UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

ZANGO, INC.,

Plaintiff,

v.

KASPERSKY LAB, INC.,

Defendant.

CASE NO. C07-0807-JCC

ORDER

I. INTRODUCTION

Plaintiff's suit alleges that Defendant's filtering software wrongfully interferes with the operation of Plaintiff's own software. Because the Court finds that the Communications Decency Act ("CDA") immunizes Defendant from such claims, this Court hereby DISMISSES the entire matter under Federal Rule of Civil Procedure 56.

II. BACKGROUND AND FACTS

Plaintiff Zango is an Internet company that "provides consumers free access to a large catalog of online videos, games, music, tools and utilities" sponsored by advertisements. (Pl.'s Mot. for a TRO 3 (Dkt. No. 4).) Plaintiff Zango also offers a "premium version" of its software that provides the same content without advertisements for a fee.

Software sold by Defendant Kaspersky Lab Inc. ("Kaspersky USA") designates Plaintiff Zango's product as potentially harmful or malicious software ("malware") and interferes with its operations in a number of ways. In some cases, it may completely block its installation. Defendant's software products are called Kaspersky Internet Security and Kaspersky Anti-Virus (collectively "the Kaspersky Software"). The Kaspersky Software is developed by a separate company named Kaspersky Lab ZAO ("Kaspersky Moscow"), but is distributed in the United States by Kaspersky USA. The nature of the relationship between Kaspersky Moscow and Kaspersky USA is in dispute.

In its Complaint, Plaintiff Zango asserted claims for injunctive relief, tortious interference with contractual rights or business expectancy, a violation of the Washington Consumer Protection Act, trade libel, and unjust enrichment. (Compl. 5–7 (Dkt. No. 1 at 12–14).) Defendant moved to dismiss for lack of personal jurisdiction under Federal Rule of Civil Procedure 12(b)(2). (Dkt. No. 28.) It also moved to dismiss under Rule 12(b)(6) or, in the alternative, for summary judgment under Rule 56. (*Id.*)

III. ANALYSIS

A. Personal Jurisdiction

This Court has recently examined an almost identical motion to dismiss in *Zango, Inc. v. PC Tools Pty Ltd.*, No. C07-0797-JCC, Dkt. No. 41 (W.D. Wash. July 31, 2007). That Order determined that there were sufficient minimum contacts to exercise jurisdiction in this district over an Australian-based anti-malware company that intentionally sold its product directly to Washington consumers over its website. (*Id.* at 3–5.) For similar reasons, the Court finds that it has personal jurisdiction over this Defendant.

Any potentially relevant differences between the two cases do not alter this Court's conclusion. Jurisdiction is appropriate even though Defendant Kaspersky USA alleges that the relevant software is developed by a separate company, Kaspersky Moscow, which is not a party of this suit. Defendant Kaspersky USA purposely directed itself at the forum by knowingly selling its blocking software directly to Washington residents and Plaintiff's alleged harm arises out of these alleged sales. *See id.*; *Yahoo! Inc. v. La Ligue Contre Le Racisme Et L'Antisemitisme*, 433 F.3d 1199, 1207 (9th Cir. 2006) ("If a

jurisdictionally sufficient amount of harm is suffered in the forum state, it does not matter that even more harm might have been suffered in another state.") Just as in *PC Tools*, Defendant has also failed to make the requisite "compelling case" that the exercise of jurisdiction is unreasonable, especially given that the dispute is primarily over the nature of Plaintiff's Washington-based software. Although the question of whether Kaspersky Moscow or Kaspersky USA made the decision to classify Plaintiff Zango's software as malicious might affect liability on the substantive claims, it does not alter this Court's jurisdictional analysis. Accordingly, Defendant's motion to dismiss for lack of personal jurisdiction is denied.

B. Immunity Under the CDA

1. Standard of Review

Although initially presented as a motion under Rule 12(b)(6), Defendant Kaspersky USA's motion is properly reviewed as a motion for summary judgment under Rule 56 because "matters outside the pleading [we]re presented to and not excluded by the court." Fed. R. Civ. P. 12(b).[1] Rule 56 of the Federal Rules of Civil Procedure states that a party is entitled to summary judgment in its favor "if the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, if any, show that there is no genuine issue as to any material fact and that the moving party is entitled to a judgment as a matter of law." Fed. R. Civ. P. 56(c). In determining whether an issue of fact exists, the Court must view all evidence in the light most favorable to the nonmoving party and draw all reasonable inferences in that party's favor. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248–50 (1986); *Bagdadi v. Nazar*, 84 F.3d 1194, 1197 (9th Cir. 1996). A genuine issue of material fact exists where there is sufficient evidence for a reasonable factfinder to find for the nonmoving party. *Anderson*, 477 U.S. at 248. The inquiry is "whether the evidence presents a sufficient disagreement to require submission to a

---

[1] Plaintiff Zango's request that it "should be allowed to conduct discovery to gather additional facts" to respond to this summary judgment motion (Pl.'s Opp'n 7 (Dkt. No. 41 at 10)) is DENIED. The Court construes this request as a Rule 56(f) motion for additional time to conduct discovery and denies the motion because Plaintiff provides no justification for why such additional discovery would be necessary with respect to the immunity issue, and this Court can think of none.

jury or whether it is so one-sided that one party must prevail as a matter of law." *Id.* at 251–52. The moving party bears the burden of showing that there is no evidence which supports an element essential to the nonmovant's claim. *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). Once the movant has met this burden, the nonmoving party then must show that there is in fact a genuine issue for trial. *Anderson*, 477 U.S. at 250.

2. Whether Defendant is Entitled to Immunity at Summary Judgment

Defendant Kaspersky USA argues that it is entitled to immunity under 47 U.S.C. §§ 230(c)(2)(A) and (B). Section 230 was explicitly enacted "to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools who use the Internet and other interactive computer services," § 230(b)(3), and "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," § 230(b)(4).

One mechanism through which such policies were implemented is contained in § 230(c)(2). Under the heading "Protection for 'good samaritan' blocking and screening of offensive material" the statute states:

> 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 [A].[2]

47 U.S.C. § 230(c)(2). Courts interpreting the statute's immunity have found it to be "quite robust"

---

[2] The statute actually reads "material described in paragraph (1)." However, there appears to be no such material described in paragraph (1) and thus this Court assumes that the entry is a clerical error and that the reference should actually be to "paragraph (A)." This apparent typographical error has been pointed out by the West Group. 47 U.S.C.A. § 230(c)(2)(B) n.1 (West 2001 & 2007 Supp.) ("Probably should be 'subparagraph (A)'").

Carafano v. Metrosplash.com, Inc. 339 F.3d 1119, 1123 (9th Cir. 2003); *see also Batzel v. Smith*, 333 F.3d 1018, 1031 n.19 (9th Cir. 2003) (noting that § 230(c) affords "broad immunity").

Defendant Kaspersky USA first argues that it qualifies for immunity under § 230(c)(2)(B) because it is a provider or user of an interactive computer service that enables (or makes available) to others the technical means to restrict access to content that it (as a provider) considers sexually explicit, harassing, and otherwise objectionable. Plaintiff disputes, among other things, that Defendant is an "interactive computer service," that Plaintiff's software is "otherwise objectionable," and that Defendant Kaspersky USA has met a purported "good faith" requirement under the statute.

a. Whether Defendant Kaspersky USA is an "Interactive Computer Service"

Courts have read the term "provider" of an "interactive computer service" very broadly. The term "interactive computer service" is not limited to those who provide Internet access to consumers but rather includes "'*any*' information services or other systems, as long as the service or system allows 'multiple users' to access 'a computer server.'" *Batzel*, 333 F.3d at 1030.

Specifically, it includes any "access software provider" that "provides or enables computer access by multiple users to a computer server." § 230(f)(2). "Access software provider," in turn, is defined as a provider of software or tools that, among other things, "filter[s], screen[s], allow[s], or disallow[s] content." § 230(f)(4)(a). Clearly, Defendant's anti-malware software is exactly the type of "access software provider" contemplated by § 230(f)(4)(a) because it performs precisely the functions described. *See id.*

Thus, the only remaining issue is whether, as an "access software provider," the Kaspersky Software "allows multiple users to access a computer server." *See Batzel*, 333 F.3d at 1030 (internal quotations omitted). An examination of the specific technology readily demonstrates that the Kaspersky Software provides precisely such access. "After being downloaded and installed by Kaspersky's customers, the Kaspersky Internet security software regularly reaches out to communicate with online

servers to update the Kaspersky Internet security software's database of suspect code (*e.g.*, viruses, adware, spyware, and other malware)." (Orenberg Decl. ¶ 3 (Dkt. No. 50 at 1–2).) "A customer may configure the Kaspersky Internet security software to communicate with the online update servers via the Internet as often as once per hour." *Id.* ¶ 5. Thus, the software allows multiple users to access Kaspersky Moscow's remote servers, qualifying the Kaspersky Software as an "interactive computer service."

Plaintiff argues that the Kaspersky Software merely allows *itself* to communicate with an outside server, it does not allow *users* to do so. (Pl.'s Supp. Opp'n 4 (Dkt. No. 51 at 5).) Plaintiff's characterization of the Kaspersky Software's interaction as missing the requisite user is without merit. All Internet-based interactions necessarily involve computers interacting with one another to facilitate communication. Here, end-users install the Kaspersky Software on their computers. They then utilize the Kaspersky Software to reach out to a remote server and obtain content regarding the newest malware threats. This type of access is sufficient to qualify as an interactive computer service under the broad reading that courts has repeatedly given that term. *See Batzel*, 333 F.3d at 1030 & n.15. To the extent Plaintiff is arguing that all forms of interaction between user and server must be intentional in order to qualify as an interactive computer service (meaning that automatic updates do not count), such a reading is unsupported by the statute or its underlying policy considerations. Further, this argument ignores the fact that the Kaspersky Software at issue here does, in fact, allow intentional user access by giving users the option of conducting manual updates.

Accordingly, Defendant Kaspersky USA's software qualifies as an "interactive computer service." Defendant is thus entitled to immunity under § 230(c)(2)(B).

b. Whether the Blocked Material is "Otherwise Objectionable"

Plaintiff Zango argues that it does not provide "objectionable material" and therefore the Kaspersky Software's blocking of its software is not protected. This argument is based on a misreading of the statute. Section 230(c)(2)(A), which provides the definition of the relevant material described in Section 230(c)(2)(B), does not require that the material actually be objectionable; rather, it affords

protection for blocking material "that the provider or user considers to be" objectionable. 47 U.S.C. § 230(c)(2)(A). There is no question that Kaspersky USA considers the software to be objectionable.

c. Good Faith

Plaintiff Zango argues that § 230(c)(2)(B) only immunizes those actions taken in good faith, and that it has sufficiently alleged that Defendant Kaspersky USA has acted in bad faith in blocking Plaintiff's software as part of a scare campaign intended to generate additional interest in Defendant's software.

By its own terms, however, Section 230(c)(2)(B) has no good faith requirement. *Compare* 47 U.S.C. § 230(c)(2)(B) *with* 47 U.S.C. § 230(c)(2)(A). Thus, Defendant Kaspersky is immune under § 230(c)(2)(B) for "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 [A]" which is, "material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable." § 230(c)(2)(A)–(B). Here, Kaspersky USA has given users ("others," under the statute) the technical means to restrict access to material that Kaspersky USA considers objectionable by distributing to them Kaspersky Moscow's software. It is thus immune from liability under § 230(c)(2)(B).

Further, even if there was a good faith requirement to Section 230(c)(2)(B), Plaintiff's mere conclusory assertion of bad faith, without more, would be insufficient to withstand summary judgment. Accordingly, Defendant Kaspersky USA is immune from liability for all of Plaintiff Zango's claims under Section 230(c)(2)(B); thus, the Court need not reach the issue of whether it would be separately immune under Section 230(c)(2)(A). Defendant is thus entitled to summary judgment.

IV. CONCLUSION

For the foregoing reasons, Defendant's Kaspersky USA's motion to dismiss for lack of personal jurisdiction (Dkt. No. 28) is hereby DENIED; Defendant's motion for summary judgment (Dkt. No. 28) is hereby GRANTED. The Clerk is directed to close this case.

SO ORDERED this 28th day of August, 2007.

John C. Coughenour
United States District Judge