Oklahoma Law Review

Volume 74 | Number 3

2022

Software v. Software: How Section 230 of the Communications Decency Act Threatens to Undermine Antitrust Law

Bailey S. Barnes

Software v. Software: How Section 230 of the Communications Decency Act Threatens to Undermine Antitrust Law

I. Introduction

Americans are spending an increasing amount of time on their computers.[1] There are myriad benefits to being online, such as an increasingly globalized economy and a slew of educational resources.[2] Many utilize the internet maliciously, however.[3] An online message board known as 8chan has been linked to several mass shootings.[4] Social media sites have been used to coordinate violent riots.[5] Hackers increasingly threaten the security of private data.[6] In late 2020, for example, the U.S.

---

1. *Screen Time Across Several Devices Has Increased for Many Americans During the Covid-19 Pandemic*, IPSOS (July 21, 2020), https://www.ipsos.com/en-us/screen-time-across-several-devices-has-increased-many-americans-during-covid-19-pandemic (noting that 55% of Americans reported spending more time in front of a computer screen since the beginning of the COVID-19 pandemic).

2. *See* Laura Silver et al., *People Say the Internet Brings Economic and Educational Benefits - but Some Are Concerned About the Societal Impact of Social Media*, PEW RSCH. CTR. (Mar. 7, 2019), https://www.pewresearch.org/internet/2019/03/07/people-say-the-internet-brings-economic-and-educational-benefits-but-some-are-concerned-about-the-societal-impact-of-social-media/ (reporting respondents' views on whether the internet has had "a good influence on morality, politics, physical health, local culture, civility and the economy").

3. *See* James Grimmelmann, *Spyware vs. Spyware: Software Conflicts and User Autonomy*, 16 OHIO ST. TECH. L.J. 25, 28–33 (2020) (listing ways software companies have a practice of "doing drive-bys on each other like warring street gangs").

4. Kevin Roose, *'Shut the Site Down,' Says the Creator of 8chan, a Megaphone for Gunmen*, N.Y. TIMES (Aug. 4, 2019), https://www.nytimes.com/2019/08/04/technology/8chan-shooting-manifesto.html ("In recent months, 8chan has become a go-to resource for violent extremists. At least three mass shootings . . . have been announced in advance on the site . . . .").

5. Rebecca Heilweil & Shirin Ghaffary, *How Trump's Internet Built and Broadcast the Capitol Insurrection*, VOX: RECODE (Jan. 8, 2021, 5:00 PM EST), https://www.vox.com/recode/22221285/trump-online-capitol-riot-far-right-parler-twitter-facebook.

6. *See generally* Nicholas Confessore, *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*, N.Y. TIMES (Apr. 4, 2018), https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (reporting pre-election data harvesting of Facebook profiles for millions of American voters); Nick Statt, *Twitter Hack Conspirators May Include a 16-Year-Old from Massachusetts*, VERGE (Sept. 2, 2020, 1:09 PM EDT), https://www.theverge.com/2020/9/2/21418437/twitter-hack-16-year-old-massachusetts-investigation-findings (reporting that in 2020 a teenager hacked into

government discovered an unprecedented cyberattack where hackers infiltrated software used by the federal government, gaining access to over 18,000 government agencies' private data.[7]

While ever-increasing in magnitude, online threats are not new.[8] Malware, a term meaning "bad software," encompasses a variety of different online threats that can compromise a user's personal information.[9] As a result, internet users must take certain steps to protect themselves. In addition to practical security solutions such as two-factor authentication and complex passwords,[10] software companies have developed a range of products to protect users online.[11] Anti-malware software serves to protect users from dangers they might encounter on the internet.[12]

Many modern internet users utilize some sort of anti-malware software to protect their data from online threats.[13] However, section 230 of the Communications Decency Act ("Section 230") grants software providers unfettered discretion to make covert filtering and blocking decisions on behalf of their users.[14] This power enables software providers to filter out

---

prominent Twitter accounts, including those of Elon Musk and Joe Biden, for a bitcoin scam).

7. David E. Sanger & Nicole Perlroth, *Trump Contradicts Pompeo over Russia's Role in Hack*, N.Y. TIMES (Jan. 12, 2021), https://www.nytimes.com/2020/12/19/us/trump-contradicts-pompeo-over-russias-role-in-hack.html.

8. *See Top 10 Most Notorious Cyber Attacks in History*, ARN, https://www.arnnet.com.au/slideshow/341113/top-10-most-notorious-cyber-attacks-history/ (last visited Jan. 4, 2021) (listing major cyber-attacks from as early as 1988).

9. Kevin Purdy & Thorin Klosowski, *You Don't Need to Buy Antivirus Software*, N.Y. TIMES: WIRECUTTER (Apr. 21, 2020), https://www.nytimes.com/wirecutter/blog/best-antivirus/.

10. Catalina Gonella & Noah Friedman, *5 Easy Ways to Protect Yourself from Being Hacked, According to a Former NSA Hacker*, BUS. INSIDER (June 16, 2021, 3:42 PM), https://www.businessinsider.com/nsa-hacker-5-ways-to-protect-yourself-online-2018-7.

11. Carrie Marshall, Brian Turner & Mike Williams, *Best Malware Removal Software 2021: Free and Paid Services*, TECHRADAR (Aug. 11, 2021), https://www.techradar.com/best/best-malware-removal.

12. Purdy & Klosowski, *supra* note 9.

13. *See generally* Sophie Anderson, *Antivirus and Cybersecurity Statistics, Trends, & Facts 2021*, SAFETYDETECTIVES, https://www.safetydetectives.com/blog/antivirus-statistics/ (last visited Oct. 2, 2021).

14. *See* 47 U.S.C. § 230(c)(2)(A) (restricting software providers' liability for "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").

any competitor for any reason.[15] In effect, this framework cripples Section 230's policy to safeguard user control and threatens antitrust law's aim to protect competition.[16]

A primary function of anti-malware software is protecting users from online threats. Thus, in response to the ever-changing world of the internet, anti-malware software is constantly redefining what constitutes a "threat" online.[17] In recent years, however, an aspect of anti-malware software has garnered a negative reputation.[18] By design, anti-malware software is incredibly invasive because "[s]ecurity products are intended to evaluate everything that touches your machine in search of anything malicious, or even vaguely suspicious."[19]

While a primary function of anti-malware software is protecting users from online threats, the software itself has become a threat. For example, because of its invasiveness,[20] anti-malware software can be utilized to spy on its own users.[21] U.S. intelligence agencies have accused Kaspersky Lab ("Kaspersky"), a cybersecurity company offering anti-malware software, of gathering sensitive information from a U.S. national security agent's home computer.[22] Security experts have similarly accused Avast Security, another anti-malware software provider, of spying on its users and selling their data.[23] Nevertheless, anti-malware software remains a necessary component of living in a digital world.[24]

---

15. *See id.*; *see also* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1048 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) (alleging that Malwarebytes filtered out its competitor Enigma "at its own malicious whim"); PC Drivers Headquarters, LP v. Malwarebytes, Inc., No. 1:18-CV-234-RP, 2018 WL 2996897, at *1 (W.D. Tex. Apr. 23, 2018) (alleging that Malwarebytes filtered out PC Drivers despite attempted cooperation between the parties).

16. 47 U.S.C. § 230(b)(3); *see* N. Pac. Ry. Co. v. United States, 356 U.S. 1, 4 (1958).

17. Purdy & Klosowski, *supra* note 9.

18. Nicole Perlroth, *How Antivirus Software Can Be Turned into a Tool for Spying*, N.Y. TIMES (Jan. 1, 2018), https://www.nytimes.com/2018/01/01/technology/kaspersky-lab-antivirus.html.

19. *Id.*

20. *Id.*

21. *Id.* ("It has been a secret, long known to intelligence agencies but rarely to consumers, that security software can be a powerful spy tool.").

22. *Id.*; *see also Online Security for You & Your Family*, AO KASPERSKY LAB, https://usa.kaspersky.com/home-security/v3 (last visited Jan. 4, 2021).

23. Karl Bode, *Should Your Antivirus Software Be Spying on You?*, TECHDIRT (Jan. 30, 2020, 12:33 PM), https://www.techdirt.com/articles/20200127/08001343803/should-your-antivirus-software-be-spying-you.shtml; *see also Avast Online Security and Avast Secure*

Section 230 has provided immunity for some of the disputably "bad" software companies.[25] While Section 230 was originally created to prevent minors from being exposed to obscenities on the internet,[26] Congress's express policy provisions accompanying the statute demonstrated its intent to create a flourishing online world.[27] This Comment focuses on Section 230's express "user control" policy, which "encourage[s] the development of technologies which maximize user control."[28]

To accomplish these goals, Congress provided immunity to software providers when making decisions "in good faith" to limit users' access to material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[29] The inclusion of this provision, known as the "Good Samaritan" provision, presents the issue of whether the phrase "otherwise objectionable" conveys unbridled discretion to companies making decisions as to what their users will and won't see.[30]

In *Enigma Software Group USA, LLC v. Malwarebytes, Inc.*, the Ninth Circuit held that the catchall "otherwise objectionable" was not without

---

Browser Are Spying on You, ALMOST SECURE (Oct. 28, 2019), https://palant.info/2019/10/28/avast-online-security-and-avast-secure-browser-are-spying-on-you/.

24. Perlroth, *supra* note 18 ("In the battle against malicious code, antivirus products are a staple . . . ." (quoting Patrick Wardle, chief research officer at Digita Security)).

25. *See, e.g.*, Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1170 (9th Cir. 2009) (immunizing Kaspersky from potential liability under § 230(c)(2)).

26. *See* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1047 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) ("The history of § 230(c)(2) shows that access to pornography was Congress's motivating concern . . . .").

27. *See* 47 U.S.C. § 230(b)(1)–(5).

28. *Id.* § 230(b)(3).

29. *Id.* § 230(c)(2)(A).

30. *Compare* Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d. 876, 880, 882 (N.D. Cal. 2015) (holding that "otherwise objectionable" did not immunize YouTube after "it removed [a] video after it determined the view count . . . was inflated through automated means, and thus violated its Terms of Service"), *and* Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014) (holding that Yahoo!'s automatic text response system did not qualify for immunity under the Good Samaritan provision because it "did not engage in any form of content analysis of the subject text to identify material that was offensive or harmful prior to the automatic sending of a notification message"), *with* PC Drivers Headquarters, LP v. Malwarebytes, Inc., 371 F. Supp. 3d 652, 660 (N.D. Cal. 2019) (holding that Malwarebytes's software filters qualified for the Good Samaritan immunity even though filtering "ha[d] the secondary effect of depriving PC Drivers of the benefits of page-click advertising" because such filtering provided "the 'technical means' to restrict access to statutorily defined objectionable material").

limit.[31] Instead, the court determined that when a software provider filters out a competitor with anticompetitive animus, it is not afforded immunity under the Good Samaritan provision.[32] This contradicts the broad immunity traditionally provided under the statute, but it might reflect a recent push to narrow the statute's scope.[33] After the Supreme Court denied Malwarebytes's petition for certiorari in October 2020,[34] the Ninth Circuit's holding now represents a leading limitation to the Good Samaritan provision.

Enigma's holding acknowledges that if a software provider can make covert decisions on behalf of its users, Section 230's user control policy provision is undermined.[35] Further, such unfettered discretion creates an avenue for anticompetitive conduct, a force antitrust law seeks to prevent.[36] Ultimately, it is debatable whether Malwarebytes could be liable under antitrust law, and this Comment does not intend to show that it could be. Instead, this Comment aims to show how *Enigma*'s holding highlights the interplay between Section 230 and antitrust law regarding user control, anticompetitive conduct, and the anti-malware software market.[37]

Part II of this Comment discusses caselaw surrounding relevant portions of Section 230. Specifically, it describes lower courts' differing interpretations of when to deviate from the broad immunity traditionally provided by the statute. Part III elaborates on the Ninth Circuit's interpretation of the Good Samaritan provision in *Enigma* and discusses relevant caselaw that influenced the decision. Part IV describes antitrust implications stemming from the Good Samaritan provision and the *Enigma*

31. *Enigma*, 946 F.3d at 1047.

32. *Id.*

33. *See infra* notes 78–79 and accompanying text.

34. Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13 (2020).

35. *Enigma*, 946 F.3d at 1051 ("Immunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy. . . . Users would not reasonably anticipate providers blocking valuable online content in order to stifle competition.").

36. *See generally* Morgan v. Ponder, 892 F.2d 1355, 1358 (8th Cir. 1989) ("Anticompetitive conduct is conduct without legitimate business purpose that makes sense only because it eliminates competition."); Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 605 n.32 (1984) (stating anticompetitive conduct exists where it "impair[s] the opportunities" of competitors or where conduct "does not further competition on the merits or does so in an unnecessarily restrictive way") (quoting 3 PHILLIP E. AREEDA & DONALD F. TURNER, ANTITRUST LAW 78 (1978)).

37. *See infra* Part IV.

holding. Finally, Part V discusses solutions Congress should consider in a potential amendment to the Good Samaritan provision.

This Comment concludes that Section 230 allows software companies to engage in conduct antithetical to the policy behind both Section 230 and antitrust law. Congress should modify the provision in line with the Ninth Circuit's holding in *Enigma*.

II. Section 230 Background

When Congress enacted Section 230 in 1996, global internet users topped out around sixteen million.[38] As of January 2021, it had grown to nearly five billion users.[39] Over this time, access to the internet evolved into a basic human right.[40] Section 230 has been credited as a "catalyst" for the immense growth of the tech industry in the United States.[41]

Section 230 was created as part of Title V of the Telecommunications Act of 1996,[42] which became known as the Communications Decency Act ("CDA").[43] The initial purpose of the CDA was to protect minors from

38. *Internet Growth Statistics*, INTERNET WORLD STATS, https://www.internetworldstats.com/emarketing.htm (July 3, 2021).

39. *Worldwide Digital Population as of January 2021*, STATISTA, https://www.statista.com/statistics/617136/digital-population-worldwide/ (last visited Nov. 3, 2021).

40. Catherine Howell & Darrell M. West, *The Internet as a Human Right*, BROOKINGS: TECHTANK (Nov. 7, 2016), https://www.brookings.edu/blog/techtank/2016/11/07/the-internet-as-a-human-right/ (noting that the United Nations declared the Internet to be a human right). *See generally* Karl Bode, *The Case for Internet Access as a Human Right*, VICE (Nov. 13, 2019, 11:06 AM), https://www.vice.com/en/article/3kxmm5/the-case-for-internet-access-as-a-human-right ("Internet access is not merely a luxury for those who can afford it . . . . It is instead highly conducive to a multitude of crucial human interests and rights.").

41. *See* JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET 145 (2019).

42. Batzel v. Smith, 333 F.3d 1018, 1026 (9th Cir. 2003); *see also* Reno v. Am. Civ. Liberties Union, 521 U.S. 844, 858–59 (1997) ("The Telecommunications Act of 1996 . . . was an unusually important legislative enactment. . . . [I]ts primary purpose was to reduce regulation and encourage the 'rapid deployment of new telecommunications technologies.'"); *Telecommunications Act of 1996*, FED. COMMC'NS COMM'N, https://www.fcc.gov/general/telecommunications-act-1996 (June 20, 2013) ("The Telecommunications Act of 1996 is the first major overhaul of telecommunications law in almost 62 years. The goal of this new law is . . . to let any communications business compete in any market against any other.").

43. Tit. V, Pub. L. No. 104-104, 110 Stat. 133 (1996) (codified in scattered sections of 47 U.S.C.); *see also Batzel*, 333 F.3d at 1026; *Reno*, 521 U.S. at 858.

harmful material on the internet.[44] To achieve this aim, former Representative Chris Cox and Senator Ron Wyden—the creators of Section 230—argued that it would be more effective to allow internet users to have the power to "set their own standards" rather than allowing the government to "impos[e] penalties on Internet posters and their service providers."[45] This value is reflected in Section 230's express user control policy, "encourag[ing] the development of technologies which maximize user control over what information is received."[46] In addition to this overarching goal, "there is little doubt that [Section 230] . . . sought to further First Amendment and e-commerce interests on the Internet."[47]

Out of Title V's original statutory scheme, Section 230 is the only provision remaining. The Supreme Court struck down Title V's other provisions as violating the First Amendment.[48] Thus, interactive computer services ("ICSs") are immune from tortious content provided by third parties and for good faith decisions to moderate online content.[49]

---

44. Patricia Spiccia, Note, *The Best Things in Life Are Not Free: Why Immunity Under Section 230 of the Communications Decency Act Should Be Earned and Not Freely Given*, 48 VAL. U. L. REV. 369, 381 (2013) ("[J]uvenile access to pornography was the initial issue Congress sought to address . . . .").

45. KOSSEFF, *supra* note 41, at 63.

46. 47 U.S.C. § 230(b)(3).

47. *Batzel*, 333 F.3d at 1028; *see also* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1047 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) ("The history of § 230(c)(2) shows that access to pornography was Congress's motivating concern, but the language used in § 230 included much more, covering any online material considered to be 'excessively violent, harassing, or otherwise objectionable.'"); Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1103 (N.D. Cal. 2011) ("A principal purpose of the CDA is to encourage [internet service providers] to engage in effective self-regulation . . . .").

48. *See* Trae Havens, Note, *The First Amendment Has Entered the Chat: Oklahoma's Cyberharassment Law*, 73 OKLA. L. REV. 401, 410–11 (2021) (noting that several amendments to the CDA on First Amendment grounds resulted in the dismantling of 47 U.S.C. § 223 from Title V); *see also Reno*, 521 U.S. at 877–79 (striking down 47 U.S.C. § 223) ("We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech").

49. *See Batzel*, 333 F.3d at 1026–27 ("Absent § 230, a person who published or distributed speech over the Internet could be held liable for defamation even if he or she was not the author of the defamatory text . . . ."); Zeran v. Am. Online, Inc., 129 F.3d 327, 330–31 (4th Cir. 1997) ("Congress made a policy choice . . . not to deter harmful online speech through the separate route of imposing tort liability on companies that serve as intermediaries for other parties' potentially injurious messages."); E360Insight, LLC v.

A. Broad Immunity for Interactive Computer Services

Section 230 was a "direct and swift response" to *Stratton Oakmont, Inc. v. Prodigy Services Co*.[50] In *Stratton Oakmont*, a district court held that a website owner could be liable where it "failed to delete posts that allegedly defamed the plaintiff," even if the website owner was unaware of the defamatory content.[51] Section 230 overturned this decision,[52] distinguishing ICS liability from traditional publisher liability.[53] As a result, § 230(c)(1) immunizes ICSs from being treated as "the publisher or speaker of any information provided by another information content provider."[54] The Good Samaritan provision goes a step further, immunizing ICSs from liability based on good faith efforts to restrict access to content "that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable."[55]

Congress defined an ICS as "any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server."[56] Common ICSs include websites and e-mail

---

Comcast Corp., 546 F. Supp. 2d 605, 607, 609 (N.D. Ill. 2008) (interpreting § 230(c)(2) to immunize an ICS's decision to filter spam email from its users' inboxes).

50. KOSSEFF, *supra* note 41, at 2; *see also* Stratton Oakmont, Inc. v. Prodigy Servs. Co., No. 031063/94, 1995 WL 323710 (N.Y. Sup. Ct. May 24, 1995), *superseded by statute*, 47 U.S.C. § 230, *as recognized in* Shiamili v. Real Estate Grp., 17 N.Y.3d 281, 287–88 (N.Y. 2011).

51. KOSSEFF, *supra* note 41, at 2.

52. Ali Grace Zieglowsky, Note, *Immoral Immunity: Using a Totality of the Circumstances Approach to Narrow the Scope of Section 230 of the Communications Decency Act*, 61 HASTINGS L.J. 1307, 1309 (2010) ("Congress enacted § 230 . . . aim[ing] to overturn the decision in *Stratton Oakmont* . . . .").

53. *See* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 14 (2020) ("[Historically] [p]ublishers . . . were subjected to a higher standard because they exercised editorial control. They could be strictly liable for transmitting illegal content.").

54. 47 U.S.C. § 230(c)(1); *see also id.* § 230(f)(3) (defining an information content provider as "any person or entity that is responsible, in whole or in part, for the creation or development of information"); Fair Hous. Council v. Roommates.com, LLC, 521 F.3d 1157, 1162 (9th Cir. 2008) ("If [a website] passively displays content that is created entirely by third parties, then it is only a service provider with respect to that content. But as to content that it creates itself, or is 'responsible, in whole or in part' for creating or developing, the website is also a content provider.").

55. 47 U.S.C. § 230(c)(2).

56. *Id.* § 230(f)(2); *see also* Zeran v. Am. Online, Inc., 129 F.3d 327, 328–29 (4th Cir. 1997) ("[ICSs] offer not only a connection to the Internet as a whole, but also allow their subscribers to access information communicated and stored only on each computer service's

providers.[57] Congress specifically defined an "access software provider" as "a provider of software . . . or enabling tools that . . . filter, screen, allow, or disallow content."[58] Important for purposes of this Comment, anti-malware software qualifies as an access software provider and is afforded the immunity provided by Section 230.[59]

B. The Good Samaritan Provision

The Good Samaritan provision provides sweeping immunity to ICSs.[60] Such immunity encourages ICSs to filter out harmful material by "immunizing them from liability where those efforts failed."[61] In effect, Good Samaritan immunity serves Section 230's original purpose of preventing minors from accessing harmful material online.[62]

Several courts have determined that if a plaintiff adequately pleads that an ICS lacks good faith under the Good Samaritan provision, immunity is

---

individual proprietary network. AOL is just such an interactive computer service." (citation omitted)).

57. *Fair Hous. Council*, 521 F.3d at 1162 n.6 ("Today, the most common interactive computer services are websites."); *see also Malwarebytes, Inc.*, 141 S. Ct. at 14 ("[Section 230(c)(1)] ensures that a company (like an e-mail provider) can host and transmit third-party content without subjecting itself to the liability that sometimes attaches to the publisher or speaker of unlawful content.").

58. 47 U.S.C. § 230(f)(4).

59. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1175 (9th Cir. 2009) ("Kaspersky is an 'access software provider' because, by providing anti-malware software, it 'provide[s] software . . . or enabling tools that . . . filter, screen, allow, or disallow content." (quoting 47 U.S.C. § 230(f)(4))).

60. 47 U.S.C. § 230(c); *see also* Zango, Inc. v. Kaspersky Lab, Inc., No. C07-0807-JCC, 2007 WL 5189857, at *3 (W.D. Wash. Aug. 28, 2007), *aff'd*, 568 F.3d 1169 (9th Cir. 2009) ("Courts interpreting [§ 230(c)(2)'s] immunity have found it to be 'quite robust.'"); Kyle Langvardt, *Regulating Online Content Moderation*, 106 GEO. L.J. 1353, 1369–70 (2018) ("Section 230(c)(2) was intended as a 'Good Samaritan' provision to prevent platforms from assuming new tort liabilities when they took on the job of content moderation."). *See generally* Mike Masnick, *Masnick's Impossibility Theorem: Content Moderation at Scale Is Impossible to Do Well*, TECHDIRT (Nov. 20, 2019, 9:31 AM), https://www.techdirt.com/articles/20191111/23032743367/masnicks-impossibility-theorem-content-moderation-scale-is-impossible-to-do-well.shtml (describing the challenges in moderating content).

61. Goddard v. Google, Inc., No. C 08-2738 JF (PVT), 2008 WL 5245490, at *6 (N.D. Cal. Dec. 17, 2008).

62. 47 U.S.C. § 230(b)(4) (stating that § 230(b)'s purpose is "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").

unavailable.[63] These holdings stem from the plain language of the provision, immunizing actions "taken in good faith."[64] Despite this, the phrase "good faith" lacks a specific definition from courts and Congress alike.[65] Similarly, the phrase "otherwise objectionable" has not been adequately delineated. The Ninth Circuit has noted that determining whether content is "objectionable" under the Good Samaritan provision is necessarily subjective.[66]

While § 230(c)(1) has been the subject of litigation more frequently than its counterpart,[67] the Good Samaritan provision has garnered significant publicity in recent years.[68] The conversation frequently concerns the phrase

63. *See* e360Insight, LLC v. Comcast Corp., 546 F. Supp. 2d 605, 609 (N.D. Ill. 2008) (suggesting that if the plaintiff had adequately pled that the defendant lacked good faith, immunity would not have extended); *see also* Smith v. Trusted Universal Standards in Elec. Transactions, Inc., No. 09-4567 (RBK/KMW), 2010 WL 1799456, at *5, *7–8 (D.N.J. May 4, 2010) (refusing to extend immunity to the defendant after plaintiff alleged Comcast acted in bad faith when it blocked emails); e-ventures Worldwide, LLC v. Google, Inc., No. 2:14–cv–646–FtM–PAM–CM, 2017 WL 2210029, at *3 (M.D. Fla. Feb. 8, 2017) (denying Google's immunity under the Communications Decency Act because e-ventures raised a genuine issue of material fact as to whether Google removed e-venture's websites in "good faith"); Nat'l Numismatic Certification, LLC v. eBay, Inc., No. 6:08-cv-42-Orl-19GJK, 2008 WL 2704404, at *24 (M.D. Fla. July 8, 2008) (denying eBay's motion to dismiss under § 230(c)(2) because eBay allegedly acted "in bad faith"); *Goddard*, 2008 WL 5245490, at *6 (immunizing Google under § 230(c)(2) because plaintiff did not allege bad faith). *But see* Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1105 (N.D. Cal. 2011) ("Although Holomaxx pleads conclusorily [sic] that Microsoft acted in bad faith, the appropriate question is whether Holomaxx has 'pled an absence of good faith.'").

64. Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 882 (N.D. Cal. 2015) (quoting 47 U.S.C. § 230(c)(2)(A)).

65. An executive order from President Trump in May 2020 attempted to delineate the bounds of "good faith," suggesting lack of good faith if actions are "deceptive, pretextual, or inconsistent with a provider's terms of service; or . . . taken after failing to provide adequate notice, reasoned explanation, or a meaningful opportunity to be heard." Exec. Order No. 13,925, 85 Fed. Reg. 34,079, 34,081 (May 28, 2020), https://www.govinfo.gov/content/pkg/FR-2020-06-02/pdf/2020-12030.pdf.

66. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1044 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) ("[T]he provision establishes a subjective standard whereby internet users and software providers decide what online material is objectionable.").

67. Nicholas Conlon, *Freedom to Filter Versus User Control: Limiting the Scope of § 230(c)(2) Immunity*, 2014 U. ILL. J.L. TECH. & POL'Y 105, 114 ("Subsection (c)(1) has been the subject of far more litigation than subsection (c)(2) . . . .").

68. *See* Ailan Evans, *Is Anything Actually Going to Happen to Facebook?*, DAILY CALLER (Oct. 18, 2021, 8:25 PM ET), https://dailycaller.com/2021/10/18/facebook-section-

"otherwise objectionable" in the context of online speech.[69] One of many proposed amendments to the provision came from the Justice Department.[70] Other proposals have advocated amending the act to mitigate online censorship,[71] with some having proposed to repeal Section 230 entirely.[72] Notably, Senator Wyden and former Representative Cox opposed proposals to repeal the act, suggesting that it would close "the many online avenues that ordinary citizens currently use to express themselves."[73] Instead, they encouraged Congress to "examine whether it's possible to amend Section

230-frances-haugen/ (describing proposed amendments to Section 230 in September and October of 2021); Eric Goldman, *Section 230 Year-in-Review for 2020*, TECH. & MKTG. L. BLOG (Jan. 11, 2021), https://blog.ericgoldman.org/archives/2021/01/section-230-year-in-review-for-2020.htm ("Over two dozen Section 230 reform or repeal bills were introduced in Congress' 116th session."); Tom Kulik, *A Lack of (Good) Faith III: Rethinking Section 230 for the 21st Century*, ABOVE L. (Oct. 26, 2020, 11:18 AM), https://abovethelaw.com/2020/10/a-lack-of-good-faith-iii-rethinking-section-230-for-the-21st-century/ ("Who would have thought that the [2020] election season would have vaulted Section 230 of the Communications Decency Act into the forefront of the electoral conversation?").

69. *See* Matt Schruers, *What Is Section 230's "Otherwise Objectionable" Provision?*, DISCO (July 29, 2020), https://www.project-disco.org/innovation/072920-what-is-section-230s-otherwise-objectionable-provision/.

70. Press Release, U.S. Dep't of Just., The Justice Department Unveils Proposed Section 230 Legislation (Sept. 23, 2020), https://www.justice.gov/opa/pr/justice-department-unveils-proposed-section-230-legislation; *see also Department of Justice's Review of Section 230 of the Communication's Decency Act of 1996*, U.S. DEP'T JUST. ARCHIVES, https://www.justice.gov/ag/department-justice-s-review-section-230-communications-decency-act-1996 (last visited Mar. 22, 2022) (suggesting a replacement of "otherwise objectionable" with more definitive language and, therefore, extending immunity to good faith efforts to remove material that is "unlawful" or "promotes terrorism"); Mike Masnick, *Justice Department Releases Its Dangerous & Unconstitutional Plan to Revise Section 230*, TECHDIRT (Sept. 24, 2020, 9:28 AM), https://www.techdirt.com/articles/20200923/14472345369/justice-department-releases-dangerous-unconstitutional-plan-to-revise-section-230.shtml [hereinafter Masnick, *Justice Department*] (criticizing the proposal as a content-based regulation of speech and thus unconstitutional under the First Amendment).

71. *See* Stop the Censorship Act of 2020, H.R. 7808, 116th Cong. § 2 (2020); Stop Suppressing Speech Act of 2020, S. 4828, 116th Cong. § 2 (2020); Ending Support for Internet Censorship Act, S. 1914, 116th Cong. § 2 (2019).

72. *See* COVID-Related Tax Relief Act of 2020, S. 5085, 116th Cong. § 2 (2020); Abandoning Online Censorship Act, H.R. 8896, 116th Cong. § 2 (2020); A Bill to Repeal Section 230 of the Communications Act of 1934, S. 5020, 116th Cong. (2020).

73. Ron Wyden & Chris Cox, Opinion, *Don't Let Donald Trump Crush Internet Free Speech*, USA TODAY (Dec. 18, 2020, 2:33 PM), https://www.usatoday.com/story/opinion/2020/12/18/section-230-and-complications-free-speech-internet-column/3928033001/. Specifically, the authors argued against former President Trump's demand to repeal Section 230 entirely. *Id.*

230 without doing more harm than good."[74] While the Good Samaritan provision faces increasing scrutiny, Congress has declined to amend it.

C. "Otherwise Objectionable" and Relevant Caselaw

The Ninth Circuit's holding in *Enigma* articulated a limit to the definition of "otherwise objectionable."[75] Specific interpretations of the phrase are scarce, but the Ninth Circuit was not the first court to determine its finite scope. Many courts that have done so, however, are in the Ninth Circuit.[76] This geographic pattern is likely because of the sheer number of tech companies in Silicon Valley.[77]

While broad immunity under the Good Samaritan provision is well established,[78] absolute immunity is not guaranteed.[79] Some courts have applied limited immunity when interpreting "otherwise objectionable."[80] For example, a California district court declined to extend immunity to YouTube when it removed a user's video, claiming it was "otherwise objectionable."[81] YouTube asserted that the plaintiff's video violated its terms of service because it used automated technologies to inflate the

74. *Id.*

75. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) ("We hold that the phrase 'otherwise objectionable' does not include software that the provider finds objectionable for anticompetitive reasons.").

76. *See* Song Fi Inc. v. Google, Inc., 108 F. Supp. 3d 876, 882–84 (N.D. Cal. 2015); Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014); PC Drivers Headquarters, LP v. Malwarebytes Inc., 371 F. Supp. 3d 652, 662 (N.D. Cal. 2019); Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011).

77. *See Silicon Valley Map of Tech Companies and Startups*, EMPLOYBL (Mar. 10, 2020), https://www.employbl.com/blog/silicon-valley-companies-map (linking a list of 262 tech companies in Silicon Valley as of March 2020). *See generally* Alexis C. Madrigal, *Silicon Valley Abandons the Culture That Made It the Envy of the World*, ATLANTIC (Jan. 15, 2020), https://www.theatlantic.com/technology/archive/2020/01/why-silicon-valley-and-big-tech-dont-innovate-anymore/604969/ ("From Apple to Facebook, Silicon Valley's freewheeling ecosystem of new, nimble corporations created massive wealth and retilted the world's economic axis.").

78. Murphy v. Twitter, Inc., 274 Cal. Rptr. 3d 360, 363 (Cal. Ct. App. 2021) ("Under section 230, interactive computer service providers have broad immunity . . . .").

79. *See* Fair Hous. Council v. Roommates.Com, LLC, 521 F.3d 1157, 1174 (9th Cir. 2008) (noting that close cases "must be resolved in favor of immunity").

80. *See, e.g.*, *Song Fi*, 108 F. Supp. 3d at 882 (declining to interpret "otherwise objectionable" as meaning "anything to which a content provider objects regardless of why it is objectionable").

81. *Id.*

video's view count.[82] The court referenced the plain meaning of "otherwise objectionable," holding that YouTube's decision was not "the kind of self-regulatory editing and screening that Congress intended to immunize."[83]

Another court similarly expressed a limited purview of the phrase, declining to extend "otherwise objectionable" to "any or all information or content."[84] On the other end of the spectrum, however, "otherwise objectionable" has been interpreted without bounds, immunizing "any action" with little qualification.[85]

Interpreting "otherwise objectionable" is certainly subjective,[86] but it is unlikely that Congress intended it to grant complete immunity. Courts are beginning to recognize this, slowly chipping away at the expansive interpretations established in the early years of the internet.[87] Unless Congress modifies the Good Samaritan provision, courts will continue to apply inconsistent interpretations of the statute, deteriorating an already unpredictable application of the law.

III. A New Frontier for "Otherwise Objectionable"

A. Background

In *Enigma*, the Ninth Circuit created a novel limitation to "otherwise objectionable."[88] The court denied Malwarebytes's motion to dismiss, holding that when an ICS filters out a competitor's software with anticompetitive animus, it falls outside the scope of immunity provided by

82. *Id.* at 880.

83. *Id.* at 884.

84. Sherman v. Yahoo! Inc., 997 F. Supp. 2d 1129, 1138 (S.D. Cal. 2014) (holding that "immunity is inapplicable where Yahoo! did not engage in any form of content analysis of the subject text" before sending an automatic notification that the text was objectionable).

85. PC Drivers Headquarters, LP v. Malwarebytes Inc., 371 F. Supp. 3d 652, 660 (N.D. Cal. 2019) ("The phrase 'any action' has only one qualifier for the immunity to apply: that the 'action' is 'taken to enable or make available to information content providers or others the technical means to restrict access to material.'").

86. Holomaxx Techs. v. Microsoft Corp., 783 F. Supp. 2d 1097, 1104 (N.D. Cal. 2011) (acknowledging that the "otherwise objectionable" determination is subjective).

87. *See Song Fi*, 108 F. Supp. 3d at 884 ("[T]he ordinary meaning of 'otherwise objectionable,' as well as the context, history, and purpose of the Communications Decency Act all counsel against reading 'otherwise objectionable' to mean anything to which a content provider objects regardless of why it is objectionable.").

88. *See* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

the Good Samaritan provision.[89] Specifically, the court held that the broad language of "otherwise objectionable" does not encompass such filtering.[90]

Enigma Software Group ("Enigma") is a software company that sells a variety of anti-malware products.[91] Enigma's most popular product, Spyhunter, is purported to "scan for, identify, remove and block malware, potentially unwanted programs ("PUPs") and other objects."[92] The software has received mixed reviews from experts, with one stating it "does what it promises . . . [b]ut competitors deliver much more."[93] Another expert, Bleeping Computer ("Bleeping"),[94] critiqued Spyhunter by "making fact based claims . . . about Enigma's dubious product, dubious customer service tactics . . . and dubious lawsuits."[95] In response to this criticism, Enigma sued Bleeping for defamation.[96] The parties settled after Bleeping filed counterclaims against Enigma.[97] As a result, Enigma garnered a

89. *Id.* at 1052.

90. *Id.* at 1045.

91. *Products*, ENIGMASOFT, https://www.enigmasoftware.com/products/ (last visited Oct. 5, 2021).

92. *SpyHunter*, ENIGMASOFT, https://www.enigmasoftware.com/products/spyhunter/#windows (last visited Jan. 4, 2020). *See generally Enigma*, 946 F.3d at 1047 ("PUPs include, for example, what Malwarebytes describes as software that contains 'obtrusive, misleading, or deceptive advertisements, branding or search practices.'"); Chris Hoffman, *PUPs Explained: What Is a "Potentially Unwanted Program"?*, HOW-TO GEEK (Nov. 4, 2015, 6:40 AM EDT), https://www.howtogeek.com/232791/pups-explained-what-is-a-potentially-unwanted-program/ ("'Potentially unwanted programs' often arrive bundled with other software and . . . slow [your computer] down, track you, clutter the system, and show you additional advertisements.").

93. Neil J. Rubenking, *Enigma SpyHunter 4 Review*, PCMAG (Mar. 24, 2016), https://www.pcmag.com/reviews/enigma-spyhunter-4.

94. Enigma Software Grp. USA, LLC v. Bleeping Computer LLC, 194 F. Supp. 3d 263, 270 (S.D.N.Y. 2016) (identifying Bleeping as a website offering "information, advice, and resources about computer technology and security").

95. Tim Cushing, *Shady Anti-Spyware Developer Loses Lawsuit Against Competitor Who Flagged Its Software as Malicious*, TECHDIRT (Nov. 14, 2017, 3:36 PM), https://www.techdirt.com/articles/20171112/19434338601/shady-anti-spyware-developer-loses-lawsuit-against-competitor-who-flagged-software-as-malicious.shtml.

96. *Bleeping Computer*, 194 F. Supp. 3d at 272. Luckily, Bleeping received $5,000 from Malwarebytes to fund its legal defense. Cushing, *supra* note 95.

97. *Enigma Software Group Resolves Bleeping Computer Litigation*, CISION (Mar. 3, 2017, 22:48 PM GMT), https://www.prnewswire.com/in/news-releases/enigma-software-group-resolves-bleeping-computer-litigation-615362934.html. While most details of the settlement are confidential, Bleeping disclosed in a post-settlement press release that it had taken down the allegedly defamatory posts about Enigma. *Id.*

questionable reputation, being described by some as "shady" and "litigious."[98]

Enigma and defendant Malwarebytes have been competitors since Malwarebytes's inception in 2008.[99] Like Enigma, Malwarebytes advertises itself as a provider of anti-malware software.[100] Its malware detection services are "designed to scan consumer[s'] computers and to report to consumers in commercial advertisements or promotions any threats, PUPs, malware and viruses for de-installation."[101] In 2016, Malwarebytes listed Enigma as a PUP after revising its qualifying criteria.[102] The effect of this revision was that when a Malwarebytes user attempted to download Enigma's software, "the user was alerted of a security risk and . . . the download was prohibited."[103] This was not the first time Enigma had been filtered out by another company's anti-malware software.[104]

In its complaint, Enigma alleged that Malwarebytes intentionally "configured its software to block users from accessing Enigma's software in order to divert Enigma's customers."[105] The district court[106] granted

98. Tim Cushing, *Enigma Software Countersued for Waging a 'Smear Campaign' Against Site It Claimed Defamed It*, TECHDIRT (Aug. 17, 2016, 2:42 PM), https://www.techdirt.com/articles/20160813/15314035235/enigma-software-countersued-waging-smear-campaign-against-site-it-claimed-defamed-it.shtml. In a 2007 announcement, Enigma stated that it had sent out seven cease and desist letters to software companies who listed its software as a "security threat." CagedTech, *Enigma Software Group Inc. Responds to CheckPoint Software and Competing Corporations Listing SpyHunter as a Security Risk*, ENIGMASOFT (July 13, 2007), https://www.enigmasoftware.com/esgi-responds-to-checkpoint-software/ [hereinafter *Enigma Software Group Inc. Responds*].

99. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1047 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

100. *Malwarebytes Premium*, MALWAREBYTES, https://www.malwarebytes.com/lp/sem/en/sem2.html?gclid=EAIaIQobChMIvYuz3YjB7AIVC02GCh0etQ4gEAAYASAAEgLovfD_BwE (last visited Oct. 5, 2021).

101. PC Drivers Headquarters, LP v. Malwarebytes, Inc., 371 F. Supp. 3d 652, 656 (N.D. Cal. 2019).

102. *Enigma*, 946 F.3d at 1048. The Ninth Circuit describes this revision as including "any program that, according to Malwarebytes, users did not seem to like." *Id. See generally* Hoffman, *supra* note 92 (defining PUPs); Purdy & Klosowski, *supra* note 9 (describing how anti-malware software firms constantly revise criteria for what is deemed a threat online).

103. *Enigma*, 946 F.3d at 1048.

104. *See Enigma Software Group Inc. Responds*, *supra* note 98. Enigma itself reported that it was being filtered out by other software as early as 2004. *Id.*

105. *Enigma*, 946 F.3d at 1044.

Malwarebytes's motion to dismiss, interpreting Ninth Circuit precedent in *Zango, Inc. v. Kaspersky Lab, Inc.* "to mean that anti-malware software providers are free to block users from accessing any material that those providers, in their discretion, deem to be objectionable."[107]

The Ninth Circuit disagreed with the district court's reliance on *Zango*.[108] Nevertheless, *Zango* may be the most persuasive case leading to the holding in *Enigma*. In *Zango*, the Ninth Circuit analyzed claims against software provider Kaspersky Lab for, among other things, tortious interference with contractual rights and unjust enrichment.[109] Kaspersky's software "detects malware that may be present [online] that a computer user is about to download."[110] Zango alleged that Kaspersky, in essence, disabled its toolbar from customers' computers.[111] The *Zango* court held that Kaspersky, as a provider of an ICS, was entitled to immunity under the Good Samaritan provision.[112]

Perhaps more influential than *Zango*'s holding itself is Judge Fisher's concurrence.[113] Judge Fisher expressed concern that providing excessively broad immunity under the Good Samaritan provision would be inconsistent with congressional intent.[114] Excessively broad immunity, according to Judge Fisher, could be problematic if "providers of blocking software were to be given free license to *unilaterally* block the dissemination of material by content providers."[115] He warned against construing "otherwise objectionable" in a way that allowed for abuse by a software provider

106. While Enigma originally filed its claim in New York state court, the New York court granted a motion to transfer to the Northern District of California because "the conduct at issue had national reach." *Id.* at 1048.

107. *Id.* (citing Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009)).

108. *Id.* at 1049–50.

109. *Zango*, 568 F.3d at 1172.

110. *Id.* at 1171.

111. *Id.*

112. *Id.* at 1177–78. Notably, Zango did not allege in its complaint whether Kaspersky's action was done in good faith. *See id.* at 1178 n.1 (Fisher, J., concurring) (indicating that Zango waived its argument for a good faith limitation to immunity by making the argument only in reply).

113. *See, e.g.*, Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1045 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020) (citing the warnings from Judge Fisher's concurrence as grounds to reverse the district court decision).

114. *Zango*, 568 F.3d at 1178 (Fisher, J., concurring).

115. *Id.*

seeking to "block content for anticompetitive purposes or merely at its malicious whim."[116]

In contrast to the district court, the Ninth Circuit refused to rely on *Zango*.[117] Specifically, the *Enigma* court emphasized that the issue in *Zango* was whether Section 230 immunity extended to software providers at all,[118] not "whether there were limitations on a provider's discretion to declare online content 'objectionable.'"[119] Instead, the Ninth Circuit held that Section 230 does not immunize "blocking a competitor's program for anticompetitive reasons," and since Enigma pled specifically that Malwarebytes's actions *were* anticompetitive, Malwarebytes was not entitled to Section 230 immunity.[120]

The Ninth Circuit rejected Malwarebytes's assertion that because it was an ICS—even if it acted with anticompetitive intent—it qualified for immunity.[121] The court described the assertion as being "contrary" to the history and purpose of the provision.[122] In sum, the Ninth Circuit held that allowing Malwarebytes to exercise unbridled discretion to determine what is "objectionable" would "enable and potentially motivate internet-service providers to act for their own, and not the public, benefit."[123] Such discretion would contradict Congress's express user control policy.[124]

Nevertheless, the Ninth Circuit acknowledged the importance of allowing ICSs to possess some discretion to filter online threats, such as spam and malware, and thus refused to interpret the Good Samaritan

116. *Id.*

117. *Enigma*, 946 F.3d at 1049 ("District courts nationwide have grappled with the issues discussed in *Zango*'s majority and concurring opinions, and have reached differing results.").

118. *Id.* at 1050.

119. *Id.* at 1049.

120. *Id.* at 1052.

121. *Id.* at 1051.

122. *Id.*

123. *Id.* (citing Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178 (9th Cir. 2009) (Fisher, J., concurring)).

124. *Id.* ("Immunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy."). An express policy of Section 230 is "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools." 47 U.S.C. § 230(b)(3).

provision too narrowly.[125] Three months after *Enigma*, a California district court immunized a software company that allegedly filtered out another company for anticompetitive reasons.[126] The court held that because the plaintiff was not a direct competitor of the defendant, *Enigma*'s holding did not preclude the defendant from the Good Samaritan provision's immunity.[127] This tapering of *Enigma* suggests that although the Ninth Circuit's holding was novel, it was also limited.

B. Enigma*'s Holding Solidified (For Now)*

On October 9, 2020, the Supreme Court denied Malwarebytes's petition for writ of certiorari, ending the *Enigma* saga and solidifying the Ninth Circuit's interpretation of what falls within the purview of "otherwise objectionable."[128] Justice Thomas issued a statement with the denial,[129] suggesting that an unnecessarily broad interpretation of Section 230 would result in "serious consequences."[130]

Justice Thomas touched briefly on the Good Samaritan provision, writing, "Where Congress uses a particular phrase in one subsection and a different phrase in another, we ordinarily presume that the difference is meaningful."[131] Notably, Justice Thomas suggested that courts should apply the statutory interpretation canon *ejusdem generis* when interpreting the Good Samaritan provision.[132] In *Enigma*, however, the Ninth Circuit

---

125. *Enigma*, 946 F.3d at 1052 ("Congress wanted to give internet users tools to avoid . . . harassing materials. Spam, malware and adware could fairly be . . . called 'otherwise objectionable' . . . .").

126. Asurvio LP v. Malwarebytes Inc., No. 5:18-CV-05409-EJD, 2020 WL 1478345, at *1 (N.D. Cal. Mar. 26, 2020).

127. *Id.* at *5.

128. *See* Malwarebytes, Inc. v. Enigma Software Grp. USA, LLC, 141 S. Ct. 13, 13 (2020). After denial of certiorari, Enigma attempted to revive its litigation with Malwarebytes on alternative claims, including violations of the Lanham Act, New York state law, and various tort allegations. *See* Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., No. 5:17-cv-02915-EJD, 2021 WL 3493764, at *1 (N.D. Cal. Aug. 9, 2021). A district court judge granted Malwarebytes's motion to dismiss for failure to state a claim on non-Section 230 grounds. *Id.* at *11.

129. *Malwarebytes, Inc.*, 141 S. Ct. at 14 ("I write to explain why, in an appropriate case, we should consider whether the text of this increasingly important statute aligns with the current state of immunity enjoyed by Internet platforms.").

130. *Id.* at 18.

131. *Id.* at 16.

132. *See id. See generally In re* Pangang Grp. Co., LTD., 901 F.3d 1046, 1056 (9th Cir. 2018) ("The canon of ejusdem generis refers to the inference that a general term in a list

rejected applying the canon: "[W]e do not . . . determine the precise relationship between the term 'otherwise objectionable' and the seven categories that precede it."[133] Despite this inconsistency, Justice Thomas's statement doesn't appear to be designed to provide guidance to lower courts but rather is an open invitation to bring a Section 230 case to the Court (just a different Section 230 case, apparently).[134]

As a result of the Supreme Court's denial of certiorari, the future of Section 230's "otherwise objectionable" catchall is left to each lower court's determination. Undoubtedly, the Ninth Circuit's holding in *Enigma* is remarkably persuasive authority for courts facing similar issues. Nevertheless, without Supreme Court guidance and absent congressional intervention, software companies acting outside the scope of the Ninth Circuit's authority potentially have complete discretion to filter out competitors for anticompetitive reasons, abusing both Section 230's express user control policy and antitrust law.

IV. Antitrust Implications

While *Enigma* did not directly implicate antitrust law,[135] both Section 230 and antitrust law share a similar policy goal: protecting competition.[136] Congress intended for Section 230 to "preserve the vibrant and competitive

---

'should be understood as a reference to subjects akin to th[ose] with specific enumeration.'" (alteration in original) (quoting Ali v. Fed. Bureau of Prisons, 552 U.S. 214, 223 (2008))).

133. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1052 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

134. *Malwarebytes, Inc.*, 141 S. Ct. at 18 ("Without the benefit of briefing on the merits, we need not decide today the correct interpretation of § 230. But in an appropriate case, it behooves us to do so.").

135. *See* Enigma Software Grp. USA LLC v. Malwarebytes Inc., No. 5:17-CV-02915-EJD, 2017 WL 5153698, at *1 (N.D. Cal. Nov. 7, 2017) (listing the causes of action as false advertising under the Lanham Act, violations of New York state law, tortious interference with contractual relations, and tortious interference with business relations).

136. *Enigma*, 946 F.3d at 1051 ("Congress . . . gave providers discretion to identify objectionable content in large part to protect competition, not suppress it."); Dina Srinivasan, *The Antitrust Case Against Facebook: A Monopolist's Journey Towards Pervasive Surveillance in Spite of Consumers' Preference for Privacy*, 16 BERKELEY BUS. L.J. 39, 91 (2019) (stating that antitrust laws "regulate a range of conduct that harms the competitive process").

free market."[137] Similarly, antitrust law seeks to "preserv[e] free and unfettered competition as the rule of trade."[138]

A number of scholars have noted that antitrust law is not up to speed with the digital economy; therefore, changes within modern economics "threaten to complicate digital platform antitrust litigation."[139] Digital platforms possess a unique combination of characteristics that drive power into the hands of a single company: (1) "strong network effects";[140] (2) "strong economies of scale and scope";[141] (3) "marginal costs close to zero";[142] (4) "high and increasing returns to the use of data";[143] and (5) "low distribution costs that allow for a global reach."[144] In combination, these factors create a "winner takes all" effect, harming competition by deterring competitors from entering the market.[145] The questionable nature of antitrust law's slow adjustment to the modern age leaves room to doubt that competition in the anti-malware software market is adequately safeguarded.[146]

Relevant to this Comment is antitrust law's emphasis on stifling "anticompetitive" conduct.[147] No clearly articulated test exists to determine

---

137. 47 U.S.C. § 230(b)(2).

138. N. Pac. Ry. Co. v. United States, 356 U.S. 1, 4 (1958).

139. Josh Palmer, *It's High Tide Again in Internet Markets*, COMPETITION: J. ANTITRUST, UCL & PRIVACY SECTION CAL. LAWS. ASS'N, Fall 2020, at 70, 80–81 ("The complex interdependencies among the various platform sides have led well-established economists to call into question the sufficiency of traditional economic analyses and tools to handle competition analysis in digital platforms."); *see also* Gregory Day & Abbey Stemler, *Are Dark Patterns Anticompetitive?*, 72 ALA. L. REV. 1, 5 (2020).

140. STIGLER COMM. ON DIGITAL PLATFORMS, STIGLER CTR. FOR THE STUDY OF THE ECON. & THE STATE, FINAL REPORT 7 (Sept. 2019), https://www.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf (explaining network effects as "the more people use a product, the more appealing this product becomes for other users").

141. *Id.* (describing economies of scale and scope as "the cost of producing more or of expanding in other sectors decreases with company's size").

142. *Id.*

143. *Id.* at 7–8 (describing high and increasing returns as "the more data you control, the better your product").

144. *Id.* at 8.

145. *Id.*; *see also* L.A. Land Co. v. Brunswick Corp., 6 F.3d 1422, 1427–28 (9th Cir. 1993) (suggesting that a barrier to entry is created where factors deter competitors from the market).

146. *See generally* Palmer, *supra* note 139.

147. *See, e.g.*, Spirit Airlines, Inc. v. Nw. Airlines, Inc., 431 F.3d 917, 951 (6th Cir. 2005) ("[A]nticompetitive conduct can come in too many different forms, and is too

whether conduct is anticompetitive. However, courts look at whether conduct "impair[s] the opportunities" of competitors or whether conduct "does not further competition on the merits or does so in an unnecessarily restrictive way."[148]

Enigma recognized that Section 230's user control policy combined with antitrust law's focus on anticompetitive conduct threatened the anti-malware software market. Congress "gave providers discretion to identify objectionable content . . . to protect competition, not suppress it."[149]

Allowing ICS users to maintain control over what they encounter on their computers is a core tenet behind Section 230.[150] If "otherwise objectionable" immunizes software companies that filter out competitors for anticompetitive reasons, Section 230 undermines software users' power of choice.

Admittedly, anti-malware software providers must maintain some discretion in what content to filter.[151] Former Representative Cox and Senator Wyden hoped that software companies would be able to set their own standards and that "[t]he market . . . would encourage the companies to develop conduct codes that are most appropriate for their audiences."[152] In the same vein, users always maintain control over which programs to install

---

dependent upon context, for any court or commentator ever to have enumerated all the varieties." (internal quotation marks omitted) (quoting Conwood Co., L.P. v. U.S. Tobacco Co., 290 F.3d 768, 784 (6th Cir. 2002))); Gen. Indus. Corp. v. Hartz Mountain Corp., 810 F.2d 795, 804 (8th Cir. 1987) ("Anticompetitive conduct is conduct without legitimate business purpose that makes sense only because it eliminates competition.").

148. Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 605 n.32 (1984) (quoting 3 AREEDA & TURNER, *supra* note 36, at 78); *see also* United States v. Grinnell Corp., 384 U.S. 563, 570–71 (1966) (describing anticompetitive conduct as the "willful acquisition or maintenance of [monopoly] power as distinguished from growth or development as a consequence of a superior product, business acumen, or historic accident").

149. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1051 (9th Cir. 2019).

150. *See generally* 47 U.S.C. § 230(b)(3). Section 230 authors argued it would be more effective to allow internet users to have the power to "set their own standards" rather than allowing the government to "impos[e] penalties on Internet posters and their service providers . . . ." KOSSEFF, *supra* note 41, at 63. *But see* 47 U.S.C. § 230(c)(2)(A) (granting both providers and users of ICSs immunity to restrict access to certain content in good faith).

151. *Enigma*, 946 F.3d at 1052 ("Congress wanted to give internet users tools to avoid . . . harassing materials. Spam, malware and adware could fairly be . . . called 'otherwise objectionable' . . . ."). *See generally* 47 U.S.C. § 230(c)(2).

152. KOSSEFF, *supra* note 41, at 64.

or remove.[153] As Judge Fisher warned in *Zango*, however, the threat to user control arises where users are *unaware* of filtering decisions being made on their behalf.[154]

When Malwarebytes removed Enigma's software from its users' computers, it did not allow its users to determine for themselves which software they wanted to install.[155] Instead, Malwarebytes simply prohibited its users from downloading any Enigma software.[156] In effect, Malwarebytes stripped away its customers' ability to control what they encounter online, in opposition to Congress's express intent.[157] The Ninth Circuit thus acknowledged the danger of an expansive interpretation of "otherwise objectionable," stating that "[i]mmunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy."[158]

Likewise, a broad interpretation of "otherwise objectionable" undermines antitrust law's focus on preventing anticompetitive conduct. If software providers' actions are immune from liability, there is little—if any—disincentive from filtering out competitors who threaten their bottom line.[159] In such a case, power begets power: the more users a software has, the more users it will be able to prevent from accessing competitors' software. Such conduct is antithetical to competition on the merits.[160] It impairs the opportunities of rivals by removing them from the market

153. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1179 (9th Cir. 2009) (Fisher, J., concurring) ("Computer users are of course always free to replace their blocking software with software more in line with their preferences . . . .").

154. *Id.*

155. *Enigma*, 946 F.3d at 1048.

156. *Id.*

157. *See id.* After Malwarebytes began flagging Enigma's software as PUPs, "anytime a user with Malwarebytes's software tried to download those Enigma programs, the user was alerted of a security risk and . . . the download was prohibited." *Id.*

158. *Id.* at 1051.

159. *See* Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1179 (9th Cir. 2009) (Fisher, J., concurring) ("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.").

160. *See* Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 605 n.32 (1984). Exclusionary conduct "tends to impair the opportunities of rivals" and "either does not further competition on the merits or does so in an unnecessarily restrictive way." *Id.* (quoting 3 AREEDA & TURNER, *supra* note 36, at 78).

entirely rather than letting users discern which software is more suitable to their preferences.

The *Enigma* court used the word "anticompetitive" twenty-one times in its majority opinion,[161] suggesting Malwarebytes's conduct fell within the legal scope of the word. Notably, "anticompetitive conduct falls outside the bounds of 'competition on the merits,'"[162] and if conduct impairs competitors' opportunities, competition is not on the merits.[163] When Malwarebytes removed Enigma's software from its users' computers, it prevented Enigma from competing on the merits by removing it from a portion of the market.[164]

Further, allowing software providers such discretion is a barrier to entry, deterring potential firms from entering the software market. Barriers to entry include "factors in the market that deter entry while permitting incumbent firms to earn monopoly returns."[165] If software companies have discretion to filter competitors for anticompetitive reasons, new companies are disincentivized from entering the market. Any company seeking to enter the software market would be wise to avoid the anti-malware sector, or any sector with an ability to filter out rivals. An established company like Malwarebytes,[166] with discretion to filter rivals from being seen by their users, would reap benefits by facing less competition.[167] But despite Malwarebytes's anticompetitive conduct, it is dubious whether the company could be liable under established antitrust law.

---

161. *Enigma*, 946 F.3d at 1045–54.

162. Srinivasan, *supra* note 136, at 90.

163. *Aspen Skiing Co.*, 472 U.S. at 605 n.32.

164. *See Enigma*, 946 F.3d at 1048 ("[A]nytime a user with Malwarebytes's software tried to download those Enigma programs, the user was alerted of a security risk and . . . the download was prohibited.").

165. L.A. Land Co. v. Brunswick Corp., 6 F.3d 1422, 1427–28 (9th Cir. 1993) (quoting PHILLIP E. AREEDA & HERBERT HOVENKAMP, ANTITRUST LAW 509–10 (Supp. 1992)).

166. Shanhong Liu, *Global Market Share Held by Windows Anti-Malware Vendors 2020*, STATISTA (Sept. 29, 2021), https://www.statista.com/statistics/271048/market-share-held-by-antivirus-vendors-for-windows-systems/ (reporting that, as of May 2020, Malwarebytes holds an 8.72% market share in the Windows anti-malware application market).

167. *See generally* Stephen King, *Why (Inefficient) Businesses Want to Limit Competition*, CONVERSATION (June 13, 2013, 9:05 AM EDT), https://theconversation.com/why-inefficient-businesses-want-to-limit-competition-15186 (explaining that consumers benefit from more competition, but businesses prefer less competition, "find[ing] it mutually beneficial to prevent competition among incumbents and raise barriers to keep out new competitors").

Section 2 of the Sherman Act makes it an offense to monopolize, attempt to monopolize, or conspire to monopolize any area of commerce.[168]Anticompetitive conduct coupled with monopoly power violates section 2 of the Sherman Act.[169] A monopoly is defined as the "power to control prices or exclude competition."[170] Generally, courts look to market share to determine monopoly power.[171] With only an 8.72% market share, Malwarebytes likely can't be considered a monopoly.[172] While "neither size nor market share alone suffice to establish a monopoly,"[173] the Supreme Court has held that maintaining greater than two-thirds of a market plus 80% of a related market was an illegal monopoly.[174] The discrepancy between Malwarebytes's market share and the Supreme Court's holding suggests it does not hold illegal monopoly power.

Nevertheless, a company is not required to possess monopoly power to be liable under section 2.[175] Attempted monopolization is prohibited when a

168. 15 U.S.C. § 2 ("Every person who shall monopolize, or attempt to monopolize, or combine or conspire with any other person or persons, to monopolize any part of the trade or commerce among the several States, or with foreign nations, shall be deemed guilty of a felony . . . .").

169. *Id.*; *see also* Aspen Skiing Co. v. Aspen Highlands Skiing Corp., 472 U.S. 585, 602 (1984) (suggesting that the words "anticompetitive," "exclusionary," and "predatory" can be used interchangeably).

170. United States v. E.I. du Pont de Nemours & Co., 351 U.S. 377, 391 (1956). However, not every monopoly is illegal: "Patents . . . furnish the most familiar type of classic monopoly." *Id.* at 392.

171. *See, e.g.*, United States v. Grinnell Corp., 384 U.S. 563, 571 (1966) ("The existence of [monopoly] power ordinarily may be inferred from the predominant share of the market."); Am. Tobacco Co. v. United States, 328 U.S. 781, 797, 815 (1946) (upholding a jury's verdict that American Tobacco Co. conspired to monopolize the tobacco industry because it controlled "over two-thirds of the entire domestic field of cigarettes, and . . . over 80% of the field of comparable cigarettes").

172. *See generally* Liu, *supra* note 166.

173. United States v. Syufy Enters., 903 F.2d 659, 671 (9th Cir. 1990); *see also* L.A. Land Co. v. Brunswick Corp., 6 F.3d 1422, 1426, 1429 (9th Cir. 1993) (declining to hold that a company had monopoly power, despite a 100% market share).

174. *Am. Tobacco Co.*, 328 U.S. at 797. The Second Circuit has similarly held that holding 90% of the market constituted monopoly power. United States v. Aluminum Co., 148 F.2d 416, 429 (2d Cir. 1945). The Fifth Circuit has found that 71% to 76% market share was sufficient to constitute a monopoly. Heatransfer Corp. v. Volkswagenwerk, A.G., 553 F.2d 964, 981 (5th Cir. 1977).

175. *See* Tops Mkts., Inc. v. Quality Mkts., Inc., 142 F.3d 90, 100 (2d Cir. 1998) ("[A] lesser degree of market power may establish an attempted monopolization claim than that

plaintiff can show (1) anticompetitive conduct,[176] (2) a specific intent to acquire monopoly power,[177] and (3) a "dangerous probability" of doing so.[178]

As previously discussed, Malwarebytes's conduct is likely considered anticompetitive. Its anticompetitive conduct could also be used to establish a specific intent to monopolize, because removing competitors from a market is "clearly threatening to competition."[179]

Finally, while it could be challenging to show that the company had a dangerous probability of success, it remains plausible.[180] To determine whether a firm has a dangerous probability of success, courts look to its "capacity to commit the offense," the "scope of its objective," and "the character of its conduct."[181] Most importantly, courts also consider the "actual or threatened impact on competition in the relevant market."[182] Malwarebytes's slim market share suggests it likely does not have the capacity of acquiring monopoly power through filtering out competitors.[183] Further, the scope of Malwarebytes's objective and the character of its conduct are difficult to determine objectively. In its complaint, Enigma

---

necessary to establish a completed monopolization claim."); Spectrum Sports, Inc. v. McQuillan, 506 U.S. 447, 456 (1993) (discussing the requirements to hold an entity liable under section 2 for *attempted* monopolization).

176. *Spectrum Sports*, 506 U.S. at 456.

177. *Id.*; *see also* Times-Picayune Pub. Co. v. United States, 345 U.S. 594, 615 (1953) (inferring a specific intent to monopolize "whenever unlawful effects are found"); Swift & Co. v. United States, 196 U.S. 375, 396 (1905) ("[A]n intent to [monopolize] is necessary in order to produce a dangerous probability that it will happen."); Syufy Enters. v. Am. Multicinema, Inc., 793 F.2d 990, 999 (9th Cir. 1986) (finding that "the jury could reasonably have inferred a specific intent to monopolize" when plaintiff provided evidence that defendant threatened to "run [a competitor] out of town").

178. *Spectrum Sports*, 506 U.S. at 456; *see also* United States v. Am. Airlines, Inc., 743 F.2d 1114, 1119 (5th Cir. 1984) (noting that the requirement of a dangerous probability of success "expresses a significant antitrust principle that the antitrust laws protect competition, not competitors").

179. Catch Curve, Inc. v. Venali, Inc., 519 F. Supp. 2d 1028, 1035 (C.D. Cal. 2007) ("[A]nticompetitive conduct alone can satisfy the specific intent requirement if the conduct 'form[s] the basis for a substantial claim of restraint of trade' or is 'clearly threatening to competition or clearly exclusionary'" (alteration in original) (quoting Twin City Sportservice, Inc. v. Charles O. Finley & Co., Inc., 676 F.2d 1291, 1309 (9th Cir. 1982))).

180. *See, e.g.*, *Am. Airlines, Inc.*, 743 F.2d at 1119 (concluding that the government properly stated a claim for dangerous probability of success).

181. 54 AM. JUR. 2D *Monopolies and Restraints of Trade* § 67 (2021).

182. *Id.*

183. *See* Liu, *supra* note 166.

alleged that Malwarebytes filtered its software for anticompetitive purposes,[184] but Malwarebytes retorted that it filtered the software because Enigma poses a threat to its users.[185] Because the Ninth Circuit ruled on a motion to dismiss, a trier of fact has not determined the issue.[186] Malwarebytes's conduct, however, implicates the greatest factor that courts weigh in determining whether there is a "dangerous probability of success": threatening competition within the anti-malware software market. If permitted, Malwarebytes would continually filter out its competitor, Enigma.[187]

Perhaps Malwarebytes could be liable under section 2 for attempted monopolization. Even if not, however, an expansive reading of "otherwise objectionable" renders liability a possibility within the anti-malware software market. Because "[c]ourts have consistently confirmed that the goal of the antitrust laws is to protect competition rather than competitors,"[188] Section 230 grants software providers an avenue to evade this antitrust principle.

The vagueness of Section 230's "otherwise objectionable" immunizes an unspecified range of conduct and undermines Congress's express intent to preserve user control.[189] This ambiguity, coupled with antitrust law's failure to evolve with the modern digital economy, threatens the free market of anti-malware software.[190] Congress should amend Section 230 to prevent anticompetitive conduct within this market.

---

184. Enigma Software Grp. USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1048 (9th Cir. 2019), *cert. denied*, 141 S. Ct. 13 (2020).

185. *Id.*

186. *See id.* at 1045.

187. *See id.* at 1048 ("[A]nytime a user with Malwarebytes's software tried to download those Enigma programs, the user was alerted of a security risk and . . . the download was prohibited . . . ."). Malwarebytes has also been accused of similar conduct by companies other than Enigma. *See, e.g.*, PC Drivers Headquarters, LP v. Malwarebytes, Inc., No. 1:18-CV-234-RP, 2018 WL 2996897, at *1 (W.D. Tex. Apr. 23, 2018); Asurvio LP v. Malwarebytes Inc., No. 5:18-CV-05409-EJD, 2020 WL 1478345, at *1 (N.D. Cal. Mar. 26, 2020).

188. L.A. Land Co. v. Brunswick Corp., 6 F.3d 1422, 1427 (9th Cir. 1993).

189. *See* 47 U.S.C. § 230(c)(2)(A); *see also* PC Drivers Headquarters, LP v. Malwarebytes, Inc., 371 F. Supp. 3d 652, 660 (N.D. Cal. 2019) (applying a broad interpretation of "otherwise objectionable" by immunizing "any action" taken by an ICS, with little qualification).

190. *See generally* Makan Delrahim, Assistant Att'y Gen., Antitrust Div., U.S. Dep't of Just., Address at Harvard Law School: "Blind[ing] Me with Science": Antitrust, Data, and Digital Markets (Nov. 8, 2019), https://www.justice.gov/opa/speech/file/1217071/download.

V. Proposed Solutions

Software providers possess the ability to covertly strip away users' choice to determine which software to use.[191] This surreptitious power is what Judge Fisher warned against in *Zango* and led to the Ninth Circuit's holding in *Enigma*.[192] It allows software providers to impair user control without consequence and erode competition on the merits.[193]

Congress should amend the Good Samaritan provision to preclude immunity for access software providers when they filter a direct competitor with anticompetitive animus. Instead of allowing "otherwise objectionable" to insulate software providers depending on whatever the relevant court determines, Congress should add a subsection to § 230(c), isolating "access software provider" from the Good Samaritan provision's undefined "otherwise objectionable." This amendment should codify *Enigma*'s holding by specifically prohibiting access software providers from filtering out competitors with anticompetitive animus.[194]

Because there is little caselaw interpreting "otherwise objectionable," altering the language of Section 230 itself is a favorable solution. Another option includes the remaining circuits following the Ninth Circuit's holding in *Enigma*: "[T]he phrase 'otherwise objectionable' does not include software that the provider finds objectionable for anticompetitive reasons."[195]

(calling the analogy between product markets and data markets "too simplistic to be useful" for modern antitrust enforcement).

191. *See, e.g.*, *Enigma*, 946 F.3d at 1044 ("[A]nytime a user with Malwarebytes's software tried to download those Enigma programs, the user was alerted of a security risk and . . . the download was prohibited . . . ."); *Asurvio*, 2020 WL 1478345, at *2 ("Malwarebytes categorized . . . Asurvio's [software] with a negative PUP rating and a security risk to Malwarebytes' customers.").

192. Zango, Inc. v. Kaspersky Lab, Inc., 568 F.3d 1169, 1178 (9th Cir. 2009) (Fisher, J., concurring) ("[E]xtending immunity beyond the facts of this case could pose serious problems if providers of blocking software were to be given free license to *unilaterally* block the dissemination of material by content providers under the literal terms of § 230(c)(2)(A)."); *Enigma*, 946 F.3d at 1045 ("We heed [Judge Fisher's] warning and reverse the district court's decision that read *Zango* to require such an interpretation.").

193. *See Enigma*, 946 F.3d at 1051 ("[I]mmunity for filtering practices aimed at suppressing competition, rather than protecting internet users, would lessen user control over what information they receive, contrary to Congress's stated policy.").

194. *See generally id.* at 1052 ("[W]e hold that § 230 does not provide immunity for blocking a competitor's program for anticompetitive reasons . . . .").

195. *Id.* at 1045.

To avoid unintended results, Congress should narrowly tailor its amendment to Section 230. By addressing access software providers specifically, as opposed to implicating all ICSs, Congress would avoid the unnecessarily broad ramifications that an alteration to the Good Samaritan provision would have.[196] For example, an amendment addressing all ICSs in the Good Samaritan provision could qualify as content-based discrimination under the First Amendment.[197] As Section 230's creators warned, Congress should be careful when amending the statute and "examine whether it's possible to amend Section 230 without doing more harm than good."[198]

Ultimately, this amendment would protect both user control and the free market by ensuring that software providers are not filtered out by direct competitors for anticompetitive reasons. Nevertheless, while such an amendment would threaten to impose additional liability on access software providers, an amendment should otherwise respect a software provider's discretion to determine how to protect its users from threats online.[199]

Procedurally, this amendment would allow for a software provider to survive a motion to dismiss when it adequately pleads that a direct competitor has taken anticompetitive action against them.[200] The amendment would not create a new cause of action or hinder what an anti-malware software could actually filter out.

An amendment separating "access software providers" from the broad immunity encompassing all ICSs would serve the policy goals of both Section 230 and antitrust law. Allowing users of access software providers to determine just what sort of software they want on their computers serves Section 230's user control policy,[201] and imposing liability on companies

196. *See generally* Mike Masnick, *Apparently Trump Refuses to Allow the Government to Do Anything at All Until the Open Internet Is Destroyed*, TECHDIRT (Dec. 23, 2020, 1:49 PM), https://www.techdirt.com/articles/20201223/13392945940/apparently-trump-refuses-to-allow-government-to-do-anything-all-until-open-internet-is-destroyed.shtml (describing the broad ramifications if Section 230 is repealed).

197. *See generally* Masnick, *Justice Department*, *supra* note 70.

198. Wyden & Cox, *supra* note 73.

199. *See Enigma*, 946 F.3d at 1044 ("[Section 230] establishes a subjective standard whereby internet users and software providers decide what online material is objectionable.").

200. *See* Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33, 39 (2019) (describing how judges can typically discern from a plaintiff's complaint whether Section 230 provides immunity).

201. *See generally* 47 U.S.C. § 230(b)(3).

who filter out a competitor with anticompetitive animus serves antitrust law's aim to preserve competition in the free market.[202]

VI. Conclusion

When Congress created Section 230 in 1996, it could not have anticipated the digital world we live in today, nor could it have envisioned the issues arising under the statute's vague language. In response to the lack of remedies available to potential software provider plaintiffs like Enigma, and considering the antitrust issues posed by the current language of Section 230, Congress should amend the Good Samaritan provision of Section 230 to address the past twenty-five years of internet and software development.

Bailey S. Barnes

202. *See generally* N. Pac. Ry. Co. v. United States, 356 U.S. 1, 4 (1958).