Enigma Software Group USA, LLC v. Malwarebytes, Inc.

Allie Pisula

946 F.3D 1040 (9TH CIR. 2019)

In *Enigma Software Group USA, LLC v. Malwarebytes, Inc.,* the United States Court of Appeals for the Ninth Circuit reversed and remanded the district court's decision to grant the defendant's motion to dismiss all four claims brought by plaintiff.[1] The court held that the "otherwise objectionable" clause of 47 U.S.C. § 230(c)(2) does not include blocking content for anticompetitive reasons and that, since all four of Enigma's claims alleged anticompetitive behavior by Malwarebytes, the district court wrongly dismissed the claims.[2]

I. BACKGROUND

Section 230(c)(2) of the Communications Decency Act (CDA) contains an immunity provision, called the "Good Samaritan" provision, that allows internet-service providers to restrict access to "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable" without being subject to liability for offensive content.[3]

Congress enacted the Good Samaritan provision primarily in response to *Stratton Oakmont, Inc. v. Prodigy Services Co.*, which held that when a service provider chooses to filter some offensive content, that provider takes on the responsibility for any non-filtered offensive content, regardless of the provider's degree of knowledge of such content.[4] Some members of Congress, such as Representative Chris Cox, spoke up against this ruling, saying that it deterred creation of filtering software.[5] A driving force behind congressional desire for filtering software was to restrict the availability of online pornography to children.[6]

In early 1996, Congress adopted two different approaches to the issue raised by *Stratton Oakmont*: the Exon-Coats amendment and the Online Family Empowerment Act (OFEA).[7] The Exon-Coats amendment, which

1. Enigma Software Group USA, LLC v. Malwarebytes, Inc., 946 F.3d 1040, 1054 (9th Cir. 2019).
2. *See id.* at 1045.
3. *See id.* at 1045 (quoting 47 U.S.C. § 230(c)(2) (1996)).
4. *See id.* at 1046 (citing *Stratton Oakmont, Inc. v. Prodigy Services Co.,* 1995 WL 323710, *5 (N.Y. Sup. Ct. May 24, 1995)).
5. *See Enigma*, 946 F.3d at 1046.
6. *See id.*
7. *See id.*

attempted to stop pornography from dissemination, was invalidated by *Reno v. ACLU*.[8] OFEA, however, was enacted as § 230(c)(2) and successfully overruled the *Stratton Oakmont* decision by allowing internet-service providers to claim immunity for offensive content liability when filtering certain third-party content.[9]

Although filtering pornography was the main concern of Congress at the time, § 230 includes broad language that allows the filtration of more categories of offensive content.[10] Additionally, Congress included five policy goals at the start of the statute, presumably to help interpret the broad language.[11] The court pointed out that three of those policy goals are relevant to the case at hand: (i) "to encourage the development of technologies which maximize user control[;]" (ii) "to empower parents to restrict their children's access to objectionable or inappropriate online content[;]" and (iii) "to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services."[12]

Since the enactment of § 230, the Ninth Circuit has only decided one other case relevant to the scope of the section: *Zango, Inc. v. Kaspersky Lab, Inc.*.[13] In that case, the court was called upon to determine whether or not computer security software providers could claim immunity under § 230.[14] The court answered that question in the affirmative, adding that providers also had discretion in determining what content falls under the "otherwise objectionable" clause of the statute.[15] Although the majority opinion in that case did not discuss the scope of that discretion any further, the concurring opinion by Judge Fisher warned that there would need to be limits on this discretion in the future.[16]

Enigma and Malwarebytes are direct competitors in the market for computer security software across the U.S.[17] Computer security software helps protect users from "malicious or threatening software" by alerting them of the presence of such malware and then blocking it from their computer.[18] When determining which content to block, Malwarebytes uses a program to look for Potentially Unwanted Programs (PUPs).[19] When a PUP is found, the program alerts the user to the PUP's presence via a pop-up alert and recommends that the user block that content.[20] In 2016, Malwarebytes began flagging Enigma's software, which Enigma claims is due to Malwarebytes changing their PUP program to include anticompetitive criteria when searching for programs to flag.[21]

---

8. *See id.*
9. *See id.* at 1046-47.
10. *See id.* at 1047.
11. *See id.*
12. *See id.*
13. *See id.* (citing *Zango*, 568 F.3d 1169, 1175 (9th Cir. 2009)).
14. *See id.* (citing *Zango*, 568 F.3d at 1175).
15. *See id.*(citing *Zango*, 568 F.3d at 1175).
16. *See id.* at 1047 (citing *Zango*, 568 F.3d at 1175 (Fisher, J., concurring)).
17. *See id.*
18. *See id.*
19. *See id.*
20. *See id.*
21. *See id.* at 1048.

In Enigma's complaint, the company asserted three claims under New York state law and one claim under federal law, which alleged a violation of the Lanham Act.[22] Malwarebytes's motion to transfer venue was granted, and thus the case moved from New York to California.[23] The district court granted Malwarebytes' motion to dismiss for failure to state a claim based on their finding that Malwarebytes had immunity under § 230 for all three state law claims. The district court based its ruling on its understanding that *Zango* gave unlimited discretion to internet-service providers in determining which content was "otherwise objectionable."[24]

In regards to the federal law claim, the district court held that since Enigma's claim under the Lanham Act was related to false advertising and not intellectual property, the intellectual property exception to § 230 (found at 47 U.S.C. § 230(e)(2), and which states that § 230 immunity "shall not be construed to limit or expand any law pertaining to intellectual property") was inapplicable, even though the Lanham Act relates partially to intellectual property.[25] The district court therefore ruled in favor of Malwarebytes and dismissed all four claims.[26] Enigma's primary contention on appeal is that the district court interpreted *Zango* too broadly and that the Good Samaritan clause does not include anticompetitive conduct.[27]

II. ANALYSIS

The Ninth Circuit analyzed whether or not internet-service providers could block content for anticompetitive reasons and still fall under the immunity granted by § 230.[28] The court found that although there was a split among the district courts in applying the *Zango* ruling, the decisions holding *Zango* to not be overly expansive were the most persuasive because these decisions were most in line with the congressional history behind the CDA and with the stated policy goals of § 230.[29] Primarily, the court found that Congress's intention was to drive competition for filtering software, not hinder it, and that to hold that blocking content for anticompetitive reasons was valid under the "otherwise objectionable" clause would go against that intention.[30] The court concluded that since the immunity did not apply to content blocked for anticompetitive reasons, the three state law claims should not have been dismissed and therefore, the decision as to these three claims was reversed and remanded.[31]

In response to the Lanham Act claim, the court affirmed the finding of the district court that merely having a claim under the Act was not enough for the claim to fall under the intellectual property exception of § 230 if the claim

22. *See id.*
23. *See id.*
24. *See id.*
25. *See id.* at 1048-49.
26. *See id.* at 1049.
27. *See id.*
28. *See id.* at 1050.
29. *See id.* at 1050-51.
30. *See id.* at 1051.
31. *See id.* at 1052.

itself was not directly related to intellectual property.[32] Although the federal claim did not fall under the intellectual property exception, the federal claim was based on allegations of anticompetitive conduct like the state law claims and therefore the decision as to the federal claim was also reversed and remanded.[33]

Judge Rawlinson dissented, claiming that the arguments in favor of limiting the "otherwise objectionable" clause were unpersuasive and that the clause at issue allows for total discretion on behalf of the internet-service provider.[34]

III. CONCLUSION

The United States Court of Appeals for the Ninth Circuit held that 47 U.S.C. § 230(c)(2) does not provide immunity to internet-service providers who block content for anticompetitive reasons, because to hold that it does would violate the history and stated policy goals of the statute, and, therefore, the district court erred in dismissing the four claims brought by Enigma.[35]

32. *See id.* at 1053.
33. *See id.* at 1054.
34. *See id.* at 1054-55 (Rawlinson, J., dissenting).
35. *See id.* at 1044-54.