Recap*, TECH. & MARKETING L. BLOG (Mar. 21, 2011), http://blog.ericgoldman.org/archives/2011/03/47_usc_230_retr.htm.

resolve the case on alternative grounds.[58] Nevertheless, because such an immunity is possible, plaintiffs cannot simply bypass § 230(c)(2) by invoking the online provider's marketing copy or user agreement in the complaint.

Implications

This Section has posited that § 230(c)(2) provides online providers with a robust immunity for their decisions to filter objectionable online content or activities. Applying that argument, § 230(c)(2) wipes out most user claims against online providers for account termination because the online provider can argue that the termination was intended to shut down the user's objectionable content or activity.

In this situation, terminated users have limited ways to bypass § 230(c)(2) immunity. Users can argue that the online provider is a state actor, but that is doomed to fail against commercial providers. Alternatively, users can argue that the online provider did not exercise "good faith" in the termination, or that the provider's termination grounds did not satisfy the requirements of blocking "objectionable" material, but plaintiffs have not fared well with those arguments. Finally, users can argue that the online provider made a promise inconsistent with the termination agreement. Section 230(c)(2) may nevertheless preempt that argument; even if it does not, those arguments may fail on other doctrinal grounds.

Because it preempts so many claims and is subject to limited workarounds, § 230(c)(2) plays an essential role in any discussion about user protections against account termination. The next Section will explain why the flexibility that § 230(c)(2) gives to online providers is good policy.

WHY A BROAD § 230(C)(2) IMMUNITY IS GOOD POLICY

Every online community needs governance. In some communities, the online provider encourages users to self-organize, in which case the provider tries to minimize its intervention. Even in that case, the online provider sets the initial rules and retains the technical capacity (and usually the legal capacity) to terminate accounts. In other communities, online providers take an active role (sometimes, extremely active) in policing the community's interactions.

Online user communities inevitably require at least some provider intervention. At times, users need "protection" from other users. The provider can give users self-help tools to reduce their reliance on the online provider's

58. *See, e.g.*, Goddard v. Google, Inc., 640 F. Supp. 2d 1193 (N.D. Cal. 2009) (rejecting plaintiffs' assertion that the online provider had even made a promise to them; or that the plaintiffs could be third-party beneficiaries of any promises made). A number of other cases make similar doctrinal moves, such as *Noah v. AOL Time Warner, Inc.*, 261 F. Supp. 2d 532 (E.D. Va. 2003) and *Green v. America Online*, 318 F.3d 465 (3d Cir. 2003).

intervention, but technological tools cannot ameliorate all community-damaging conduct by determined users. Eventually, the online provider needs to curb a rogue user's behavior to protect the rest of the community. Alternatively, a provider may need to respond to users who are jeopardizing the site's security or technical infrastructure. Depending on the problem's severity and its effects on other users, that response could require banishment from the community.

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. In theory, online providers can partially achieve the same legal outcome through their user agreements, but contract risk mitigation is often messier than statutory immunity. When online providers raise contract defenses, the plaintiffs can attack the providers by disputing contract formation and interpretation. Additionally, plaintiffs often try to bypass contracts by asserting a long laundry list of ancillary and overlapping non-contract claims such as false advertising, fraud, unfair practices, unjust enrichment, and many others. Because online providers rarely defend only against a simple breach of contract claim, it takes substantial time and money on everyone's part to work through the litigation's complexity. In contrast, a robust statutory immunity lets courts adjudicate cases quickly and at low cost to the litigants and the judicial system.[59]

For this reason, courts should be skeptical of all plaintiffs' attempts to work around § 230 immunity.[60] When judges reject a defendant's motion to dismiss based on immunity and then reject the plaintiff's claim at a later procedural stage, they risk undercutting the immunity's principal benefit of fast, cheap, and reliable defense wins.[61] To improve the immunity's efficacy, Congress should consider deleting the "good faith" reference in the statute. It invites judicial confusion and increases the chances that both parties will incur more adjudication costs only to reach the same result: a prevailing defendant.

---

59. Eric Goldman, *Unregulating Online Harassment*, 87 DENV. U. L. REV. 59 (2010).

60. *Cf.* Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008) ("Such close cases, we believe, must be resolved in favor of immunity, lest we cut the heart out of section 230 by forcing websites to face death by ten thousand duck-bites . . . ."); Levitt v. Yelp! Inc., Nos. C-10-1321 EMC, C-10-2351 EMC, 2011 WL 5079526, at *8 (N.D. Cal. Oct. 26, 2011) ("[T]he need to defend against a proliferation of lawsuits, regardless of whether the provider ultimately prevails, undermines the purpose of section 230.").

61. In fact, a few recent rulings found § 230 immunity after rejecting it at the motion to dismiss stage—thus causing the litigants to spend substantial time and money wrangling with each other just to reach the same result. *See, e.g.*, Kruska v. Perverted Justice Found. Inc., No. CV-08-00054-PHX-SMM, 2011 WL 1260224 (D. Ariz. Apr. 15, 2011); Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2011 WL 900096 (D.N.J. Mar. 15, 2011); *see also* Eric Goldman, *Review Website Should Get 47 USC 230 Dismissal but Judge Keeps Case Open in "Abundance of Caution"—Frontier Van Lines v. MoverReviews.com*, TECH. & MARKETING L. BLOG (May 27, 2011), http://blog.ericgoldman.org/archives/2011/05/review_website.htm.

Although § 230(c)(2)'s immunity superficially seems to confer too much power to online providers, in fact, online providers have substantial incentives to exercise this power wisely.

First, commercial online providers terminate customers reluctantly because users generate economic value for the provider. Of course, that economic value must be balanced against the foregone economic value of other users inhibited by the rogue user, so an economic evaluation leaves niche subgroups in the community at a greater risk of termination (warranted or not). Nevertheless, major conflicts between a site's subcommunities are a key circumstance where an online provider may need to intercede.

Second, an online provider needs to retain its users' trust. Capricious termination of user accounts undermines the remaining users' trust.[62] This can sour the provider's relationship with the remaining users, prompting them to seek out replacement venues that provide the desired level of trust, or reducing their motivation to invest in the community.[63] Further, to the extent that prospective new users learn about a site's reputation for untrustworthiness, they will be driven toward alternatives.

Thus, marketplace incentives work unexpectedly well to discipline online providers from capriciously wielding their termination power.[64] This is true even if many users face substantial nonrecoupable or switching costs, both financially and in terms of their social networks. Some users, both existing and prospective, can be swayed by the online provider's capriciousness—and by the provider's willingness to oust problem users who are disrupting the community. The online provider's desire to keep these swayable users often can provide enough financial incentives for the online provider to make good choices.

Thus, broadly conceived, § 230(c)(2) removes legal regulation of an online provider's account termination, making the marketplace the main governance mechanism over an online provider's choices. Fortunately, the marketplace is effective enough to discipline those choices.

CONCLUSION

Due to the consequences of a user's account termination, the legal rules governing such terminations garner substantial attention. Section 230(c)(2) plays a crucial—and often dispositive—role in that conversation about these legal rules.

---

62. Even if a user's termination is not a public event in the sense that other users can easily observe the termination, the terminated user has many other ways of spreading the news publicly.

63. Eric Goldman, *Speech Showdowns at the Virtual Corral*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 845 (2005); Salil K. Mehra, *Paradise Is a Walled Garden? Trust, Antitrust, and User Dynamism*, 18 GEO. MASON L. REV. 889, 909–13 (2011).

64. Eric Goldman, *AOIR Regulating Virtual Worlds Panel, and My Notes on Investment Expectations in Virtual Worlds*, TECH. & MARKETING L. BLOG (Oct. 22, 2007), http://blog.ericgoldman.org/archives/2007/10/aoir_regulating.htm.

User-rights advocates may resist § 230(c)(2)'s broad immunity, but its breadth may be justified. Online providers need the discretion to manage their communities, and the marketplace provides adequate discipline for those managerial decisions.