United States District Court
Northern District of California

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

ENIGMA SOFTWARE GROUP USA LLC,

Plaintiff,

v.

MALWAREBYTES INC.,

Defendant.

Case No. 5:17-cv-02915-EJD

ORDER GRANTING DEFENDANT'S MOTION TO DISMISS

Re: Dkt. No. 97

Plaintiff Enigma Software Group USA LLC ("Enigma") brings claims against Defendant Malwarebytes Inc. based on its allegation that Malwarebytes unlawfully characterized Enigma's software as harmful to users' computers. Malwarebytes now moves to dismiss under Fed. R. Civ. P. 12(b)(6). Malwarebytes's motion will be granted.

I. BACKGROUND

Malwarebytes develops software that protects internet users from malware, adware, and other unwanted computer programs. First Am. Compl. ("FAC") ¶¶ 3, 36, Dkt. No. 33. Malwarebytes's software scans users' computers for "potentially unwanted programs," which it automatically flags and quarantines. Id. ¶ 5. When the software detects an unwanted program, it displays a notification and asks the user if she wants to remove the program from her computer. Id.

Enigma also provides anti-malware software to internet users. Id. ¶ 4. Enigma alleges that, in 2016, Malwarebytes revised the criteria it uses to identify unwanted programs. Id. ¶ 7. Under the new criteria, Malwarebytes's software identifies Enigma's software as a potential threat. Id. Enigma alleges that Malwarebytes's classification of Enigma's software is wrong because Enigma's programs "are legitimate and pose no security threat to users' computers." Id. ¶ 9. Enigma alleges that Malwarebytes revised its criteria to interfere with Enigma's customer base and to retaliate against Enigma for a separate lawsuit Enigma filed against a Malwarebytes affiliate. Id. ¶¶ 8, 19–20.

On that basis, Enigma brings claims for (1) false advertising in violation of § 43(a) of the Lanham Act (FAC ¶¶ 134–43), (2) violations of New York General Business Law § 349[1] (FAC ¶¶ 144–50), (3) tortious interference with contractual relations (FAC ¶¶ 151–160), and (4) tortious interference with business relations (FAC ¶¶ 161–68).

Malwarebytes now moves to dismiss under Fed. R. Civ. P. 12(b)(6). Def.'s Mot. to Dismiss ("MTD"), Dkt. No. 97.

II. LEGAL STANDARD

A motion to dismiss under Fed. R. Civ. P. 12(b)(6) tests the legal sufficiency of claims alleged in the complaint. Parks Sch. of Bus., Inc. v. Symington, 51 F.3d 1480, 1484 (9th Cir. 1995). Dismissal "is proper only where there is no cognizable legal theory or an absence of

[1] This case was transferred from the Southern District of New York on May 12, 2017. Dkt. No. 67.

sufficient facts alleged to support a cognizable legal theory." Navarro v. Block, 250 F.3d 729, 732 (9th Cir. 2001). The complaint "must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' " Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)).

III. DISCUSSION

Malwarebytes argues that all of Enigma's claims are barred by the immunity provisions of § 230(c)(2) of the Communications Decency Act. Mot. 7. That section provides:

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

47 U.S.C. § 230(c)(2). Congress enacted these provisions "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet," and to encourage "development and utilization of blocking and filtering technologies." Id. § 230(b)(3), (4).

Malwarebytes argues that this case is "indistinguishable" from the Ninth Circuit's opinion in Zango interpreting § 230(c)(2). Mot. 8; Zango, Inc. v. Kaspersky, 568 F.3d 1169 (9th Cir. 2009). In that case, Zango alleged that Kaspersky's anti-malware software incorrectly classified Zango's software as harmful. Zango, 568 F.3d at 1170–71. The Ninth Circuit considered whether "companies that provide filtering tools," such as Kaspersky, are eligible for immunity under § 230(c). Id. at 1173. The panel first explained that providers of blocking software are eligible for § 230(c)(2) immunity as long as they meet the statutory requirements. Id. at 1173–75. Next, it found that Kaspersky was an "interactive computer service" within the meaning of the statute. Id. at

1175–76. It also found that Kaspersky "has 'made available' for its users the technical means to restrict items that Kaspersky has defined as malware." Id. at 1176. The panel found that Kaspersky qualified for immunity under § 230(c)(2)(B) "so long as the blocked items are objectionable material under § 230(c)(2)(A)." Id. It concluded that Kaspersky properly classified malware as "objectionable" material, and as such, it found that Kaspersky satisfied the requirements for immunity under § 230(c)(2)(B). Id. at 1177–78 (holding that any "provider of access tools that filter, screen, allow, or disallow content that the provider or user considers obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable is protected from liability by 47 U.S.C. § 230(c)(2)(B) for any action taken to make available to others the technical means to restrict access to that material").

Enigma argues that Zango is distinguishable in two respects. First, Enigma argues that malware, as defined by Malwarebytes's criteria, is not one of the types of materials to which § 230(c)(2) immunity applies. Pl.'s Opp'n to Def.'s Mot. to Dismiss ("Opp'n") 11–12, 14, Dkt. No. 100. By its terms, § 230(c)(2)(A) applies to material that is "obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." § 230(c)(2)(B) applies to the same material.[2] Enigma argues that malware is not within the scope of "objectionable" material because it is "not remotely related to the content categories enumerated" in subsection (A) (i.e., materials that are "obscene, lewd, lascivious," and so on). Opp'n 10. Enigma further argues that Zango did not address whether an anti-malware provider has discretion to decide what is "objectionable," because, as the Ninth Circuit noted, Zango waived that argument by failing to raise it in its opening appellate brief. Id.; Zango, 568 F.3d at 1175–76.

However, while it is true that the Zango panel found that Zango waived this argument, Enigma overlooks Zango's clear holding that § 230(c)(2)(B) immunity applies to "a provider of computer services that makes available software that filters or screens material that the user or the

[2] Subsection (B) refers to "material described in paragraph (1)." This is a typo in the statute; it should read: "material described in paragraph (A)." See Zango, 568 F.3d at 1173 n.5 (" 'paragraph (1)' is a scrivener's error referring to 'paragraph (A)' ").

provider deems objectionable." Zango, 568 F.3d at 1173 (emphasis in original); see also id. at 1177 (holding that immunity applies to material "that the provider or user considers . . . objectionable") (emphasis added); id. (immunity applies to "material that either the user or the provider deems objectionable") (emphasis in original). This interpretation of Zango aligns with the plain language of the statute, which likewise states that immunity applies to "material that the provider or user considers to be . . . objectionable." 47 U.S.C. § 230(c)(2)(A) (emphasis added). In Zango, the provider of the anti-malware software, Kaspersky, exercised its discretion to select the criteria it would use to identify objectionable computer programs. The Ninth Circuit held that malware, as Kaspersky defined it, was properly within the scope of "objectionable" material. In that respect, the Court agrees with Malwarebytes that Zango is factually indistinguishable from the scenario here.

Second, Enigma argues that Malwarebytes is entitled to § 230(c)(2)(B) immunity only if it acted in "good faith." Opp'n 11–14. Subsection (A) protects "any action voluntarily taken in good faith" to restrict access to objectionable material (emphasis added). Subsection (B) does not contain a good-faith requirement. Nonetheless, Enigma argues that good faith is "an implied requirement in subsection (B) that is part and parcel of the proper, plain meaning of the statute when read as a whole." Opp'n 14. The Zango court did not decide whether subsection (B) contains a good-faith requirement, since Zango waived that argument on appeal and the panel did not need to resolve it to reach its decision. Zango, 568 F.3d at 1177. However, as the panel recognized, subsection (B) "has no good faith language." Id. Here, the Court must assume that Congress acted intentionally when it decided to include a good-faith requirement in subsection (A) but not in (B). See, e.g., Conn. Nat'l Bank v. Germain, 503 U.S. 249, 253–54 (1992) ("[I]n interpreting a statute a court should always turn first to one, cardinal canon before all others. We have stated time and again that courts must presume that a legislature says in a statute what it means and means in a statute what it says there."); Bailey v. United States, 516 U.S. 137, 146 (1995) ("The difference between the two provisions demonstrates that, had Congress meant to broaden application of the

statute . . . , Congress could and would have so specified."). This reading is bolstered by the fact that subsection (B) includes an explicit reference to subsection (A) with respect to the types of material to which immunity applies. Congress could have included a similar reference in subection (B) to subsection (A)'s good-faith requirement, but it chose not to. As such, the Court agrees with Malwarebytes that it need not consider whether Malwarebytes acted in good faith for the purposes of deciding whether Malwarebytes is entitled to immunity under § 230(c)(2)(B). Def.'s Reply in Support of Mot. to Dismiss ("Reply") 5–7, Dkt. No. 102.

Enigma argues Malwarebytes is nonetheless ineligible for immunity with respect to Enigma's Lanham Act claim (FAC ¶¶ 134–143) because § 230 provides that "nothing in [§ 230] shall be construed to limit or expand any law pertaining to intellectual property." 47 U.S.C. § 230(e)(2); Opp'n 15.[3] Enigma's argument fails because its complaint does not allege an intellectual property claim. The Lanham Act contains two parts: one governing trademark infringement (15 U.S.C. § 1114) and one governing unfair competition (15 U.S.C. § 1125(a)). The unfair competition provision, in turn, "creates two distinct bases of liability": one governing false association (15 U.S.C. § 1125(a)(1)(A)) and one governing false advertising (15 U.S.C. § 1125(a)(1)(B)). Lexmark Int'l, Inc. v. Static Control Components, Inc., 134 S. Ct. 1377, 1384 (2014). Enigma's complaint asserts a false advertising claim under § 1125(a)(1)(B). FAC ¶ 135. Enigma does not assert claims under the trademark provisions of the Lanham Act. The complaint does not allege that Enigma owns trademarks or any other form of intellectual property, nor does it allege that Malwarebytes has committed any form of intellectual property infringement, including misuse of its trademarks. Accordingly, the Court finds that Enigma's false advertising claim under the Lanham Act, 15 U.S.C. § 1125(a)(1)(B), does not arise under a "law pertaining to intellectual property" under 47 U.S.C. § 230(e)(2). See Perfect 10, Inc. v. CCBill, LLC, 340 F. Supp. 2d 1077, 1109–10 (C.D. Cal. 2004) ("Since false advertising . . . does not pertain to intellectual property

[3] Enigma does not dispute that immunity would apply to its other three claims for business torts. Opp'n 15; see also Zango, 568 F.3d at 1177 ("we have interpreted § 230 immunity to cover business torts").

rights, the Court finds that the immunity provided under the CDA for [the plaintiff's] false advertising claim is not excluded under § 230(e)(2).").

IV. CONCLUSION

Because Malwarebytes is entitled to immunity under 47 U.S.C. § 230(c)(2)(B) with respect to all of Enigma's claims, Malwarebytes's motion to dismiss is GRANTED. The Clerk shall close this file.

IT IS SO ORDERED.

Dated: November 7, 2017

EDWARD J. DAVILA
United States District Judge

United States District Court
Northern District of California